Auditaspecten binnen autorisaties in SAP R/3

Vrije Universiteit Amsterdam
Postgraduate IT Audit Opleiding

Eindscriptie, mei 2007

Ewald Franse

Voorwoord

Deze scriptie is de afsluiting van de Postgraduate IT Audit opleiding aan de Vrije Universiteit van Amsterdam. In de scriptie moet een probleem of vraagstuk uit de dagelijkse praktijk op academisch verantwoorde wijze uitgewerkt worden. Ik heb een scriptie geschreven met als onderwerp ‘Auditaspecten binnen autorisaties in SAP R/3’ en de hieraan gekoppelde aandachtspunten in het algemeen en specifiek voor SAP R/3. Gezien de actualiteit van het onderwerp en het belang hiervan voor IT-auditors, is dit een interessant onderwerp om in een scriptie te behandelen.

Vanuit de Vrije Universiteit Amsterdam is de heer Bart Bokhorst aangewezen als mijn afstudeerbegeleider. Ik wil hem bedanken voor de goede inhoudelijke ideeën, zijn uitleg en het doorlezen van de stukken. Zijn vakkundig inzicht heeft geholpen in het opleveren van dit uiteindelijke resultaat.

Ik wil verder mijn bedrijfsbegeleider Henk Peter Wind bedanken voor de opstartfase van de scriptie en het meelezen en adviseren tijdens de uitvoerende fase.

Ten slotte wil ik de (gast)docenten bedanken voor de leerzame colleges tijdens mijn studie. Dit alles heeft mij geholpen bij het schrijven van deze scriptie en ook bij het verbreden van mijn vakkennis op het gebied van EDP audit.

Ewald Franse
Amsterdam, mei 2007

Inhoudsopgave

1. Inleiding

1.1. Aanleiding

Bij het uitvoeren van een audit op een SAP R/3 systeem is de inrichting van autorisaties een belangrijk auditobject voor de IT-auditor. Een goede autorisatie-inrichting is noodzakelijk om personen toegang te verlenen op basis van need to know of need to access basis. Hierbij dient ook rekening te worden gehouden met de noodzakelijke functiescheiding en beperking van de toegang tot kritische functionaliteiten. Voor IT-auditors blijkt het in de praktijk vaak lastig te zijn om een goede audit uit te voeren naar autorisaties binnen SAP R/3, aangezien de opbouw hiervan vaak als complex wordt ervaren. Autorisaties binnen SAP R/3 kennen verschillende niveaus en objecten. Dit varieert van het gebruikers-ID tot aan bepaalde autorisaties binnen een transactie, met daartussen nog verschillende koppelingen die van invloed zijn. Daarbij komt ook nog dat SAP R/3 systemen over het algemeen worden gebruikt binnen grote organisaties en er daardoor bijvoorbeeld sprake is van duizenden gebruikers op het systeem. Voor IT-auditors die een audit uitvoeren naar autorisaties binnen SAP R/3, is het uiteraard van belang om te weten wat de auditaspecten hierbij zijn. De doelstelling is om te komen tot een set van auditaspecten, die de IT-auditor een handvat biedt bij het uitvoeren van een audit naar autorisaties binnen SAP R/3. Het moet voor een IT-auditor die te maken heeft met autorisaties in SAP R/3 duidelijk zijn op welke technische en functionele aspecten hij of zij in welke mate moet letten. Hierbij moet duidelijk zijn waar de grootste risico's zich bevinden en waar dus extra op gecontroleerd zou moeten worden. Ook voor andere personen die te maken hebben met autorisaties in SAP R/3, zoals Security Managers en Autorisatiebeheerders, is het positief als zij weten welke aspecten bij de inrichting van SAP R/3 autorisaties voor auditors relevant zijn. Hierdoor kunnen zij de kwaliteit van de inrichting van autorisaties in SAP R/3 binnen hun organisatie verbeteren.

1.2. Onderzoeksvragen

De centrale onderzoeksvraag van deze scriptie is:

Wat zijn de auditaspecten binnen autorisaties in SAP R/3?

Hierbij zullen de volgende deelvragen worden beantwoord:

- Wat zijn de belangrijkste aspecten? Oftewel, welke controles zou een IT-auditor altijd moeten doen bij een audit van autorisaties binnen SAP R/3?
- Wat is de samenhang tussen de aspecten?

Er zal hierbij in het bijzonder in worden gegaan op de kwaliteitsaspecten vertrouwelijkheid en integriteit.

1.3. Onderzoeksaanpak

Om te beginnen heb ik literatuur op het gebied van informatiebeveiliging en IT-audit geraadpleegd over aspecten, die in het algemeen van belang zijn bij autorisaties. Met betrekking tot algemene autorisatie aspecten is diverse literatuur beschikbaar. Ook zijn over dit onderwerp diverse artikelen geschreven. Deze literatuur en de artikelen geven een globaal beeld welke aspecten voor een IT-auditor relevant zijn bij een audit van autorisaties. Denk hierbij vooral aan AO/IC aspecten als functiescheiding.

Ik heb ook artikelen/studierapporten ten aanzien van Role Based Acces Control (RBAC) bestudeerd, aangezien SAP R/3 autorisaties meestal ook Role Based zijn en er dus diverse overeenkomsten zullen bestaan. Er is echter wel een wezenlijk verschil tussen de algemene uitgangspunten van RBAC en Role Based Access in SAP R/3. Namelijk dat het de Access Control binnen SAP R/3 systemen betreft en het niet over verschillende platformen heen gaat.

Verder zijn er nog een aantal artikelen opgenomen met betrekking tot Sarbanes-Oxley. Bij veel organisaties is het moeten voldoen aan Sarbanes-Oxley namelijk een belangrijke reden om een audit uit te laten voeren naar autorisaties binnen geautomatiseerde systemen.

Om een audit binnen SAP R/3 uit te voeren is het van groot belang dat de IT-auditor de autorisatiestructuur binnen SAP R/3 begrijpt. Daarom is deze autorisatiestructuur beschreven. Hierbij is informatie over SAP R/3 geraadpleegd. Ook is gebruik gemaakt van informatie binnen Control Solutions International (CSI). In de beschrijving van de autorisatiestructuur binnen SAP R/3 wordt duidelijk gemaakt welke elementen binnen de autorisatiestructuur relevant zijn bij een audit van autorisaties.

Uiteindelijk heb ik in kaart gebracht welke aspecten van belang zijn bij een audit van autorisaties in SAP R/3 en welke eisen hierbij aan autorisaties kunnen worden gesteld. Hierbij is aangegeven in welke mate deze zaken van toepassing zijn gelet op de diverse kwaliteitsaspecten.

1.4. Leeswijzer

De scriptie is als volgt opgebouwd. Hoofdstuk 2 gaat in op achtergronden van autorisaties. Verder worden in dit hoofdstuk de algemene auditaspecten binnen autorisaties beschreven. Hoofdstuk 3 beschrijft het SAP R/3 autorisatieconcept. Hierbij wordt ingegaan op de autorisatie-opbouw in SAP R/3. De meest kritische aspecten worden hierbij extra belicht. In hoofdstuk 4 wordt de toepassing van de algemene auditaspecten binnen autorisaties in SAP R/3 beschreven. Verder wordt er ingegaan op de samenhang met kwaliteitsaspecten. Tenslotte staat in hoofdstuk 5 de conclusie beschreven.

2. Auditaspecten binnen autorisaties

2.1. Achtergrond

Autorisaties vormen een belangrijk onderdeel van de systeembeveiliging. Autorisaties bepalen de activiteiten die gebruikers binnen informatiesystemen kunnen uitvoeren. Hierbij kan er voor processen of gegevens binnen informatiesystemen worden bepaald of gebruikers deze mogen creëren, wijzigen, verwijderen, lezen of uitvoeren.

De autorisatie-inrichting in IT systemen is van invloed op verschillende bedrijfsrisico's. Hierbij kan een onderscheid worden gemaakt naar de volgende risico's:

- Risico van onbevoegde kennisname; als vertrouwelijke personeelsgegevens of financiële gegevens door een onbevoegde worden ingezien, kan dit nadelige directe- en indirecte gevolgen hebben, zoals reputatieschade en balansverliezen.
- Procesrisico; dit betreft het risico op vernietiging, onderbreking en ongewenste wijzigingen in interne bedrijfsprocessen, administratieve processen, gegevens of externe bedrijfstransacties. Bijvoorbeeld dat er gegevens verloren gaan, doordat een ongeautoriseerde partij deze heeft verwijderd van het systeem. In het ernstigste geval kunnen dergelijke risico's leiden tot het verlies van bedrijfspartners, onderbreking van de productie en vermindering van bedrijfsactiva.
- Technisch risico; dit zijn symptomen van kwetsbaarheden in IT systemen. Technische risico's kunnen zich voordoen in individuele systemen, opslagmedia, communicatiekanalen of output devices. Deze risico's beïnvloeden veilige data opslag. Een gevolg van onveilige data opslag is verlies van informatie. Verder kan dit risico nadelige gevolgen hebben voor de continuïteit van processtromen. Een voorbeeld hiervan is dat een ongeautoriseerde partij wijzigingen doorvoert in de technische componenten binnen een systeem.
- Juridisch risico; er komt steeds meer wetgeving waaraan organisaties moeten voldoen. Dit betreft vooral gegevensbescherming, financiële rapportage en boekhoudingregels. Juridische risico's hangen samen met de hiervoor beschreven risico's. De oorzaken hiervan hebben ook betrekking op andere risico's, zoals onjuistheden in de financiële rapportage. Het gevolg van juridische risico's is vaak een rechtszaak. Directieleden worden steeds vaker verantwoordelijk gesteld voor het voldoen aan regels en wetgeving, met als gevolg dat zij hiervoor ook bestraft kunnen worden. Dit heeft niet alleen financiële consequenties meer, maar kan in zeer ernstige gevallen zelfs leiden tot een gevangenisstraf. De juridische risico's beïnvloeden vooral het managementniveau van organisaties en vormen ook een potentieel risico met betrekking tot aandelenkoersen.

Deze risico's hangen vaak samen vanwege de interactie tussen technische IT componenten, processen en systeemgebruikers. Uiteindelijk leiden deze risico's in veel gevallen tot financiële verliezen. Een goede autorisatie-inrichting in IT systemen is van belang om dergelijke risico's te minimaliseren.

Er bestaan verschillende autorisatievormen binnen informatiesystemen. Deze zijn afhankelijk van het specifieke informatiesysteem. De meest voorkomende autorisatievormen op dit moment zijn gebruikers toewijzen aan autorisatiegroepen en gebruikers toewijzen aan rollen of profielen in de vorm van een functie of deeltaak. Deze autorisatiegroepen, rollen of profielen zijn uiteindelijk gekoppeld aan autorisatie-objecten die bepalen welke activiteiten gebruikers mogen uitvoeren, voor welke processen of gegevens binnen informatiesystemen.

Daarnaast is ook nog een verschil in uitgangspunt bij het autoriseren tussen:

1. Niets is toegestaan tenzij men hiervoor geautoriseerd is;
2. Alles is toegestaan tenzij er expliciet is bepaald dat iets niet is toegestaan.

De eerste methode is het meest betrouwbaar, omdat als een gebruiker zonder autorisaties is opgevoerd, deze geen toegang heeft in plaats van alle toegang. Om toegang te krijgen moet er een actie worden uitgevoerd, namelijk een autorisatie toekennen. Zonder actie is alles per definitie beschermd. Men kan dus nooit per ongeluk toegang krijgen, omdat men bijvoorbeeld vergeten is de objecten te beschermen of hiermee te laat geweest is.

In dit hoofdstuk zal er nog niet op een specifieke vorm van autoriseren worden ingegaan en zal er worden gesproken over ‘autorisaties’.

Het beheer van autorisaties kan worden opgedeeld in drie verschillende niveaus:

1. Het eerste en hoogste niveau is het strategische niveau. Op dit niveau wordt het beleid met betrekking tot autorisatiebeheer gedefinieerd. Het gaat hierbij om de uitgangspunten in hoofdlijnen.
2. Het tweede niveau is het tactische niveau. Op dit niveau worden de processen rondom autorisatiebeheer gedefinieerd. Dit gaat ook om het beheer van het autorisatiemodel.
3. Het derde niveau is het operationele niveau. Op dit niveau worden de uiteindelijke autorisaties toegekend. Dit gebeurt in de regel aan de hand van werkinstructies.

In de ideale situatie zijn gebruikers alleen voor de activiteiten binnen processen of gegevens geautoriseerd die zij nodig hebben voor hun werkzaamheden. In de praktijk is dit vaak moeilijk te realiseren, omdat er sprake is van een groot aantal verschillende gebruikers, die toegang moeten hebben tot een groot aantal verschillende activiteiten binnen processen of gegevens. Om reden van beheersbaarheid hebben gebruikers in de praktijk daarom vaker meer autorisaties dan strikt noodzakelijk. Door autorisaties die weinig risico’s opleveren samen te voegen en niet afzonderlijk toe te wijzen, kan worden volstaan met minder groepen. Het vereenvoudigen van het beheer komt de overzichtelijkheid ten goede en daarmee uiteindelijk ook de beveiliging.

2.2. Autorisaties als auditobject

De aanleiding om een audit uit te voeren naar de autorisatie-inrichting binnen de informatiesystemen en processen die hierbij van invloed zijn, is meestal dat organisaties zekerheid willen hebben over de betrouwbaarheid van de autorisatie-inrichting. Om deze zekerheid vanuit een onafhankelijke partij te verkrijgen, zal er periodiek een audit moeten worden uitgevoerd naar de autorisatie-inrichting.

Het kan voorkomen dat er een audit wordt uitgevoerd naar de inrichting van autorisaties omdat er fraude is gepleegd. Dit kan veroorzaakt zijn doordat personen autorisaties hebben die zij niet nodig hebben in het kader van hun werkzaamheden, of omdat er sprake is van functievermenging tussen de activiteiten waarvoor personen zijn geautoriseerd.

Een belangrijke reden waarom de laatste jaren steeds vaker audits worden uitgevoerd van de autorisaties binnen informatiesystemen, is dat organisaties moeten voldoen aan Sarbanes-Oxley Act. Dit betreft bedrijven die genoteerd zijn aan de New York Stock Exchange of NASDAQ. Het belangrijkste gedeelte van de Sarbanes-Oxley Act dat van invloed is op de inrichting van autorisaties is Section 404. Hierin wordt de behoefte benadrukt van investeerders om niet alleen te kunnen vertrouwen op de financiële rapporten die door een bedrijf worden uitgebracht, maar ook op de onderliggende processen en de controles, die een integraal deel van het tot stand komen van die rapporten zijn. Auditors dienen hierbij een oordeel te geven over de financiële rapportages en de onderliggende processen en de controles bij de totstandkoming hiervan. Autorisaties zijn hierbij van belang aangezien deze bepalen of personen de mogelijkheid hebben om invloed hierop te hebben. De autorisaties binnen processen die als kritisch zijn gedefinieerd, binnen organisaties in het kader van Sarbanes-Oxley Section 404, dienen dus ook periodiek te worden gecontroleerd.

Dit zijn financiële processen en andere bedrijfsprocessen die van invloed zijn bij de totstandkoming van de financiële rapportages. Sarbanes-Oxley Section 404 gaat echter niet specifiek op de aspecten van autorisaties in. Dat betekent dat deze aspecten door de organisatie en de auditors moeten worden bepaald. Het belangrijkste autorisatie aspect hierbij is, dat personen alleen toegang mogen hebben, tot in het kader van in Sarbanes-Oxley Section 404 als kritisch of vertrouwelijk gedefinieerde processen en gegevens, indien dit in het kader van hun functie binnen de organisatie noodzakelijk is. Hierbij speelt ook het aspect functiescheiding een belangrijke rol. Het mag niet mogelijk zijn dat personen geautoriseerd zijn voor een combinatie van processen en/of gegevens die het mogelijk maken om fraude te plegen.

De volgende onderdelen zijn van belang bij een audit van autorisaties binnen informatiesystemen:

- Autorisatiebeleid;
- Autorisatiebeheer processen;
- Rapportage en controle autorisaties.

Deze onderdelen zullen in de volgende paragrafen worden beschreven.

2.3. Autorisatiebeleid

Binnen de organisatie dient autorisatiebeleid geformuleerd te zijn. Dit beleid zou periodiek moeten worden gecontroleerd op eventueel noodzakelijke aanpassingen. In het beleid dient het eigenaarschap van het proces Autorisatiebeheer te zijn bepaald.

2.3.1. Doel

Om te beginnen zullen het doel (of de doelen) en de uitgangspunten gedefinieerd moeten zijn. Dit is noodzakelijk om de uitwerking van het beleid vorm te geven. In de doelstelling zal aangeven worden wat men met het autorisatiebeleid wil bereiken. De hoofddoelstelling zal meestal het voorkomen van ongeautoriseerde toegang zijn. Daarbij kunnen nog een aantal subdoelstellingen worden geformuleerd ten behoeve van het bereiken van de hoofddoelstelling. Voor het voorkomen van ongeautoriseerde toegang is het bijvoorbeeld noodzakelijk, dat personen alleen toegang hebben tot gegevens die noodzakelijk zijn bij de uitoefening van hun functie. In de uitgangspunten zou onder meer vermeld moeten staan wat de scope is en welke randvoorwaarden er gelden. In de scope dient bijvoorbeeld aangegeven te worden op welke informatiesystemen het beleid betrekking heeft. In de randvoorwaarden dienen zaken uitgesloten te worden waarop het beleid niet ingaat. Het uitgewerkte beleid zou uiteindelijk afgeleid moeten zijn van de geformuleerde doelstelling(en) en uitgangspunten.

2.3.2. Richtlijnen

Er dienen in het beleid richtlijnen te zijn opgenomen waarin bepaald wordt welke omgevingen en doelsystemen binnen de scope vallen. Hierbij dienen bepalingen te zijn opgenomen voor de ontwikkeling-, test-, acceptatie- en productie-omgeving. De uitgangspunten voor de autorisaties dienen te zijn gedefinieerd en betreffen:

- Geen ontwikkelingsactiviteiten op productie-omgevingen;
- Scheiding van soorten gebruikers en autorisaties op verschillende omgevingen;
    - Geen eindgebruikers op ontwikkelomgeving;
    - Geen systeembeheerders en -ontwikkelaars met operationele autorisaties voor eindgebruikersfunctionaliteiten op productie-omgeving.

In het autorisatiebeleid dienen richtlijnen te zijn opgenomen of er gebruikers-ID's mogen bestaan die alle autorisaties hebben. Als dit het geval is dienen hiervoor randvoorwaarden te zijn beschreven. Deze zouden de bepaling moeten bevatten, dat er gespecificeerd dient te zijn welke gebruikers-ID's het betreft en op welke systemen dit van toepassing is. Hierbij dient ook altijd de reden te worden vermeld waarom de betreffende gebruikers-ID's alle autorisaties hebben en wat hier de risico's met bijbehorende compenserende maatregelen zijn.

Ook dienen in het autorisatiebeleid richtlijnen te zijn opgenomen met betrekking tot de opbouw van autorisaties. Hierbij dienen de volgende zaken te zijn bepaald:

- De soorten autorisaties die worden gebruikt:
    - functie/proces gerelateerd;
    - taak gerelateerd;
    - project gerelateerd;
    - organisatie gerelateerd;
    - geografisch gerelateerd;
- De autorisatiestructuur, waarbij minimaal aandacht besteed is aan:
    - autorisatie hiërarchieën;
    - het automatisch 'erven' van autorisaties;
- De naamgevingconventies binnen autorisaties;
- Rekening houden met functiescheiding binnen autorisaties.

De wijze van controle op de inrichting en uitvoering van de activiteiten dient ook in het autorisatiebeleid te zijn opgenomen. Er dient hierbij te worden bepaald welke functionaris met welke frequentie bepaalde controles uitvoert. Controlerende activiteiten moeten in functie gescheiden zijn van uitvoerende activiteiten.

In het autorisatiebeleid moet rekening worden gehouden met het effect van classificatie van gegevens en systemen. Bij de classificatie "kritisch" kan er bijvoorbeeld sprake zijn van het uitvoeren van extra controles op autorisaties. Het inrichtingsproces van autorisaties moet hiermee rekening houden.

2.3.3. Taken en verantwoordelijkheden

Bij het proces voor autorisatiebeheer zijn diverse functionarissen direct of indirect betrokken.
De activiteiten die deze functionarissen uitvoeren dienen in het autorisatiebeleid te zijn vastgelegd, waarbij sprake is van een controletechnische functiescheiding tussen de volgende activiteiten en verantwoordelijkheden:

- Eigenaarschap van het proces Autorisatiebeheer, verantwoordelijk voor het realiseren van de doelstellingen van het proces en het onderhoud van het gehanteerde autorisatiemodel;
- Gebruikersbeheer, verantwoordelijk voor het beheer van de gebruikers-ID's en de koppeling van gebruikers aan autorisaties;
- Security functie, verantwoordelijk voor het goedkeuren en toezicht op de interne autorisaties van het autorisatiebeheer. Daarnaast kunnen zij ook een bredere controlerende functie hebben afhankelijk van de positionering van deze functie binnen de organisatie. Dit betreft dan bijvoorbeeld het goedkeuren en toezicht van autorisaties van andere functionarissen binnen de organisatie;
- Autorisatiebeheer, verantwoordelijk voor het beheer van de autorisaties;
- Eigenaarschap van objecten, verantwoordelijk voor de toegang tot het object. Deze objecten betreffen applicaties, organisatieprocessen en bedrijfsgegevens;
- Functioneel beheer van applicaties, verantwoordelijk voor aansturing van de autorisatiebeheerder betreffende het aanmaken van autorisatiegroepen/applicatierollen, de koppeling daarvan met de objecten en het vastleggen van de gerelateerde permissies;

- Aanvrager, verantwoordelijk voor een juiste en tijdige aanvraag van wijzigingen in de implementatie en toewijzing van autorisaties. De aanvrager is in de meeste gevallen een (lijn)manager die autorisaties aanvraagt voor medewerkers waarvoor deze verantwoordelijk is.
- Controlefunctie, verantwoordelijk voor de periodieke toetsing op de beheersbaarheid van de geïmplementeerde autorisaties en controle op de effectiviteit ervan.

Een combinatie van controlerende en uitvoerende verantwoordelijkheden dient niet bij één persoon te worden belegd, in verband met controletechnische functiescheiding. Verder dient de aanvrager niet te zijn betrokken in de goedkeuring en uitvoering van de betreffende aanvraag. De aanvrager mag zelf geen wijzigingen aanvragen die van invloed zijn op het eigen gebruikers-ID.

2.3.4. Koppeling andere processen

In het autorisatiebeleid zal beschreven moeten zijn, hoe de koppeling tussen het gehele incidenten- en wijzigingsproces voor informatiesystemen, en het incidenten- en wijzigingsproces voor autorisaties eruit ziet. Elke wijziging dient te worden gevalideerd door daartoe bevoegde personen. Incidenten met betrekking tot autorisaties dienen te worden vastgelegd en te worden geanalyseerd. Bij veel organisaties maakt men hierbij gebruik van ITIL. Autorisatie incidenten en wijzigingen dienen dan in principe ook de ITIL processen te volgen.

Verder bestaan er koppelingen met het personeelsproces, waarbij medewerkers in-, door- en uitstromen. Bij instroom van nieuwe medewerkers zullen de noodzakelijke autorisaties geregeld moeten worden. Wanneer medewerkers doorstromen naar een andere functie binnen de organisatie dienen in veel gevallen de autorisaties te worden aangepast. En wanneer medewerkers niet meer voor de organisatie werkzaam zijn dienen de autorisaties te worden ingetrokken. Al deze personeelsmutaties moeten worden doorgeven vanuit de HR-afdelingen aan de afdelingen die de autorisaties beheren, zodat deze de benodigde aanpassingen kunnen doorvoeren en kunnen controleren of medewerkers wel de juiste autorisaties hebben toegewezen. Vaak zullen aanpassingen, zoals het aanvragen van nieuwe autorisaties en autorisatiewijzigingen, echter specifiek moeten worden aangevraagd via autorisatie-aanvraagprocedures.

Er bestaat ook een koppeling met het ontwerpproces van informatiesystemen, waarbij de autorisatie-inrichting moet worden ontworpen. De autorisatie-inrichting dient hierbij zowel door de IT-organisatie, als door vertegenwoordigers vanuit de business-organisatie te worden goedgekeurd. Het ontwerpproces is van zeer groot belang, aangezien de gekozen autorisatie-inrichting uiteindelijk de beheersbaarheid van autorisaties bepaald. Het is daarom van invloed op het autorisatiebeheer en de controle op autorisaties. Een belangrijk hulpmiddel bij het ontwerpen van de autorisatie-inrichting is een autorisatiematrix. In een dergelijke matrix dient op individueel, functie- of groepsniveau te worden aangegeven welke autorisaties worden toegewezen. Een voorbeeld hiervan is een functie-takenmatrix. Hierin staan per functie de taken aangegeven, waarvoor medewerkers die de betreffende functie vervullen geautoriseerd moeten zijn. De taken bepalen dan de autorisaties. De autorisatiematrix kan ook als controlehulpmiddel worden gebruikt om te bepalen of medewerkers de juiste autorisaties hebben toegewezen.

2.4. Autorisatiebeheer

Autorisatiebeheer kan worden onderverdeeld in de volgende deelprocessen:

1. Beheer gebruikers-ID's;
2. Koppeling van autorisaties aan gebruikers-ID's;
3. Beheer autorisaties (bijvoorbeeld rollen en autorisatiegroepen).

Van het derde proces is sprake wanneer autorisaties inhoudelijk gewijzigd kunnen worden, zoals in het geval van autoriseren door middel van rollen en profielen. Autorisaties die aan gebruikers op de systemen toegekend zijn, kunnen dus zowel veranderen doordat de autorisaties (bijvoorbeeld

rollen) inhoudelijk worden aangepast, maar ook door de (ont)koppeling van de autorisaties aan hun gebruikers-ID.

Bij het beheer van autorisaties is het belangrijk om onderscheid te maken naar het beheer van gebruikers-ID's en het koppelen van autorisaties aan gebruikers-ID's, ofwel het beheer van autorisaties in enge zin. Het maken van dit onderscheid voorkomt dat een autorisatiebeheerder in staat is fictieve (niet als kritisch te onderkennen) gebruikers-ID's aan te maken en die autorisaties te geven. De beheerder zou in dat geval zelf onbevoegde handelingen kunnen uitvoeren die heel lastig aan hem of haar zijn toe te rekenen. Hij of zij werkt immers dan niet met zijn eigen userid. Het zal in de praktijk niet altijd mogelijk zijn om het beheer van gebruikers-ID's en het koppelen van autorisaties aan gebruikers-ID's te scheiden. Dit kan te maken hebben met organisatorische redenen, zoals in het geval dat de organisatie van een zeer kleine omvang is. Ook kan het te maken hebben met technische redenen. Het kan bijvoorbeeld zo zijn dat het in bepaalde systemen niet mogelijk is om dit onderscheid te maken. In deze gevallen dienen er compenserende maatregelen te worden genomen. Er zal een extra strikte controle plaats moeten vinden op de functionarissen die zich bezighouden met het autorisatiebeheer. Hun activiteiten zouden regelmatig moeten worden gecontroleerd door middel van bijvoorbeeld steekproeven van autorisatiewijzigingen.

Los hiervan dient altijd een zo beperkt mogelijke groep personen te zijn geautoriseerd voor het koppelen van autorisaties aan gebruikers-ID's, om zo het risico te minimaliseren dat er autorisaties toegewezen worden die niet zijn gevalideerd. En aangezien het voor functionarissen die zich bezighouden met het beheer van bijvoorbeeld rollen, niet noodzakelijk is om gebruikers-ID's te kunnen onderhouden, zouden zij dus deze autorisaties niet mogen hebben.

Alle functionarissen die zich bezighouden met het beheer van gebruikers-ID's en het beheer van de autorisaties zouden gescreend moeten zijn, voordat zij deze activiteiten mogen gaan uitvoeren. Personen die zich in het verleden schuldig hebben gemaakt aan frauduleuze zaken zouden deze activiteiten niet uit mogen voeren, aangezien deze activiteiten gevoelig zijn voor fraude.

Zowel het beheer van gebruikers-ID's als het beheer van autorisaties, zal meestal worden uitgevoerd met behulp van tools. De meeste van de huidige systemen bevatten dergelijke tools. Het beheer van gebruikers-ID's en het beheer van autorisaties vindt dan in de systemen plaats, waar de autorisaties van toepassing zijn. Daarnaast zijn er ook specifieke autorisatie-tools beschikbaar, die het implementeren, beheren en controleren van gebruikers-ID's en autorisaties mogelijk maken. Deze maken het implementeren, beheren en controleren vaak ook makkelijker. Dit kan bijvoorbeeld het geval zijn wanneer gebruikers-ID's en autorisaties van verschillende systemen binnen één tool beheerd kunnen worden.

Alle wijzigingen met betrekking tot autorisaties dienen te worden gelogd. In deze logging dienen de volgende zaken te zijn vermeld:

- Welke autorisaties toegewezen of verwijderd zijn, bij welk gebruikers-ID;
- De wijziging in de betreffende autorisatie (rol/profiel/autorisatiegroep);
- De naam of het gebruikers-ID van de functionaris die de wijziging heeft doorgevoerd;
- De datum van de wijziging.

2.4.1. Beheer gebruikers-ID's

Het beheer van gebruikers-ID's omvat diverse activiteiten. De algemene gebruikersgegevens zullen moeten worden beheerd. Van iedere gebruiker dient de naam bekend te zijn, zodat deze geïdentificeerd kan worden. Verder kan het praktisch zijn als afdelings- en locatiegegevens worden geregistreerd bij het gebruikers-ID, zodat gebruikers gemakkelijk terug te vinden zijn binnen de organisatie. Dit is ook van belang bij de controle van de toewijzing van autorisaties, omdat aan de hand van de afdeling en locatie vaak al voor een deel bepaald kan worden of de gebruiker de juiste autorisaties heeft. Veel organisaties hebben echter een intranet waarop deze gegevens te achterhalen zijn aan de hand van de naam van de gebruiker, dus dan zou het bijhouden van deze

gegevens bij de gebruikers-ID's alleen maar extra beheeractiviteiten kosten. Daarnaast omvat het beheer van gebruikers-ID's ook het beheer van de gekoppelde wachtwoorden. Ook het blokkeren en deblokkeren van gebruikers-ID's is een activiteit die bij het beheer van gebruikers-ID's hoort.

Een andere activiteit die van toepassing is bij het beheer van gebruikers-ID's, is dat gebruikers-ID's worden verwijderd wanneer deze niet meer mogen worden gebruikt. Dit kan het geval zijn wanneer een persoon een andere functie heeft gekregen of niet meer werkzaam is binnen de organisatie. Hiervoor is het dus noodzakelijk dat wijzigingen in het personeelsbestand worden doorgegeven aan de beheerders van gebruikers-ID's. Verder dienen gebruikers-ID's te worden geblokkeerd indien deze tijdelijk niet worden gebruikt.

Deze gegevens staan op zich nog los van autorisaties maar zijn wel van indirect belang bij het autorisatieproces. Deze hebben namelijk te maken met identificatie en authenticatie. Het moet duidelijk zijn dat wanneer autorisaties worden toegewezen aan een gebruikers-ID, dit ook het ID is dat ook daadwerkelijk uniek aan de gebruiker is toegewezen en dat autorisaties niet aan verkeerde gebruikers-ID's worden toegewezen. Ook is het belangrijk dat niet-geautoriseerde gebruikers niet in kunnen loggen met een gebruikers-ID welke aan anderen toebehoort. Daarmee zouden deze gebruikers de autorisaties van iemand anders hebben.

2.4.2. Koppeling autorisaties aan gebruikers-ID's

De gebruikers-ID's die zijn aangemaakt dienen te worden gekoppeld aan autorisaties. De wijze waarop dit plaatsvindt, is afhankelijk van het autorisatiemechanisme dat wordt gehanteerd. Dit is meestal afhankelijk van het systeem. Gebruikers zouden alleen geautoriseerd mogen zijn voor activiteiten, die in het kader van de uitoefening van hun functie noodzakelijk zijn. Het is daarom bij de koppeling van autorisaties belangrijk dat duidelijk is welke activiteiten, door welke functie worden uitgevoerd en welke autorisaties dus moeten worden gekoppeld. Een autorisatiematrix is hierbij een goed hulpmiddel. Hierin zou dan per functie aangegeven moeten zijn, welke autorisaties toegewezen zouden moeten worden. Hier zou alleen van afgeweken mogen worden in overleg met een functionaris die verantwoordelijk is voor de AO/IC binnen de organisatie. Deze functionaris zou formeel akkoord moeten geven, alvorens de afwijkende autorisaties mogen worden gekoppeld.

Indien mogelijk zou er een directe koppeling moeten zijn met de functie die gebruikers vervullen, op basis van de gegevens in het HR systeem. Er zou een technische koppeling gemaakt kunnen worden, zodat gebruikers automatisch de autorisaties krijgen toegewezen die bij de functie horen, die zij volgens het HR systeem vervullen. In dat geval zouden de medewerkers ook andere autorisaties toegewezen kunnen krijgen, wanneer zij een andere functie gaan vervullen of wanneer hun functie-inhoud wijzigt. Oftewel automatische aanpassing van de IST- aan de SOLL-situatie. Als een technische koppeling niet mogelijk is dan zou er nog gekozen kunnen worden voor een verificatie met het HR systeem. Voordat er autorisaties aan een gebruikers-ID gekoppeld worden, zou er in het HR systeem nagegaan kunnen worden, welke functie de betreffende gebruiker vervult. Daarnaast zou de HR afdeling wijzigingen van de functie van medewerkers moeten doorgeven aan de functionaris die verantwoordelijk is voor de koppeling van autorisaties in het systeem. Een voorwaarde voor een koppeling met het HR systeem, is dat het HR systeem up-to-date moet zijn. Door een dergelijke koppeling kan het risico op een onjuiste koppeling van autorisaties aan gebruikers-ID's worden beperkt.

2.4.3. Beheer autorisaties

De autorisaties die gekoppeld worden aan de gebruikers-ID's moeten in de meeste gevallen beheerd worden. Dit is het geval als er sprake is van bijvoorbeeld rollen, profielen of autorisatiegroepen. Deze objecten moeten vaak worden aangemaakt en de inhoud ervan moet worden bepaald. De autorisaties dienen op een heldere en beheersmatige wijze te zijn opgezet. Dit is van groot belang om fouten te voorkomen bij het beheer van de autorisaties, maar ook bij de koppeling van de autorisaties aan de gebruikers-ID's. Uiteindelijk is dit ook van belang bij de

controle van de toewijzing van autorisaties. De volgende zaken zijn het meest belangrijk bij de opzet ten aanzien van het beheer van autorisaties:

- Volledige en up-to-date documentatie van de autorisaties. In de documentatie dient te zijn beschreven hoe de autorisaties zijn opgebouwd. Verder dienen eventuele uitzonderingen op de autorisatieopbouw te worden vermeld.
- Duidelijke werkinstructies. Hierin dienen de activiteiten te zijn uitgewerkt die van toepassing zijn bij het beheer van autorisaties. Dit zal vooral betrekking hebben op het incidenten- en wijzigingsproces.
- Heldere naamgevingconventies binnen autorisaties. De naamgevingconventie dient op een dusdanige wijze te zijn opgezet zodat het autorisatieproces beheersbaar is en het gemakkelijk te doorgronden is. Hiermee zal de kans op fouten worden beperkt.
- Bij de bepaling van autorisaties dienen naast de IT afdeling ook andere afdelingen in de organisatie te worden betrokken. Voor applicaties, gegevens en processen zouden eigenaren moeten worden aangewezen die bij de bepaling en wijziging van autorisaties worden betrokken.
- Indien er sprake is van meerdere systemen, dan dienen autorisatiestructuren waar mogelijk op elkaar aan te sluiten, zodat bij gelijksoortige systemen dezelfde autorisatiestructuur wordt gehanteerd. Ook dient er hierbij rekening te worden gehouden met autorisaties die over de systemen heen gaan. Denk hierbij in het bijzonder ook aan functiescheiding tussen de diverse systemen.

2.4.4. Autorisatie aanvraagprocedure

Autorisatie-aanvragen zouden altijd moeten verlopen volgens een geformaliseerde procedure, met daarin voldoende waarborgen ter voorkoming van fouten en fraude. Deze procedure dient de volgende bepalingen te bevatten:

- Autorisatie-aanvragen dienen vooraf goedgekeurd te worden door minimaal één functionaris die hiervoor bevoegd is vanuit de organisatie. Dit om te voorkomen dat gebruikers autorisaties toegewezen krijgen die zij niet nodig hebben voor hun werkzaamheden.
- Het mag niet mogelijk zijn dat gebruikers hun eigen aanvragen goedkeuren. Anders zou men autorisaties voor het eigen gebruikers-ID kunnen aanvragen, die men niet nodig heeft voor de eigen werkzaamheden. Dit met als doel om hiermee frauduleuze activiteiten te verrichten.
- Er dient handtekeningverificatie plaats te vinden van autorisatie aanvragen, die door middel van een formulier voorzien van een handtekening worden ingediend. Dit om de aanvrager te identificeren en dus uit te sluiten dat de handtekening is vervalst.
- Autorisatie-aanvragen dienen te worden gearchiveerd. Men moet elke wijziging van autorisaties van gebruikers kunnen achterhalen. Dit kan bijvoorbeeld van groot belang zijn als er fraude is gepleegd.

Deze bepalingen zijn van toepassing op de aanvraag van gebruikers-ID’s, de koppeling van gebruikers-ID’s met autorisaties en wijzigingsverzoeken ten aanzien van bijvoorbeeld rollen, profielen of autorisatiegroepen.

De volgende bepalingen zouden moeten zijn opgenomen in de autorisatie aanvraagprocedure ten aanzien van de koppeling van autorisaties met gebruikers-ID’s:

- Aanvrager mag niet alleen aangeven dat een gebruiker dezelfde autorisaties moet hebben als een andere gebruiker; oftewel het kopiëren van de autorisaties van gebruikers-ID’s is niet toegestaan. Hiermee kan voorkomen worden dat gebruikers te veel of verkeerde autorisaties toegewezen krijgen. Dit omdat de aanvrager in veel gevallen niet van te voren checkt of de gebruiker, die al in het systeem staat, daadwerkelijk de autorisaties heeft die hij of zij zou verwachten.
- Autorisaties die op tijdelijke basis extra worden toegevoegd aan gebruikers-ID’s dienen indien mogelijk te worden voorzien van een einddatum. Hiermee kan voorkomen worden dat de autorisaties langer toegewezen zijn dan dat nodig is.

- Autorisaties die worden toegevoegd aan gebruikers-ID's van tijdelijke medewerkers dienen indien mogelijk te worden voorzien van een einddatum. Hiermee kan voorkomen worden dat de autorisaties langer toegewezen zijn dan dat nodig is.

Wanneer er sprake is van autorisaties die inhoudelijk ook gewijzigd kunnen worden, dienen hiervoor ook bepalingen te zijn opgenomen in de autorisatie aanvraagprocedure. Dit is het geval wanneer er sprake is van rollen, profielen of autorisatiegroepen die kunnen worden gewijzigd. De procedure dient de volgende bepalingen te bevatten:

- Autorisatiewijzigingen dienen te worden gecontroleerd op functiescheiding. Dit om te voorkomen dat er functievermenging ontstaat binnen autorisaties en daarmee gebruikers de mogelijkheid hebben om frauduleuze activiteiten te verrichten.
- Autorisatiewijzigingen dienen te worden gecontroleerd op kritische functionaliteit. Hiermee kan voorkomen worden dat gebruikers toegang krijgen tot kritische functionaliteit die zij niet nodig hebben voor hun werkzaamheden.
- Autorisatiewijzigingen dienen indien mogelijk te worden getest op een test- en/of acceptatiesysteem. Dit om te voorkomen dat autorisaties op het productiesysteem anders zijn dan men zou verwachten.

Alvorens aan deze bepalingen is voldaan mogen de autorisatiewijzigingen niet op productie-systemen actief zijn.

Functionarissen die autorisatie-aanvragen goed moeten keuren, moeten op de hoogte zijn van de inhoud van de autorisaties. Gebruikers zouden alleen autorisaties toegewezen mogen krijgen die zij in het kader van de functie die zij vervullen nodig hebben. Een autorisatiematrix kan hierbij een goed hulpmiddel zijn. Hierin staat op individueel, functie- of taak-niveau aangegeven welke autorisaties toegewezen zouden moeten worden.

2.5. Rapportage en controle autorisaties

Er dienen periodiek controles plaats te vinden op autorisaties. Indien mogelijk zou dit geautomatiseerd plaats moeten vinden, omdat dan een volledige controle mogelijk is. Als dit niet mogelijk is dan zou een volledige controle vaak teveel tijd kosten. In dat geval zouden er steekproeven moeten worden genomen.

De uitvoerende functionarissen zouden zelf hun eigen werkzaamheden kunnen controleren, zodat eventuele onvolkomenheden kunnen worden hersteld. Het is echter van groot belang dat deze controles ook worden uitgevoerd door functionarissen die niet betrokken zijn in uitvoerende processen binnen autorisaties. Als dit niet zou plaatsvinden dan zouden de uitvoerende functionarissen onvolkomenheden (on)bewust kunnen laten bestaan. De controles zouden plaats kunnen vinden door één of meerdere van de volgende functionarissen:

- Security manager;
- AO/IC manager;
- Controller;
- Lijnmanager van de functionarissen van de betreffende gebruikers-ID's;
- IT manager;
- Interne auditor;
- Information manager.

Ook de rapportages die als input dienen voor de controle op autorisaties zouden vervaardigd moeten worden door functionarissen, die niet betrokken zijn in uitvoerende processen binnen autorisaties.

Het is aan te bevelen om alle aan gebruikers-ID's toegewezen autorisaties minimaal één maal per 6 maanden te controleren. De controles zouden zo veel mogelijk geautomatiseerd plaats moeten vinden, waarbij een automatische vergelijking van de SOLL- met de IST-situatie plaatsvindt. Hierbij dient te worden gecontroleerd of de gebruikers alleen die autorisaties toegewezen hebben gekregen, die zij nodig hebben bij de uitoefening van hun functie. Het dient dus bekend te zijn welke functie de medewerkers binnen de organisatie vervullen. Dit kan in veel gevallen achterhaald worden aan de hand van actuele gegevens vanuit het HR systeem. Bij de controle kan een autorisatiematrix als norm worden gebruikt. De in het systeem toegewezen autorisaties aan het gebruikers-ID, zouden vergeleken moeten worden met de autorisaties die de medewerker op basis van zijn of haar functie, vanuit de autorisatiematrix moet hebben.

Er dient minimaal maandelijks te worden gecontroleerd of er gebruikers-ID's bestaan die alle autorisaties hebben binnen informatiesystemen. Er dient te worden geverifieerd of dit terecht is. Ook dient er logging plaats te vinden van de activiteiten van deze gebruikers op de informatiesystemen.

Bij de autorisatiecontroles en de daarbij behorende rapportages, dient extra aandacht te worden besteed aan autorisaties binnen kritische functionaliteit en functievermenging binnen autorisaties.

2.5.1. Kritische functionaliteit

Functionaliteit binnen informatiesystemen kan als kritisch worden gedefinieerd als deze van grote invloed is op de belangrijkste processen binnen de organisatie. Het gaat dan vaak om functionaliteit die kan veroorzaken dat bepaalde processen stil komen te liggen en financiële processen. Dit betreft verschillende soorten systeemfunctionaliteit:

- Functionaliteiten binnen als kritisch geclassificeerde bedrijfsprocessen;
    - Processen die directe of indirecte invloed hebben op financiële rapportages;
    - Processen die als kritisch zijn gedefinieerd in verband met wetgeving (bijvoorbeeld Sarbanes-Oxley Section 404 en Wet Bescherming Persoonsgegevens);
    - Alle overige processen die door de organisatie als kritisch zijn geclassificeerd.
- Functionaliteiten ten behoeve van systeembeheer;
    - Beheer systeemparameters;
    - Beheer achtergrondprocessen;
    - Databasemanagement;
    - Autorisatiebeheer;
    - Gebruikersbeheer;
- Functionaliteiten ten behoeve van systeemontwikkeling.
- Functionaliteiten ten behoeve van (master)datamanagement.

Uitgangspunt bij kritische functionaliteit is dat alleen gekwalificeerde functionarissen deze uit mogen voeren. Dergelijke functionaliteit dient ook altijd bij een zo beperkt mogelijke groep gebruikers te worden belegd, waarbij deze onmisbaar is bij de uitoefening van hun functie.

Elke functionaliteit die als kritisch wordt beschouwd zou nog een classificatie kunnen krijgen in welke mate deze functionaliteit kritisch is. Autorisaties binnen kritische functionaliteiten zouden minimaal één maal per 3 maanden gecontroleerd moeten worden. Hierbij dient te worden gecontroleerd of gebruikers, die als kritisch gedefinieerde autorisaties hebben toegewezen, deze autorisaties daadwerkelijk nodig hebben bij de uitoefening van hun functie. Ook bij deze controle kan een autorisatiematrix als norm worden gebruikt. De in het systeem toegewezen kritische autorisaties aan het gebruikers-ID zouden vergeleken moeten worden met de autorisaties, die de medewerker op basis van zijn of haar functie vanuit de autorisatiematrix moet hebben.

2.5.2. Functievermenging

Het mag niet mogelijk zijn dat personen geautoriseerd zijn voor een combinatie van processen en/of gegevens die het mogelijk maken om fraude te plegen. Er zou daarom minimaal één maal per 3 maanden gecontroleerd moeten worden of er sprake is van functievermenging binnen of tussen de informatiesystemen. Er kan een onderscheid worden gemaakt tussen verschillende vormen van functievermenging binnen of tussen de informatiesystemen. Er is sprake van functievermenging op organisatorisch niveau, als gebruikers toegang hebben tot het uitvoeren van transacties of het wijzigen van gegevens binnen verschillende processen. Gebruikers mogen daarom niet zijn geautoriseerd voor meerdere processen in de fasen van de waardenkringloop:

- Inkopen;
- Inkoopschulden;
- Voorraden;
- Verkopen;
- Vorderingen;
- Geldmiddelen.

Een andere vorm van functievermenging is, dat gebruikers geautoriseerd zijn voor het onderhouden van masterdata en daarbij ook geautoriseerd zijn voor het uitvoeren van transacties met deze masterdata. Er dient ook functiescheiding te zijn met betrekking tot systeembeheeractiviteiten en het uitvoeren van wijzigingen in operationele gegevens en processen in de informatiesystemen. Ook dient er binnen het autorisatiebeheer sprake te zijn van functiescheiding tussen het koppelen van autorisaties en het beheer van gebruikers-ID's (zie hoofdstuk 2.4).

Verder is functievermenging afhankelijk van de organisatie en zal er voor elke organisatie specifiek moeten worden nagegaan in welke gevallen er sprake is van functievermenging. De voornaamste factoren hierbij zijn de grootte van de organisatie en het soort bedrijfsprocessen. Op basis hiervan zou moeten worden bepaald welke combinaties van autorisaties functievermenging veroorzaken.

Elke vorm functievermenging die naar boven komt bij de controle van de autorisaties dient te worden besproken met de verantwoordelijke functionarissen binnen de organisatie. Functievermenging zal moeten worden opgelost indien de risico's hiervan groot zijn. Hiervoor zullen autorisaties verwijderd moeten worden voor één van de activiteiten die de functievermenging veroorzaakt. Als dit niet gebeurt dan dient hiervoor akkoord te worden gegeven vanuit meerdere functionarissen op management niveau uit de eindgebruikersorganisatie. Er zullen dan compenserende maatregelen aanwezig moeten zijn, die de risico's van de functievermenging opheffen.

3. SAP R/3 autorisatieconcept

3.1. Opbouw SAP R/3 autorisatieconcept

SAP R/3 is een ERP systeem en bevat functionaliteiten ter ondersteuning van bijna alle bedrijfsprocessen. Functionaliteit ter ondersteuning van de volgende processen is binnen ieder SAP R/3 systeem standaard aanwezig:

- Financial accounting (onder andere boekhouding, debiteuren-/crediteuren administratie);
- Controlling;
- Inkoop;
- Logistiek;
- Verkoop;
- Project management;
- Human Recources.

Het is niet zo dat organisaties die SAP R/3 gebruiken, alle functionaliteiten bij deze processen hoeven te gebruiken. Verder is het mogelijk dat er extra bedrijfstakspecifieke SAP R/3 oplossingen worden geïnstalleerd.

Om functionaliteit binnen SAP R/3 uit te voeren start de gebruiker een transactie op en/of voert de gebruiker een programma uit. Uiteindelijk voert de gebruiker altijd een programma uit, want achter elke transactiecode zitten één of meerdere programma's. Elke transactie is gekoppeld aan een unieke transactiecode. Een SAP R/3 systeem bestaat standaard uit tienduizenden transactiecodes en honderdduizenden programma's. Het is ook mogelijk om binnen een SAP R/3 systeem nieuwe (maatwerk)programma's en (maatwerk)transacties te ontwikkelen. Ontwikkelaars dienen hierbij altijd rekening te houden met de naamgevingconventie. Dit is onder meer van belang om de nieuwe programma's en transacties herkenbaar te houden. Binnen SAP R/3 zijn de beginletters Y en Z vrijgehouden voor de technische naam van zelf ontwikkelde programma's en transacties.

Het SAP R/3 autorisatieconcept biedt bescherming tegen onbevoegde toegang. De gebruikers kunnen slechts de transacties en programma's gebruiken die uitdrukkelijk voor hen zijn toegestaan. De Profiel Generator en het Autorisatie Infosysteem zijn beschikbaar als hulpmiddel binnen SAP R/3 bij het werken met het autorisatieconcept. De Profiel Generator verstrekt een top-down benadering van de toewijzing van autorisaties. Het Autorisatie Infosysteem biedt een gemakkelijk toegankelijk overzicht over de autorisaties.

Om het autorisatieconcept binnen SAP R/3 af te dwingen worden autorisatiecontroles uitgevoerd wanneer de gebruikers proberen om programma's of transacties uit te voeren. In de autorisatiecontroles wordt geverifieerd of de autorisaties aan het gebruikers-ID gekoppeld zijn, alvorens de gebruiker toe te staan om de betreffende transactie of het programma verder uit te voeren. Er zijn diverse soorten autorisatiecontroles binnen SAP R/3, namelijk:

- Transactiestart autorisatie; De gebruiker moet de aangewezen autorisaties hebben om transacties op te starten. Dit is op transacties van toepassing die vanaf het menu kunnen worden opgestart of vanuit het commandoveld. Deze autorisatiecontrole vindt standaard bij elke transactie plaats. De controle hierbij vindt plaats op de transactiecode. De controle vindt ook plaats voor transacties die vanuit een programma of vanuit een andere transactie worden aangeroepen. Het is echter mogelijk om deze controle inactief te maken.
- Specifieke autorisatie voor een transactie; Naast de autorisatiecontrole bij de transactiestart zijn de transacties beschermd met extra autorisatiecontroles naast de controle op transactiecode. Dit vindt plaats aan de hand van een autorisatie-object. Wanneer er nieuwe transacties worden gecreëerd kunnen ook aanvullende autorisatiecontroles worden toegewezen.

- Autorisatiecontrole op programmaniveau; Deze controle vindt plaats door middel van het commando AUTHORITY-CHECK in een programma. Hierbij vind er een controle plaats of de gebruiker geautoriseerd is om het programma verder uit te voeren. Het is sterk aan te bevelen om deze bescherming ook in nieuwe en gewijzigde programma's te gebruiken.
- Rapportklassen en Tabel autorisatiegroepen; Naast programma- of de transactie-autorisatiecontroles, kunnen rapporten aan rapportklassen en autorisatiegroepen aan tabellen worden toegewezen. Hoewel gebruikers de transacties kunnen gebruiken om rapporten of direct tabellen te benaderen, kunnen zij tot die rapporten en tabellen slechts toegang krijgen waarvoor zij de overeenkomstige autorisaties hebben.

Het SAP R/3 autorisatieconcept bestaat altijd uit de volgende componenten:

- Gebruikers-ID; Elke gebruiker die aanlogt op een SAP Systeem moet een gebruikers-ID hebben. Het gebruikers-ID bevat alle informatie betreffende de gebruiker inclusief de koppeling met de profielen. Een gebruiker kan de activiteiten uitvoeren die in de autorisaties in het profiel zijn bepaald.
- Profielen; autorisaties in de gebruikers-ID's worden gekoppeld door middel van autorisatieprofielen.
- Autorisaties; Een autorisatie staat een gebruiker toe om een bepaalde activiteit in het SAP Systeem uit te voeren, dat op een reeks waarden wordt gebaseerd, die op basis van het autorisatie-object worden bepaald. Elke autorisatie verwijst naar precies één autorisatie-object en bepaalt de toegelaten waarden voor elk autorisatie-objectveld van dit object.
- Autorisatie-objecten; Dit is een template die gebruikt wordt om autorisaties te bepalen. De autorisaties worden opgebouwd op basis van deze objecten. Bijvoorbeeld het autorisatieobject F_AVIK_BUK (Betalingsadvies: autorisatie voor bedrijfcodes) wordt gebruikt om diverse autorisaties in Financiële Boekhouding zoals algemene Financiële weergave autorisaties, debiteuren- en crediteuren-autorisaties tot stand te brengen. Het is mogelijk om voor bepaalde transacties te bepalen dat een autorisatiecontrole op een autorisatie-object inactief is en dus niet wordt uitgevoerd bij het doorlopen van de transactie. Ook het mogelijk voor objecten te bepalen, dat de autorisatiecontrole helemaal niet plaatsvindt bij het uitvoeren van alle programma's en transacties.
- Autorisatie-objectvelden; Het autorisatieobject bevat maximaal 10 autorisatie-objectvelden. Deze velden zijn verbonden met gegevenselementen die in de programma's staan vermeld. De toelaatbare waarden vormen een autorisatie. Wanneer een autorisatiecontrole plaatsvindt, verifieert het systeem de waarden waarvoor een gebruiker is geautoriseerd, tegen de waarden die worden vereist om de actie uit te voeren. De gebruiker kan de actie slechts uitvoeren als hij of zij aan de voorwaarden voor elk veld in het object voldoet. De meeste autorisatie-objectvelden komen in meerdere autorisatie-objecten voor. Het meest gebruikte autorisatie-objectveld is het veld ACTVT (activiteit). De waarden in dit veld bepalen welke activiteiten er binnen deze autorisatie mogen worden uitgevoerd. Een veld kan ook een asterisk (*) als waarde bevatten. Dit betekent dat alle waarden (bijvoorbeeld alle activiteiten) worden toegestaan. Ook zijn er diverse velden aanwezig die een organisatorische eenheid vertegenwoordigen,zoals het veld bedrijfscode of magazijn. Hiermee wordt bepaald voor welke organisatorische eenheden men is geautoriseerd.

SAP R/3 hanteert het principe van accumulatie van toegangsrechten. Dit betekent dat bij het optellen van autorisaties in het gebruikers-ID de maximaal mogelijke toegang wordt verleend op basis van het totaal aan autorisaties. Er wordt door het SAP R/3 systeem aan een gebruiker toegang verleend, als de gebruiker alle velden met de betreffende veldwaarden heeft toegekend. Dit wordt per autorisatie-object bepaald.

Hieronder staan twee voorbeelden vermeld van een autorisatiecontrole op bedrijfscode bij het creëren van een materiaal.

Commando AUTHORITY-CHECK in programma op object M_MATE_BUK op de velden:
- **Activiteit 01 voor creëren**
- **Bedrijfscode 1000**

1
Gebruiker heeft de volgende autorisaties voor het autorisatie-object M_MATE_BUK toegewezen vanuit de gekoppelde profielen:
Autorisatie A
- *Activiteit 01 voor creëren + 02 voor wijzigen*
- *Bedrijfscode 1000*

Autorisatie B
- *Activiteit 01 voor creëren*
- *Bedrijfscode 2000*

Autorisatie wordt verleend op basis van Autorisatie A.

2
Gebruiker heeft de volgende autorisaties voor het autorisatie-object M_MATE_BUK toegewezen vanuit de gekoppelde profielen:
Autorisatie A
- *Activiteit 02 voor wijzigen*
- *Bedrijfscode 1000*

Autorisatie B
- *Activiteit 01 voor creëren*
- *Bedrijfscode 2000*

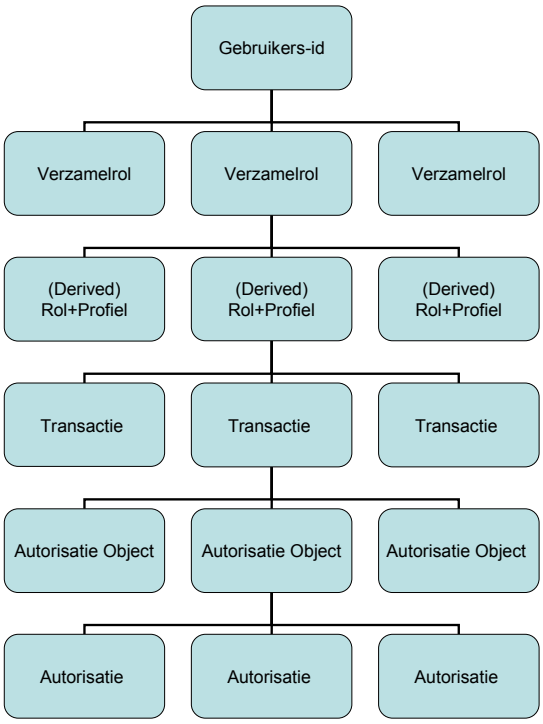
Autorisatie wordt NIET verleend.

Het SAP R/3 autorisatieconcept is zeer complex, omdat het bestaat uit vele componenten die met elkaar verbonden zijn. Er is daarbij ook sprake van zeer grote aantallen componenten. Binnen een standaard SAP R/3 systeem zijn bijvoorbeeld de volgende voor autorisaties relevante componenten aanwezig:
- Meer dan 50.000 transacties;
- Meer dan 700.000 programma's;
- Meer dan 1000 autorisatie-objecten.

Het SAP R/3 autorisatieconcept vanaf SAP R/3 versie 4.6C is opgebouwd aan de hand van Role Based Access. Rollen bevatten een profiel met de autorisaties en deze rollen worden gekoppeld aan gebruikers-ID´s. In voorgaande versies werd er in plaats van rollen gebruik gemaakt van ´Activity groups´. Aangezien momenteel bijna alle operationele SAP R/3 systemen versie 4.6C of hoger zijn en de operationele systemen van eerdere versies binnen afzienbare tijd geüpgrade zullen worden, zal in onderstaande paragrafen het principe van Role Based Access binnen SAP R-/3 worden uitgewerkt en zal er niet verder worden ingegaan op ´Activity groups´.

3.2. Role Based access

Het SAP R/3 Role Based autorisatieconcept is opgebouwd uit verschillende lagen. In het figuur hieronder is de opbouw weergegeven.



Dit figuur gaat er vanuit dat alle onderdelen binnen het autorisatieconcept worden gebruikt. Dit wordt aanbevolen door SAP en binnen de meeste SAP R/3 systemen is dit het geval. Er kunnen echter ook bepaalde lagen worden weggelaten. Een aantal van deze onderdelen zijn in de voorgaande paragraaf al beschreven. Hieronder zal met name in worden gegaan op de relaties tussen deze onderdelen in het Role Based autorisatieconcept binnen SAP R/3.

3.2.1. Gebruikers-ID

Het hoogste niveau is het gebruikers-ID waarmee de gebruiker aanlogt in SAP R/3. Hieraan is het totaal aan autorisaties gekoppeld. Een gebruikers-ID kan worden geblokkeerd zodat de gebruiker er niet meer mee aan kan loggen op het systeem. Dit kan handmatig plaatsvinden maar ook automatisch, na een aantal aanlog-pogingen waarbij het verkeerde wachtwoord is gebruikt. Verder is het mogelijk om voor een gebruikers-ID een geldigheidstermijn op te geven. Buiten deze geldigheidstermijn kan er niet met het gebruikers-ID worden aangelogd.

3.2.2. Verzamelrollen

Aan het gebruikers-ID kunnen één of meerdere verzamelrollen zijn gekoppeld. Aan een verzamelrol zijn één of meerdere rollen gekoppeld. De rollen kunnen echter ook direct aan het gebruikers-ID worden gekoppeld. Voor verzamelrollen is het mogelijk om een geldigheidstermijn op te geven bij de koppeling aan het gebruikers-ID. Deze is dan ook van toepassing op alle rollen die door middel van de verzamelrol aan het gebruikers-ID zijn gekoppeld.

3.2.3. Rollen en profielen

Een rol is meestal aan een profiel gekoppeld aangezien het profiel uiteindelijk de autorisaties bevat. Als een rol aan een profiel gekoppeld is, dan zijn uiteindelijk zowel het profiel als de rol aan het user-id gekoppeld, al dan niet vanuit een verzamelrol. De verzamelrol bevat echter alleen de rol. Ook is er nog de mogelijkheid om direct rollen en/of profielen aan een gebruikers-ID te koppelen. Ook voor rollen is het mogelijk om een geldigheidstermijn op te geven bij de koppeling aan het gebruikers-ID.

Verder kan er nog gebruik gemaakt worden van ‘derived’ rollen met bijbehorende profielen. Dit zijn rollen en profielen die afgeleid zijn van andere rollen en profielen. Het onderscheid zit hierbij in bepaalde organisatorische autorisaties.

3.2.4. Transacties

Aan een rol en profiel zijn meestal transacties gekoppeld. In de rol staan de transacties in het rolmenu vermeld. In het profiel staan de transacties vermeld in het S_TCODE autorisatie-object.

3.2.5. Autorisatie-objecten

Aan het profiel zijn de autorisatie-objecten gekoppeld met de daarbij behorende velden. Meestal zijn dit de objecten die gecontroleerd worden bij het uitvoeren van de transacties in het S_TCODE autorisatie-object.

3.2.6. Autorisaties

Het laagste niveau zijn de autorisaties. Deze zijn gekoppeld aan een autorisatie-object. De autorisaties bevatten de veldwaarden waarvoor autorisatie wordt verleend. Meestal zijn dit de autorisatie-objecten met bijbehorende velden en veldwaarden die gecontroleerd worden bij het uitvoeren van de transacties in het S_TCODE autorisatie-object, waarvoor de betreffende gebruiker geautoriseerd moet zijn. Wanneer transacties worden opgevoerd in het rolmenu zullen de bijbehorende autorisaties namelijk in veel gevallen automatisch worden ingevuld.

3.3. SAP R/3 autorisatieconcept toegepast

Doordat er sprake is van een groot aantal componenten binnen autorisaties in SAP R/3, die al dan niet met elkaar zijn gekoppeld, is het van groot belang dat de autorisaties gestructureerd zijn opgebouwd. Dit om het autorisatieconcept beheersbaar te houden. Het autorisatieconcept dient transparant te zijn, zodat het te doorgronden is voor alle betrokkenen. Om te beginnen is een duidelijke naamgevingconventie hierbij van groot belang. Op basis hiervan zou het mogelijk moeten zijn om af te leiden op welke functionaliteiten en/of gebieden de componenten betrekking hebben.

Daarnaast is het belangrijk transacties met bijbehorende autorisaties te structureren. Een goede methode hiervoor is het hanteren van een functie-taak structuur. Transacties met de bijbehorende autorisaties die altijd in combinatie met elkaar kunnen worden uitgevoerd worden gegroepeerd in een taak. De functie is dan een combinatie van een aantal taken. Dit kan dan in de vorm van een verzamelrol. De basis voor de inrichting van het autorisatieconcept is dan meestal een functie-taken matrix.

Een ander aandachtspunt bij de toepassing van het autorisatieconcept is, dat wanneer er meerdere verzamelrollen zijn gekoppeld, de doorzichtigheid van het autorisatieconcept afneemt. Dit doordat er aan elke verzamelrol meerdere losse rollen gekoppeld kunnen zijn.

3.4. Kritische autorisatie aspecten binnen SAP R/3

SAP R/3 bevat diverse autorisatie-aspecten die grote risico's kunnen opleveren op diverse gebieden, zoals de continuïteit van het bedrijfsproces en de juistheid van de jaarrekening. Deze risico's zijn altijd afhankelijk van het systeem. De aspecten zullen dus sterk per systeem verschillen. Er zijn echter een aantal aspecten die in alle systemen kritisch zijn, namelijk:

- Kritische SAP R/3 standaard autorisatieprofielen;
- Kritische autorisatie-objecten;
- Kritische transacties;
- Systeemparameters;
- Check Indicator;
- User Comparison;
- Systeemlandschap.

3.4.1. Kritische SAP R/3 standaard autorisatieprofielen

Binnen SAP R/3 zijn standaard autorisatieprofielen aanwezig die ook rechtstreeks toegewezen kunnen worden aan gebruikers. De volgende standaard profielen zijn het meest kritisch:

- SAP_ALL; Dit samengestelde profiel bevat alle SAP R/3 autorisaties. Een gebruiker met dit profiel kan alle functionaliteit in het SAP-systeem uitvoeren.
- SAP_NEW; Dit samengestelde profiel bevat de nieuwe autorisatie-objecten met alle bijbehorende autorisaties van de geïnstalleerde SAP R/3 versie. Deze rol kan gebruikt worden om gebruikers te autoriseren voor alle nieuwe autorisatie-objecten die er na een SAP R/3 versie upgrade zijn bijgekomen.

Andere zeer kritische standaard autorisatieprofielen staan vermeld in bijlage 2.

3.4.2. Kritische autorisatie-objecten

De volgende autorisatieobjecten zijn het meest kritisch binnen een SAP R/3 systeem:

- S_TCODE; hiermee wordt de autorisatie op transacties bepaald (transactiestart-autorisatie).
- S_TABU_DIS; hiermee wordt de autorisatie op autorisatiegroepen voor tabellen bepaald. Dit voorkomt dat gebruikers toegang hebben tot tabellen, gebruik makend van algemene toegangshulpmiddelen (bijvoorbeeld transactie SE16). Een gebruiker moet niet alleen de autorisatie hebben om het hulpmiddel in werking te stellen, maar hij of zij moet ook de autorisatie hebben voor de tabellen met de overeenkomstige autorisatiegroep. Hierbij kan tevens worden bepaald welke activiteit(en) uitgevoerd mogen worden (wijzigen/weergeven tabel). Bij de autorisatie op dit object is het van groot belang dat alle tabellen met gevoelige gegevens zijn toegewezen aan een specifieke autorisatiegroep.
- S_BTCH_ADM; hiermee wordt de autorisatie bepaald voor het beheer van programma's die op de achtergrond worden uitgevoerd.
- S_IMG_ACT; hiermee wordt de autorisatie bepaald voor de toegang tot Customizing. Hier worden alle functionele systeeminstellingen bepaald. Dit betreft bijvoorbeeld de schermopbouw en transactie afhandeling. Ook worden de meest kritische masterdata in Customizing beheerd zoals bedrijfscodes.

In bijlage 2 staan andere zeer kritische autorisatieobjecten vermeld.

3.4.3. Kritische transacties

Binnen SAP R/3 bestaan een groot aantal transacties die als kritisch kunnen worden gedefinieerd. Dit is afhankelijk van het proces en deze verschillen per organisatie. De meest kritische transacties die direct invloed kunnen hebben op bedrijfsprocessen en daarmee altijd als zeer kritisch worden beschouwd zijn de volgende:

- Transactiecode SA38; hiermee kunnen direct programma's worden opgestart zonder dat er een controle op transactiecode plaatsvindt;
- Transactiecode SE38; ook hiermee kunnen direct programma's worden opgestart zonder dat er een controle op transactiecode plaatsvindt. Daarnaast is het binnen deze transactie mogelijk om de programmacode te bekijken. En als er aan een aantal voorwaarden is voldaan (onder andere autorisatie voor wijzigen programmacode) de programmacode te wijzigen;
- De transactiecodes SE16/SE17/SM30/SM31; hiermee is het mogelijk om direct tabellen te benaderen en wijzigingen door te voeren;
- Transactiecode SM01; hiermee kunnen transacties worden ge(de)blokkeerd voor alle gebruikers;

Andere transacties die binnen ieder SAP R/3 systeem als kritisch worden beschouwd staan vermeld in bijlage 2.

3.4.4. Systeemparameters

Vooral de volgende systeemparameters hebben invloed op autorisaties binnen SAP R/3:

- auth/no_check_in_some_cases; hiermee wordt bepaald of autorisatiecontroles op autorisatie-objecten die gedeactiveerd zijn voor transacties worden overgeslagen. Indien deze parameter de waarde 'Y' bevat dan worden de controles overgeslagen. Indien deze parameter de waarde 'N' bevat dan worden de controles niet overgeslagen.
- auth/object_disabling_active; hiermee wordt bepaald, dat voor autorisatie-objecten waarvoor in te stellen is dat de autorisatiecontrole voor deze objecten helemaal niet plaatsvindt bij het uitvoeren van alle programma's en transacties, de autorisatiecontrole wel of niet plaatsvindt. Indien deze parameter de waarde 'Y' bevat dan worden de controles overgeslagen. Indien deze parameter de waarde 'N' bevat dan worden de controles niet overgeslagen.
- auth/no_check_on_tcode; hiermee kan worden bepaald dat de controle op het autorisatie-object S_TCODE altijd wordt overgeslagen. Indien deze parameter de waarde 'Y' bevat wordt de controle voor autorisatie op transacties (transactiestart autorisatie) overgeslagen. Indien deze parameter de waarde 'N' bevat dan wordt de controle niet overgeslagen.

3.4.5. Check Indicator

Door middel van de Check Indicator kan voor transacties worden aangegeven welke autorisatie-objecten er worden gecontroleerd. Dit heeft verder geen invloed op de autorisatiecontrole aangezien de controle vanuit het programma plaatsvindt. Er kan echter wel worden bepaald dat de controle op bepaalde autorisatie-objecten binnen een bepaalde transactie wordt overgeslagen, wanneer het programma door middel van deze transactie wordt uitgevoerd. Dit is echter niet mogelijk bij objecten ten aanzien van systeembeheer (beginnend met de letter 'S').

3.4.6. User Comparison

De User Comparison functie in SAP R/3 verifieert of de rollen, die aan een gebruikers-ID zijn toegewezen door middel van een verzamelrol, overeenkomen met de rollen die daadwerkelijk aan de verzamelrol zijn gekoppeld. Het kan bijvoorbeeld zo zijn dat er een rol uit een verzamelrol is verwijderd. In dat geval moet de User Comparison functie worden uitgevoerd, om deze rol te verwijderen bij alle gebruikers-ID's die deze verzamelrol hebben gekoppeld.

3.4.7. Systeemlandschap

SAP R/3 biedt de mogelijkheid om een systeemlandschap op te bouwen waardoor ontwikkeling, test, acceptatie en productie op verschillende systemen plaats kan vinden. Daarbij is het ook mogelijk om de systemen onder te verdelen naar clients. Dit is een deelomgeving op een systeem dat een specifieke rol vervult. Een ontwikkel- en een testomgeving kunnen bijvoorbeeld op één systeem aanwezig zijn, maar elk op een eigen client.

3.5. Autorisatie hulpmiddelen binnen SAP R/3

Gezien de complexiteit van het autorisatieconcept binnen SAP R/3 is het aan te bevelen om hulpmiddelen te gebruiken bij het autorisatiebeheer en de controle op de autorisatie-inrichting. Er kan gebruik gemaakt worden van autorisatie-tools buiten SAP. SAP R/3 biedt standaard hulpmiddelen voor het beheer en de controle van autorisaties, namelijk de Profielgenerator en het Autorisatie Infosysteem.

3.5.1. Profielgenerator

De profielgenerator maakt het beheren van autorisaties gemakkelijker, door bepaalde processen te automatiseren en meer flexibiliteit in autorisatietaken te verstrekken. Het voordeel van de profielgenerator is dat er technische aspecten van autorisaties en autorisatie-objecten automatisch worden gegenereerd. Het model van de opbouw dat wordt gehanteerd voor rollen en profielen is flexibel. De profielgenerator maakt het mogelijk (vanaf SAP R/3 versie 4.6C) om het autorisatieconcept op te bouwen door middel van functierollen en/of taakrollen. Hierbij kan gebruik worden gemaakt van losse rollen en van verzamelrollen. De profielgenerator gebruikt een top-down benadering voor het produceren van autorisaties. Het begint met de opbouw van een rolmenu met transacties en werkt omlaag tot aan de koppeling met individuele gebruikers-ID's. De profielgenerator is beschikbaar vanaf SAP R/3 versie 3.1G en loopt op alle gesteunde platformen.

3.5.2. Autorisatie Infosysteem

Ook het Autorisatie Infosysteem is beschikbaar vanaf SAP R/3 versie 3.1G. Het kan gebruikt worden om snel en gemakkelijk een overzicht van autorisaties, profielen, gebruikers en rollen te verkrijgen. Het biedt mogelijkheden om lijsten te maken met de volgende gegevens:

- Gebruikers, rollen en profielen met bepaalde autorisaties;
- Autorisaties die een bepaalde gebruiker, rol of profiel heeft;
- Alle autorisaties;
- Vergelijkingen van autorisaties van gebruikers, rollen en profielen;
- Transacties die een gebruiker, rol of profiel kan uitvoeren;
- Wijzigingen in gebruikers-ID's, rollen en profielen.

4. Toepassing auditaspecten binnen autorisaties in SAP R/3

4.1. Auditaspecten binnen autorisaties in SAP R/3

Voordat er een audit kan worden uitgevoerd van autorisaties in een SAP R/3 systeem zal er een auditplan gemaakt moeten worden. Ook dient er een normenkader te worden bepaald. Het normenkader en het auditplan dienen te worden afgestemd met de opdrachtverstrekker van de audit. In het normenkader zullen normen moeten worden bepaald voor alle relevante aspecten van autorisaties in een SAP R/3 systeem. Deze aspecten zijn vaak afhankelijk van het systeem en de organisatie waarop de audit wordt uitgevoerd. Ook zijn deze aspecten in bepaalde gevallen van extra groot belang. Er zijn een aantal aspecten altijd in bepaalde mate van belang, namelijk:

1. Aanwezigheid van autorisatiebeleid;
2. Autorisatie inrichting;
3. Autorisatieprocessen;
4. Kritische autorisaties in SAP R/3.

4.1.1. Aanwezigheid van autorisatiebeleid

Er dient een autorisatiebeleid aanwezig te zijn waarin de volgende zaken zijn opgenomen:

- Doel van het autorisatiebeleid;
- Richtlijnen waaraan iedereen zich dient te houden;
- Taken en verantwoordelijkheden binnen de processen die van toepassing zijn bij het beheer van autorisaties in SAP R/3. Hierbij dient ook de koppeling naar andere processen binnen de organisatie te zijn beschreven.

Het autorisatiebeleid dient goedgekeurd te zijn door de directie en vertegenwoordigers op managementniveau vanuit zowel de IT afdeling(en) als business afdelingen.

4.1.2. Autorisatie inrichting

De volgende aspecten zijn het meest belangrijk bij de autorisatie-inrichting in SAP R/3:

- Geen ontwikkelingsactiviteiten op productie omgevingen.
- Scheiding van soorten gebruikers en autorisaties op verschillende omgevingen.
- Indien er gebruikers-ID's bestaan die alle autorisaties (bijvoorbeeld profiel SAP_ALL) hebben, dienen hiervoor randvoorwaarden te zijn beschreven. Er dient gespecificeerd te zijn welke gebruikers-ID's het betreft en op welke systemen dit van toepassing is. Hierbij dient ook altijd de reden te worden vermeld waarom de betreffende gebruikers-ID's alle autorisaties hebben en wat hier de risico's met bijbehorende compenserende maatregelen zijn.
- Er dient een heldere naamgevingconventie te zijn voor alle componenten binnen het SAP R/3 autorisatieconcept. Hierbij dient in de naamgevingconventie duidelijk te zijn welke componenten niet standaard in het SAP R/3 systeem aanwezig zijn.
- Het autorisatieconcept dient te zijn gedocumenteerd. Deze documentatie dient volledig en up-to-date te zijn. Hierin dienen minimaal de volgende zaken te zijn vermeld:
    - De soorten autorisaties die worden gebruikt;
    - De autorisatiestructuur:
        - autorisatie hiërarchieën;
        - het automatisch 'erven' van autorisaties;
    - De naamgevingconventies binnen autorisaties;
    - Rekening houden met functiescheiding binnen autorisaties;
    - Uitzonderingen op de autorisatieopbouw en specifieke oplossingen.
- Van iedere gebruiker dient de naam bekend te zijn zodat zij geïdentificeerd kunnen worden.

- De User Comparison functie in SAP R/3 dient minimaal één maal per etmaal te worden uitgevoerd.
- De SAP R/3 systeemparameter ‘auth/no_check_on_tcode’ dient de waarde ‘N’ te bevatten zodat autorisatiecontroles op de transactiestart autorisatie niet worden overgeslagen.

Verder dient er bij de inrichting van autorisaties rekening te zijn gehouden met functievermenging. Het mag niet mogelijk zijn dat personen geautoriseerd zijn voor een combinatie van processen en/of gegevens die het mogelijk maken om fraude te plegen. Er kan een onderscheid worden gemaakt tussen verschillende vormen van functievermenging binnen of tussen de informatiesystemen. Indien er sprake is van andere informatiesystemen buiten het SAP R/3 systeem waarop de audit wordt uitgevoerd dient hier rekening mee gehouden te worden. Er dient te worden onderzocht of het mogelijk is dat autorisaties op het SAP R/3 systeem functievermenging zou kunnen veroorzaken samen met autorisaties op een ander systeem. De volgende aspecten zijn in het kader van functievermenging van belang:

- Gebruikers mogen niet zijn geautoriseerd voor meerdere processen in de fasen van de waardenkringloop.
- Gebruikers mogen niet geautoriseerd zijn voor het onderhouden van masterdata en daarbij ook geautoriseerd zijn voor het uitvoeren van transacties met deze masterdata.
- Er dient functiescheiding te zijn met betrekking tot systeembeheeractiviteiten en het uitvoeren van wijzigingen in operationele gegevens en processen in de informatiesystemen.
- Binnen het autorisatiebeheer dient er sprake te zijn van functiescheiding tussen het beheer van gebruikers-ID’s en de koppeling van autorisaties aan gebruikers-ID’s.

Of er sprake is van functievermenging dat is verder afhankelijk van de organisatie. Er zal daarom voor iedere organisatie specifiek moeten worden nagegaan in welke gevallen er sprake is van functievermenging. Er moet worden bepaald welke combinaties van functionaliteiten functievermenging veroorzaken. Op basis hiervan zou moeten worden bepaald welke combinaties van autorisaties in SAP R/3 functievermenging veroorzaken. Hierbij moet worden bepaald welke transacties of programma’s en welke onderliggende autorisaties worden gecontroleerd.

4.1.3. Autorisatieprocessen

De volgende aspecten zijn van groot belang bij de processen die van invloed zijn op autorisaties in SAP R/3:

- Een combinatie van controlerende en uitvoerende verantwoordelijkheden dient niet bij één persoon te worden belegd in verband met controletechnische functiescheiding.
- De uitvoerende processen binnen het autorisatiebeheer moeten indien mogelijk worden onderverdeeld naar het beheer van gebruikers-ID’s, de koppeling van autorisaties aan gebruikers-ID’s en het beheer van de rollen/profielen in SAP R/3.
- Het incidenten en wijzigingsproces met betrekking tot autorisaties dient voldoende waarborgen te bieden. De volgende zaken dienen minimaal in deze processen te zijn opgenomen:
    - Elke wijziging dient te worden gevalideerd door daartoe bevoegde personen;
    - Incidenten met betrekking tot autorisaties dienen te worden vastgelegd en te worden geanalyseerd.
- Alle functionarissen die zich bezighouden met het autorisatiebeheer zouden gescreend moeten zijn voordat zij deze activiteiten mogen gaan uitvoeren.
- Aanvragen voor gebruikers-ID’s en autorisatie wijzigingsverzoeken dienen vooraf goedgekeurd te worden door een functionaris die hiervoor bevoegd is. Het mag niet mogelijk zijn dat gebruikers hun eigen aanvragen goedkeuren.
- Er dient handtekeningverificatie plaats te vinden van autorisatie-aanvragen die door middel van een formulier voorzien van een handtekening worden ingediend.
- Autorisatie-aanvragen dienen te worden gearchiveerd.
- Aanvrager mag niet alleen aangeven dat een gebruiker dezelfde autorisaties moet hebben als een andere gebruiker.

- Rollen die op tijdelijke basis extra worden toegevoegd aan gebruikers-ID's dienen te worden voorzien van een einddatum.
- Gebruikers-ID's van tijdelijke medewerkers dienen te worden voorzien van een einddatum.
- Gebruikers-ID's dienen te worden verwijderd wanneer deze niet meer mogen worden gebruikt. Verder dienen gebruikers-ID's te worden geblokkeerd indien deze tijdelijk niet worden gebruikt.
- Alle wijzigingen in de koppeling van rollen en profielen aan gebruikers-ID's en de wijzigingen binnen de rollen/profielen dienen te worden gelogd. In deze logging dienen in ieder geval de volgende zaken vermeld te zijn:
    - Welke autorisaties toegewezen of verwijderd zijn bij welk gebruikers-ID of in welke rol/profiel;
    - De naam of het gebruikers-ID van de functionaris die de wijziging heeft doorgevoerd;
    - De datum van de wijziging.
- Er dienen duidelijke werkinstructies aanwezig te zijn voor de processen binnen autorisatiebeheer.
- Bij de bepaling van autorisaties dienen naast de IT afdeling ook andere afdelingen in de organisatie te worden betrokken. Voor gegevens en processen dienen eigenaren te zijn aangewezen die bij de bepaling en wijziging van autorisaties worden betrokken.
- Indien er sprake is van meerdere systemen dan dienen autorisatiestructuren, indien mogelijk, op elkaar aan te sluiten zodat bij gelijksoortige systemen dezelfde autorisatiestructuur wordt gehanteerd. Ook dient er hierbij rekening te worden gehouden met autorisaties over de systemen heen. Denk hierbij in het bijzonder ook aan functiescheiding tussen de diverse systemen.
- Autorisatiewijzigingen dienen vooraf te worden gecontroleerd op functiescheiding en kritische functionaliteit.
- Wijzigingen in rollen/profielen dienen te worden getest op een test- en/of acceptatiesysteem.
- Er dienen periodiek controles plaats te vinden op de toewijzing van autorisaties. Het is aan te bevelen om alle toegewezen autorisaties aan gebruikers-ID's minimaal één maal per 6 maanden te controleren. De volgende aspecten zijn hierbij belangrijk:
    - Gebruikers-ID's die (bijna) alle autorisaties hebben toegewezen binnen informatiesystemen dienen minimaals maandelijks te worden gecontroleerd. Ook dient er logging plaats te vinden van de activiteiten van deze gebruikers op de informatiesystemen;
    - Autorisaties binnen de meest kritische functionaliteit dienen minimaal één maal per 3 maanden te worden gecontroleerd;
    - Er dient minimaal één maal per 3 maanden te worden gecontroleerd of er sprake is van functievermenging binnen of tussen de informatiesystemen.

4.1.4. Kritische autorisaties in SAP R/3

Voordat een audit naar autorisaties in SAP R/3 kan worden uitgevoerd zal moeten worden bepaald welke functionaliteit als kritisch wordt beschouwd binnen de betreffende organisatie. Dit betreft verschillende soorten systeemfunctionaliteit in SAP R/3:

- Functionaliteiten binnen als kritisch geclassificeerde bedrijfsprocessen;
    - Processen die directe of indirecte invloed hebben op financiële rapportages;
    - Processen die als kritisch zijn gedefinieerd in verband met wetgeving (bijvoorbeeld Sarbanes-Oxley Section 404 en Wet Bescherming Persoonsgegevens);
    - Alle overige processen die door de organisatie als kritisch zijn geclassificeerd.
- Systeembeheer en -ontwikkeling.
- (Master)datamanagement.
- Automatische processen waarvoor gebruikers geen autorisatie mogen hebben.
- Weergeven en onderhouden van tabellen+query's.
- Functionaliteiten om direct programma's op te starten zonder dat er een controle op transactiecode plaatsvindt

Bij deze functionaliteiten zullen vervolgens de betreffende autorisaties in SAP R/3 moeten worden bepaald. Hierbij moet worden bepaald welke transacties of programma's en welke onderliggende autorisaties hierbij worden gecontroleerd. Hierbij dient rekening te worden gehouden met de mogelijkheid om voor transacties te bepalen, dat een autorisatiecontrole op een autorisatie-object inactief is en dus niet wordt uitgevoerd. Ook dient er rekening te worden gehouden met de mogelijkheid dat de transactiestart autorisatiecontrole is uitgeschakeld.

De volgende aspecten zijn verder van belang bij de toewijzing van autorisaties voor kritische functionaliteit:

- Functionaliteit in een SAP R/3 systeem dient te zijn geclassificeerd. De classificatie bepaald in welke mate bepaalde functionaliteit kritisch is.
- Alleen gekwalificeerde functionarissen mogen autorisaties voor kritische functionaliteit waarvoor zij zijn gekwalificeerd.
- Autorisaties voor kritische functionaliteit dient altijd aan een zo beperkt mogelijke groep gebruikers te zijn toegewezen waarbij deze functionaliteit onmisbaar is bij de uitoefening van hun functie.
- Er dienen extra autorisatiecontroles aanwezig te zijn in maatwerktransacties en programma's met functionaliteit die als kritisch is geclassificeerd.
- De standaard SAP profielen SAP_ALL en SAP_NEW dienen niet te zijn toegewezen aan gebruikers.

4.2. Samenvatting belangrijkste auditaspecten

Alle aspecten eerder in dit hoofdstuk beschreven, zijn meer of mindere mate van belang bij een audit naar autorisaties van een SAP R/3 systeem. Om aan te geven welke aspecten het meest essentieel zijn, zullen deze hieronder worden beschreven.

Doordat er sprake is van een groot aantal componenten binnen autorisaties in SAP R/3, die al dan niet met elkaar zijn gekoppeld, is het van groot belang dat de autorisaties gestructureerd zijn opgebouwd om het autorisatieconcept beheersbaar te houden. Het autorisatieconcept dient transparant te zijn zodat het te doorgronden is voor alle betrokkenen. Als dit niet het geval is dan zal dit de audit ook aanzienlijk bemoeilijken. Uiteindelijk gaat het er natuurlijk om welke autorisaties aan de gebruikers-ID's zijn toegewezen. Echter bij een SAP R/3 systeem, vaak met een groot aantal gebruikers, is het belangrijk dat de toewijzing en opbouw van autorisaties gestructureerd plaatsvindt. Anders is de kans zeer groot dat gebruikers verkeerde, meestal te ruime autorisaties krijgen toegewezen.

Een ander belangrijk aspect bij autorisaties in SAP R/3 is functievermenging. Dit is afhankelijk van de organisatie. Er zal voor elke organisatie specifiek moeten worden nagegaan in welke gevallen er sprake is van functievermenging. Er zal tijdens een audit in ieder geval aandacht moeten worden besteed aan een aantal aspecten. Vanuit AO/IC principes zouden gebruikers in ieder geval niet geautoriseerd mogen zijn voor meerdere processen in de fasen van de waardenkringloop. Verder mogen gebruikers niet geautoriseerd zijn voor het onderhouden van masterdata en daarbij ook geautoriseerd zijn voor het uitvoeren van transacties met deze masterdata. Er dient verder functiescheiding te bestaan, met betrekking tot systeembeheeractiviteiten en het uitvoeren van wijzigingen in operationele gegevens of processen in de informatiesystemen. Wanneer de organisatie aangeeft dat de functievermenging niet kan worden opgelost, dan dienen er compenserende maatregelen aanwezig te zijn, die de risico's die de functievermenging met zich meebrengen opheffen.

Verder dient er tijdens een audit naar autorisaties in SAP R/3 te worden bepaald, welke gebruikers toegang hebben tot bepaalde kritische functionaliteiten in het systeem. Ook dit verschilt per organisatie. Er zal moeten worden bepaald welke functionaliteit als kritisch wordt beschouwd binnen de betreffende organisatie. Hierbij is het van belang te bepalen of organisaties aan bepaalde wetten of externe regels moeten voldoen. Functionaliteiten ten behoeve van systeembeheer zijn altijd kritisch. Er dient dus te worden bepaald of deze wel aan de juiste gebruikers is toegewezen. Verder dient te worden nagegaan of gebruikers niet zijn geautoriseerd voor automatische processen, waarvoor gebruikers geen autorisatie mogen hebben. Dit geld ook voor functionaliteit om direct programma's op te starten zonder dat er een controle op transactiecode plaatsvindt. Ook functionaliteiten voor het direct weergeven en onderhouden van tabellen is kritisch, aangezien tabellen alle gegevens bevatten in een SAP R/3 systeem.

In ieder SAP R/3 systeem is het van groot belang dat de standaard aanwezige profielen SAP_ALL en SAP_NEW niet zijn toegewezen aan gebruikers, aangezien deze de autorisaties voor alle functionaliteit bevatten. Voordat de autorisatiecomponenten worden gecontroleerd dienen de volgende zaken te worden nagegaan, omdat deze hierbij van grote invloed zijn:

- Of er voldoende autorisatiecontroles aanwezig te zijn in maatwerktransacties en programma's met functionaliteit die als kritisch geclassificeerd is.
- Of er binnen de als kritisch gedefinieerde transacties autorisatie-objecten bestaan waarbij aan is gegeven dat deze niet worden gecontroleerd.
- De User Comparison functie in SAP R/3 dient minimaal één maal per etmaal te worden uitgevoerd.

Bij een audit naar autorisaties van een SAP R/3 systeem is het van belang dat ook de werking wordt gecontroleerd. Dit in het bijzonder bij maatwerktransacties.

Verder is het van groot belang dat de business is betrokken is bij het autorisatieproces. Vertegenwoordigers vanuit de business dienen daarom ook periodiek controles uit te voeren op autorisaties. Ook bij autorisatiewijzigingen die de bedrijfsprocessen raken dienen zij altijd goedkeuring te geven.

Het incidenten- en wijzigingsproces met betrekking tot autorisaties dient voldoende waarborgen te bieden. Elke wijziging dient te zijn gevalideerd door daartoe bevoegde personen. Verder dienen alle wijzigingen te zijn gelogd in het systeem, waarbij de datum van de wijziging en de persoon die de wijziging hebben doorgevoerd staan vermeld.

4.3. Samenhang met kwaliteitsaspecten

Autorisaties in een SAP R/3 systeem zijn van invloed op de kwaliteitsaspecten beschikbaarheid, vertrouwelijkheid, integriteit, effectiviteit en efficiency.

Met name autorisaties die betrekking hebben op systeembeheer, hebben invloed op het aspect beschikbaarheid, omdat hiermee het SAP R/3 systeem geheel of gedeeltelijk niet meer beschikbaar is. Dit betreffen systeeminstellingen en databasemanagement. Ook het autorisatie- en gebruikersbeheer zijn hierop van invloed, aangezien deze activiteiten kunnen veroorzaken dat gebruikers geen toegang meer hebben tot bepaalde functionaliteit of het gehele systeem.

Autorisaties in een SAP R/3 systeem zijn verder van invloed op vertrouwelijkheid van gegevens, aangezien er door middel van autorisaties bepaald wordt of gegevens wel of niet te wijzigen of weer te geven zijn voor gebruikers. Als gebruikers te ruime autorisaties hebben toegewezen, dan kan het zo zijn dat vertrouwelijke gegevens zichtbaar zijn voor personen die deze gegevens niet zouden mogen zien. De controleerbaarheid is hierbij van groot belang, aangezien dit bepaalt of verkeerd toegewezen autorisaties kunnen worden achterhaald. Het is dus belangrijk dat autorisaties gestructureerd zijn opgezet in een SAP R/3 systeem.

Ook zijn autorisaties in een SAP R/3 systeem van invloed op de integriteit van bedrijfsprocessen, -informatie en gegevensstromen. De autorisaties bepalen of gegevens te wijzigen zijn door gebruikers. Door de autorisaties van gebruikers te minimaliseren voor gegevens en processen die van invloed zijn op de integriteit, kan het risico op het onjuist doorvoeren van transacties en wijzigingen in het systeem zo veel mogelijk worden beperkt. De controleerbaarheid is ook hierbij van groot belang, aangezien dit bepaalt of verkeerd toegewezen autorisaties kunnen worden achterhaald.

Autorisaties in een SAP R/3 systeem zijn van invloed op de effectiviteit en efficiency van de bedrijfsvoering en gegevensverwerking in SAP R/3. Wat betreft effectiviteit is het van belang dat de daadwerkelijke autorisatietoewijzing in een SAP R/3 systeem overeenkomt met de doelstellingen in het organisatiebeleid met betrekking tot autorisaties. Aangezien SAP R/3 gecompliceerd is en daarmee het beheer, bestaat het risico dat de efficiency van de bedrijfsvoering negatief beïnvloed wordt. Mogelijk worden bedrijfsdoelstellingen niet behaald en worden te veel kosten gemaakt voor het beheer van autorisaties in een SAP R/3 systeem. Het autorisatieconcept dient daarom op een goed beheersbare manier te zijn opgezet.

De vertrouwelijkheid en integriteit zijn uiteindelijk de belangrijkste kwaliteitsaspecten waarop autorisaties in een SAP R/3 systeem van invloed zijn. Deze kwaliteitsaspecten betreffen de inrichting en toewijzing van autorisaties in het systeem. Als aan deze kwaliteitsaspecten is voldaan, dan zal er in de meeste gevallen ook aan de overige relevantie kwaliteitsaspecten zijn voldaan op autorisatiegebied. De vertrouwelijkheid en integriteit zullen vaak alleen gewaarborgd zijn, als de autorisaties op een effectieve en efficiënte wijze zijn ingericht en georganiseerd. Wanneer de vertrouwelijkheid en integriteit zijn gewaarborgd, dan heeft dit ook een positieve uitwerking op de beschikbaarheidaspecten waarop autorisaties van invloed zijn.

5. Conclusie

Bij een audit van autorisaties in een SAP R/3 systeem komen vele aspecten aan de orde. Er is geen standaard audit mogelijk, omdat veel aspecten afhankelijk zijn van de doelstelling van de audit, de organisatie en het systeem waarop de audit plaatsvindt. Er zijn echter wel een aantal aspecten altijd van belang en daar moet een auditor zich van bewust zijn. Voordat de auditor met het onderzoek begint moet er een goed beeld bestaan van de organisatie. De daarbij behorende aspecten moeten mee genomen worden in de audit. Wat betreft kwaliteitsaspecten zijn de vertrouwelijkheid en integriteit het meest relevant.

Uiteindelijk gaat het erom welke autorisaties gebruikers hebben toegewezen in een SAP R/3 systeem. Voor een juiste toewijzing van autorisaties zijn vele verschillende aspecten belangrijk. Dit betreft om te beginnen de processen rondom autorisatiebeheer. Deze dienen voldoende waarborgen te bieden. Niet alleen de IT afdeling, maar ook vertegenwoordigers vanuit de business dienen betrokken te zijn bij de bepaling van de autorisatie-inrichting. Voor een goede koppeling van autorisaties aan gebruikers is het van belang dat er een geschikt autorisatieconcept wordt gebruikt. Het autorisatieconcept dient transparant te zijn voor alle betrokkenen. Daarnaast dient het goed beheersbaar te zijn. Dit minimaliseert de kans op fouten in de toewijzing. Verder dient functievermenging te worden voorkomen in de inrichting en bij de toewijzing van autorisaties. En autorisatie voor kritische functionaliteit in een SAP R/3 systeem dient alleen aan gebruikers te zijn toegewezen die bekwaam zijn in deze functionaliteit en deze daadwerkelijk nodig hebben bij de uitoefening van hun functie.

Bij een audit van autorisaties is in veel gevallen de autorisatie-inrichting van belang. Daarom moet de auditor de autorisatiestructuur in SAP R/3 begrijpen. Ook moet de auditor weten wat de kritische aspecten zijn binnen de autorisatiestructuur in SAP R/3. Dit is noodzakelijk om tot een juist eindoordeel te komen. Er is verder sprake van een groot aantal componenten binnen autorisaties in een SAP R/3 systeem, die vaak met elkaar samenhangen en de uiteindelijke werking en toewijzing van autorisaties in SAP R/3 bepalen. Om die reden is de auditor gebaat bij goede, ondersteunende hulpmiddelen voor het ontsluiten van de autorisaties.

Bijlagen

1 Literatuur

De volgende literatuur het gebied van informatiebeveiliging en IT-audit is gebruikt bij het bepalen van de audit aspecten met betrekking tot autorisaties in algemene zin:

- Code of practice for information security management (ISO/IEC 17799)
- IT Auditing, an object oriented approach (door Margaret Elinor van Biene-Hershey)
- Bestuurlijke informatieverzorging (Starreveld)

De volgende literatuur is gebruikt bij het bepalen van audit aspecten met betrekking tot autorisaties in SAP R/3:

- Security, Audit and Control Features SAP R/3: A Technical and Risk Management Reference Guide, Second Edition (door Deloitte Touche Tohmatsu Research Team/ISACA)
- SAP Security and Authorizations (door Mario Linkies and Frank Off)

Verder zijn de volgende artikelen op het gebied van informatiebeveiliging en IT-audit geraadpleegd:

- Studie Role Based Access Control (Platform Informatiebeveiliging)
- RBAC: gewoon doen (door Peter Mienes en Bart Bokhorst)
- ERP Postimplementation Problems (door Yusuf Musaji)
- Segregation of Duties within information systems (ISACA)
- Implementation of ERP Systems: Accounting and Auditing Implications (door Benjamin B. Bae, Ph.D., and Paul Ashcroft, Ph.D.)
- Auditing Security and Privacy in ERP Applications (door S. Anantha Sayana, CISM, CISA, CIA)
- Control the actor-based access rights (door B. Elsinga en A. Hofman)
- Metadata and authorization patterns (door Eduardo B. Fernandez)
- Sarbanes-Oxley Section 404: An overview of the PCAOB's requirements (KPMG)
- Sarbanes-Oxley Section 404:10 Threats to Compliance (Deloitte)
- Sarbanes-Oxley Compliance Brief: The Challenges of Sarbanes-Oxley Section 404 Compliance (Computer Associates)
- De (on)beheersbaarheid van toegangsbeveiliging (door Peter Mienes en Bart Bokhorst)
- Handreiking Identiteiten- en Autorisatiebeheer (GvIB)

2 Kritische SAP R/3 profielen, objecten en transacties

Onderstaande in SAP R/3 standaard aanwezige autorisatieprofielen, objecten en transacties zijn het meest kritisch. Dit betreft in veel gevallen functionaliteit ten behoeve van systeembeheer. Deze functionaliteit is dus binnen elk systeem kritisch ongeacht de bedrijfsprocessen die in het systeem zijn ondergebracht.

Profiel	Profiel Tekst
S_A.CUSTOMIZ	Customizing (for All System Setting Activities)
S_A.DEVELOP	Developer
S_A.SYSTEM	System administrator (Superuser)
S_ABAP_ALL	All authorizations for ABAP/4
S_BTCH_ADM	Batch Processing: Batch Administrator
S_DB2_DBADM	DB2/390: Database Administrator
S_DEVELOP	ABAP Workbench
S_ENTW	All authorizations for the R/3 System
S_ENTW_NEW	Additional authorizations for all
S_IDOC_ALL	All authorizations for IDoc functions
S_PROGRAM	ABAP Program Flow Checks
S_RFC	RFC Access
S_SCRP_ALL	All Authorizations for SAPscript (Texts, Styles, Forms)
S_TABU	Table Maintenance
S_USER_ALL	All authorizations for user and authorization maintenance
SAP_ALL	All authorizations for the SAP System
SAP_NEW	All Authorizations for Newly Created Objects

Object	Object tekst
B_LSMW	LSMW: Transaction and Activity
S_ADMI_FCD	System Authorizations
S_BTCH_ADM	Background Processing: Background Administrator
S_BTCH_NAM	Background Processing: Background User Name
S_CTS_ADMI	Administration Functions in the Change and Transport System
S_DATASET	Authorization for File Access
S_DEVELOP	ABAP Workbench
S_IDOCCTRL	WFEDI: S_IDOCCTRL - General Access to IDoc Functions
S_IDOCDEFT	WFEDI: S_IDOCDEFT - Access to IDoc Development
S_IMG_ACTV	IMG: Authorization to Perform Functions in IMG
S_OLE_CALL	OLE Calls from ABAP Programs
S_OSS1_CTL	Authorization for OSS logon
S_PROGRAM	ABAP: Program run checks
S_RFC	Authorization check for RFC access
S_RZL_ADM	CCMS: System Administration
S_SPO_ACT	Spool: Actions
S_TABU_DIS	Table Maintenance (via standard tools such as SM30)
S_TCODE	Authoriozation Check for Transaction Start
S_USER_AGR	Authorizations: Role check
S_USER_AUT	User Master Maintenance: Authorizations
S_USER_GRP	User Master Maintenance: User Groups
S_USER_PRO	User Master Maintenance: Authorization Profile

Transactiecode	Transactie tekst
LSMW	Legacy System Migration Workbench
PFCG	Role Maintenance
SA38	ABAP Reporting
SCC1	Client Copy - Special Selections
SCC4	Client Administration
SCC5	Delete Client
SCC9	Remote Client Copy
SCCL	Local Client Copy
SE11	ABAP Dictionary
SE13	Maintain Technical Settings (Tables)
SE15	ABAP/4 Repository Information System
SE16	Data Browser
SE16N	General Table Display
SE17	General Table Display
SE36	Logical databases
SE37	ABAP Function Modules
SE38	ABAP Editor
SE73	SAPscript Font Maintenance
SE93	Maintain Transaction Codes
SM01	Lock Transactions
SM04	User List
SM18	Reorganize Security Audit Log
SM19	Security Audit Configuration
SM20	Security Audit Log Assessment
SM30	Call View Maintenance
SM31	Call View Maintenance Like SM30
SM36	Schedule Background Job
SM37	Overview of job selection
SM59	RFC Destinations (Display/Maintain)
SMT1	Trusted Systems (Display <-> Maint.)
SMT2	Trusting systems (Display <->Maint.)
SU01	User Maintenance
SU02	Maintain Authorization Profiles
SU03	Maintain Authorizations
SU10	User Mass Maintenance
SU12	Mass Changes to User Master Records