Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Borging Functiescheiding OVG-Toekennen

Risico's beperkt

Definitief

Colofon

Titel	Borging Functiescheiding OVG-Toekennen
Uitgebracht aan	Hoofddirecteur Financiën & Services DUO, Dhr. Wim Westerbeek
Datum	31 oktober 2021
Kenmerk	2021-0000248496

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Samenvatting/hoofdboodschap

DUO is een traject gestart om verbeteringen aan te brengen in haar autorisatiebeheer. Dit is een langdurig proces.
Onderdeel van autorisatiebeheer betreft functiescheiding. Voor DUO is het onduidelijk of zij functiescheiding afdoende toepast.
Functiescheiding hoort dusdanig te zijn ingericht, dat het risico op fraude, misbruik en oneigenlijk gebruik afdoende wordt gemitigeerd. De gedefinieerde functiescheiding vormt de basis voor het juist inrichten van autorisaties (het middel).
Om meer inzicht te verkrijgen heeft DUO de ADR onderzoek laten doen naar functiescheiding. Met het onderzoek beoogt zij meer inzicht in de minimaal vereiste functiescheidingen, zijnde een totaalbeeld van beschikkende functies, bewaren/beherende functies, registrerende functies, uitvoerende functies en controlerende functies te verkrijgen.
In overeenstemming met de opdrachtbevestiging is dit onderzoek gericht op OVG en met name het onderdeel OVG-Toekennen.
De inrichting en het beheer van autorisaties is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). Hierbij gelden drie principes:

1) Autorisatiebeheer moet bijdragen aan minimaal vereiste functiescheiding t.b.v. risicobeheersing;
2) Alleen toekennen autorisaties die benodigd zijn voor het uitoefenen van je functie (need-to-know);
3) Bij het toekennen van rollen met autorisaties voor applicaties, systemen en/of gegevens wordt het "minste privilege" meegewogen. Hierdoor wordt de kans op bewust of onbewust misbruik van gegevens beperkt (least privilege).

De belangrijkste boodschap die uit ons onderzoek naar voren komt is:

Functiescheiding is in praktijk geborgd. Onderliggende visie en AO-beleid ontbreken.

Het algemene beeld is dat het incidenteel doorbreken van functiescheiding binnen OVG-Toekennen niet tot onoverkomelijke risico's leidt.

Maken we de onderverdeling naar Opzet en Bestaan, dan constateren we grote verschillen. In opzet schiet functiescheiding tekort. In bestaan zijn maatregelen getroffen die functiescheiding (deels) borgen.

Opzet
Er zijn geen documenten aangetroffen waaruit blijkt wat DUO onder functiescheiding verstaat of waaruit blijkt wat in het kader van functiescheiding wel of juist niet mag. Het autorisatiebeleid DUO geeft geen concrete eisen tav functiescheiding[1]. We hebben geen risicoanalyse aangetroffen, waaruit blijkt welke functies of rollen als kritisch zijn beoordeeld. Of er functies/rollen zijn die niet met elkaar gecombineerd mogen worden is eveneens niet duidelijk.
Functiescheiding voor DUO is in opzet niet gedefinieerd, niet beschreven en niet uitgewerkt.

[1] Autorisatiebeleid DUO 2021-2023 versie 2.0

In een document "Richtlijn voor het beschrijven van de administratieve organisatie bij OCW" d.d. 20-12-2010 is in een bijlage aandacht besteed aan de theorie achter functiescheiding. Het feit dat het in een bijlage is beschreven, daterende uit 2010, is voor ons aanleiding om te zeggen dat een strategische visie ten aan zien van functiescheiding in opzet niet geregeld is.

Bestaan
Uit de gesprekken die we hebben gevoerd blijkt dat er wel wordt nagedacht over functiescheiding en dat functiescheiding is ingeregeld. Over het algemeen wordt functiescheiding door medewerkers van DUO gedefinieerd als "het beschikken over alleen de autorisaties die benodigd zijn voor het uitoefenen van je functie".
In de basis zijn Toekennen en Innen van elkaar gescheiden. Dit geldt ook voor Beheer en Ontwikkeling. Het onderscheid tussen directies is eveneens aanwezig. Dit neemt niet weg dat er uitzonderingen zijn gemaakt. Klantgerichtheid speelt een belangrijke rol bij uitzonderingen. Dit principe noemen ze Integrale Afhandeling: een klant moet volledig kunnen worden bediend door één medewerker Servicekantoor (SK). Het risico bestaat dat er onterecht toekenningen worden gedaan, waarbij de schuld/vereiste terugbetalingen worden kwijtgescholden/afgeboekt, ofwel dat er onterecht gelden wegvloeien.

Met de komst van het project autorisatiebeheer wordt de stapeling van functies opgeheven. Layer7 gaat hierin voorzien, maar dit is niet volledig geïmplementeerd. Op moment dat iemand van functie verandert en nieuwe rollen toebedeeld krijgt, moeten de oude rollen komen te vervallen.
OVG is de eerste afdeling die gebruik maakt van Layer7. De uitkomsten van ons onderzoek zijn voor een deel gebaseerd op de intenties met betrekking tot Layer7.

Er is een belangrijke rol weggelegd voor het (lijn)management. Zij zien periodiek toe op de juiste toedeling van functierollen. Functierollen worden in een driehoek van roleigenaar, rolbeheerder en resource-eigenaar beheerd en toebedeeld.
Alle mutatie-activiteiten van medewerkers worden binnen OVG gelogd. Monitoring van de logging vindt plaats op moment dat daar aanleiding toe is. Dit vinden wij beperkt.
Op functiescheiding vindt geen verdere controle plaats.
Met het in gebruik nemen van Layer7 moet het mogelijk worden om conflicterende rollen in beeld te krijgen. Zoals eerder aangegeven is dit een ontwikkeling die in gang is gezet.

Beantwoording onderzoeksvragen

***Hoofdvraag:* Welke aandachtspunten onderkent de ADR bij borging van de functiescheiding binnen DUO en welk handelingsperspectief kan de ADR hierbij geven?**
Aanbevelingen en/of vervolgstappen zijn in hoofdstuk 9 nader uitgewerkt. Wij geven de onderstaande aanbevelingen ter overweging mee:

- Beschrijf de opzet van functiescheiding
- Implementeer Layer7 zoals initieel bedacht
- Definieer functies/rollen eenduidig
- Voer een risicoanalyse uit en leg deze vast
- Monitor de logging
- Management moet rol pakken

Subvragen:

- **Wat verstaat bestuur/directie DUO onder functiescheiding op strategisch niveau? Hoe is functiescheiding gedefinieerd?**
  Functiescheiding is op strategisch niveau niet gedefinieerd (zie 1.1).
- **Hoe is functiescheiding ingeregeld / geborgd?**
  Op tactisch / operationeel niveau is nagedacht over functiescheiding (zie 1.2). Het concept van functiescheiding is niet helder en eenduidig omschreven.
- **Zijn risico's in kaart gebracht?**
  Risico's zijn niet beschreven (zie 3.1 en 3.2).
- **Vindt monitoring plaats?**
  Monitoring op logging vindt plaats indien daar aanleiding toe is. Monitoring op toegekende autorisaties vindt periodiek door het management plaats (zie 1.4; 5.2; 6.1).
- **Is functiescheiding beschreven in werkinstructies?**
  Functiescheiding blijkt niet uit werkinstructies (zie 2.2).
- **Is functiescheiding in/tussen systemen/applicaties aangebracht?**
  Scheiding in / tussen systemen / applicaties is aangebracht (zie 4.1).
- **Is er onderscheid in ontwikkeling en beheer?**
  Ontwikkeling en beheer worden van elkaar gescheiden (zie 1.3)
- **Blijkt functiescheiding in autorisatiematrices? RBAC? Layer7?**
  Autorisatiematrices geven onderscheid in rollen (zie 3.3).
  Layer7 ondersteunt de borging van functiescheiding (zie 2.1).
- **Zijn de aangetroffen functiescheidingen toereikend?**
  De risico's zijn beperkt.

1 Conflicterende taken (BIO 6.1.2)

Norm: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbedoeld wijzigen of misbruik van bedrijfsmiddelen van de organisatie te verminderen (BIO 6.1.2).

1.1 Functiescheiding op strategisch niveau is niet gedefinieerd

Er zijn geen formeel vastgestelde documenten aangetroffen waaruit blijkt wat DUO onder functiescheiding verstaat of waaruit blijkt wat in het kader van functiescheiding wel of juist niet mag. We hebben geen risicoanalyse aangetroffen, waaruit blijkt welke functies of rollen als kritisch zijn beoordeeld. Of er functies/ rollen zijn, die niet met elkaar gecombineerd mogen worden is eveneens niet duidelijk.
Functiescheiding is in opzet niet gedefinieerd, niet beschreven en niet uitgewerkt. In een document "Richtlijn voor het beschrijven van de administratieve organisatie bij OCW" d.d. 20-12-2010 is in een bijlage aandacht besteed aan de theorie achter functiescheiding. In de bijlage is nadere duiding gegeven aan functiescheiding. In dit document is in opzet scheiding aangebracht in beschikken, bewaren, registreren, controleren en uitvoeren. Verder is er ten minste onderscheid in 'verplichten' en 'betalen', 'vorderingenbeheer', 'kasbeheer' en 'financiële administratie' vereist. De vertaling van dit beleid/richtlijn, naar de DUO situatie is nog niet uitgevoerd. De directie stimuleert awareness, alsmede het vastleggen van functiescheiding.
Primaire functiescheiding is aangebracht. Financiele administratie en de betalingsfunctie zijn gescheiden van de uitvoering. Secundaire functiescheiding tussen Toekennen en Innen is in beginsel aanwezig, maar daarop worden uitzonderingen gemaakt.

1.2 Op tactisch/operationeel niveau is nagedacht over functiescheiding

Er is geen eenduidige definitie. Iedereen heeft zijn eigen perceptie op functiescheiding. Het concept van functiescheiding is in ieder geval nog niet helder en eenduidig omschreven. De geïnterviewden vonden over het algemeen dat functiescheiding binnen DUO zodanig zou moeten zijn ingericht dat medewerkers niet meer bevoegdheden/ autorisaties hebben, dan ze nodig hebben om hun functie uit te oefenen. Het is hierbij niet de bedoeling dat iemand bepaalde werkzaamheden uitvoert die hem toegang geven tot een hele keten. Bijvoorbeeld: Toekennen is gescheiden van Innen.
Scheiding tussen de rollen is strikt, al worden daar wel uitzonderingen op gemaakt. De scheiding tussen Toekennen en Innen wordt voor medewerkers van de servicekantoren losgelaten. Aanvullende beheersmaatregelen zijn (deels) ingebouwd om oneigenlijk gebruik te voorkomen. Aanvullende beheersmaatregelen bestaan uit controles achteraf, welke niet beschreven zijn.
Scheiding van rollen is belangrijk, maar DUO wil de klant wel goed en door één medewerker kunnen bedienen.

1.3 Uitgangspunten functiescheiding zijn niet beschreven

De uitgangspunten van functiescheiding zijn niet in een beleidsdocument uitgeschreven, zie ook paragraaf 1.1. In bijlage 5 van het eerdergenoemde document "richtlijn voor het beschrijven van de administratieve organisatie OCW" staan algemene principes ten aanzien van functiescheiding beschreven. Hierbij wordt onderscheid gemaakt in beschikken, bewaren, registreren, controleren en uitvoeren. Ook is er onderscheid gemaakt tussen Verplichten, Voorschotten, Betaalbaar stellen & betalen. Bij Buiten invordering stellen en Kwijtschelden is er onderscheid tussen initiëren en goedkeuren.
Er wordt scheiding aangebracht tussen:

+ Toekennen en Innen;
+ Toekennen en Uitbetalen;
+ Productie en Ontwikkeling;
+ Beheer en Productie.

De scheiding Productie en Ontwikkeling is een lastige wegens het gebruik van DevOps-teams. Dit wordt opgelost door medewerkers autorisaties van de productieomgeving of de ontwikkelomgeving te verstrekken en geen combinatie van beide omgevingen. Door samenspanning is functiescheiding te doorbreken.
Het feit dat functiescheiding in een bijlage is beschreven, daterende uit 2010, is voor ons aanleiding om te zeggen dat een strategische visie ten aanzien van functiescheiding in opzet niet geregeld is.
In de procesbeschrijvingen van de toekennen processen zien wij geen vermelding dat processen of taken door verschillende personen moeten worden uitgevoerd of dat sprake is van een vier-ogencheck. Wel zijn de volgende maatregelen/ overwegingen aangetroffen:

- Het muteren van oninbare vorderingen gebeurt na goedkeuring door de operationeel manager, de tactisch manager of de directeur (afhankelijk van de hoogte van de bedragen) zodat hier geen risico's worden gelopen.
- Het inherente risico van mutatie van bankrekeningnummers wordt, door getroffen beheersmaatregelen, niet als risico gezien. Er wordt ook van uit gegaan dat een klant zelf aan de bel trekt als hij zijn geld niet krijgt.
- Per applicatie zijn rollen gedefinieerd en elke rol kent vaste autorisaties, waardoor risico's op oneigenlijke autorisaties zijn gemitigeerd.

1.4 Monitoring van functiescheiding vindt incidenteel plaats

In de procesbeschrijvingen is geen vermelding van monitoring op het vlak van functiescheiding.
Er is sprake van logging van werkzaamheden, maar het monitoren van de logging is geen standaard activiteit. Monitoring vindt hoofdzakelijk plaats indien daar een directe aanleiding voor is.
Functiescheiding zou in de basis gemonitord moeten worden in de driehoek rolbeheerder, resource-eigenaar en rol-eigenaar. Echter, in deze driehoek is de functiescheiding niet gegarandeerd, doordat bijvoorbeeld een PO van deze 3 rollen meerdere rollen kan hebben (zie ook paragraaf 5.1).

2 Formele registratie- en afmeldingsprocedure (BIO 9.2.1)

Norm: een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken (BIO 9.2.1).

2.1 In Layer7 is voorzien in een in-, door- en uitstroomproces

De implementatie van de nieuwe tool Layer7 zal naar verwachting in 2022 voor heel DUO worden afgerond. Volgens de planning zou de tool aan het eind van dit jaar volledig functioneel moeten zijn voor OVG. Deze zal het autorisatiebeheer en de functiescheiding verder ondersteunen, doordat deze de beheerfunctie van de autorisatiematrix overneemt. De verwachting is dat door de komst van Layer7 de bestaande problemen worden opgelost. Het is op dit moment bijvoorbeeld de verantwoordelijkheid van de ontvangende manager om oude rollen in te trekken wanneer medewerkers binnen DUO naar een andere afdeling vertrekken. Dit gebeurt niet altijd, waardoor het voorkomt dat er bij monitoring onterechte autorisaties blijken uit de autorisatieoverzichten. In Layer7 zal dit intrekproces automatisch verlopen, waardoor medewerkers alleen over autorisaties beschikken die volgens Layer7 toebehoren aan hun nieuwe rol. Wanneer Layer7 een autorisatie als onrechtmatig beschouwt dan wordt deze ingetrokken. Deze autorisatie komt in een uitvallijst, welke beoordeeld en afgehandeld moet worden.

Layer7 is voorzien van een instroom, doorstroom en uitstroom proces[2]. De nieuwe (ontvangende) manager is verantwoordelijk voor het toekennen van de nieuwe rollen. Binnen Layer7 worden, in geval van doorstroom, de "oude rollen" automatisch uitgezet.
Het (lijn)management heeft een belangrijke rol in het bewaken van instroom en uitstroom. Product owners hebben niet altijd zicht op uitstroom, omdat zij op proces niveau opereren.
Bij het vervullen van een tijdelijke rol stappen medewerkers uit de eigen rol en bijbehorende autorisaties. Na de klus keren ze terug in de eigen rol en laten ze de tijdelijke autorisaties achter.
Ontheffingen, om functiescheiding tijdelijk te doorbreken, worden verleend op hoger niveau; dat moet goedgekeurd worden door de business manager/directeur OVG en door de directeur ICT. Dit verloopt langs een vast patroon waarbij 1e en 2e lijn medewerkers/adviseurs, managers, directeuren en mogelijk bestuur een beslissende rol vervullen.

2.2 Functiescheiding blijkt niet uit werkinstructies

Er is beschreven welke taken worden uitgevoerd door de medewerkers. Ook is beschreven wat geautomatiseerd wordt uitgevoerd of door andere partijen (bijv. andere afdelingen of externen) wordt opgepakt. Ten aanzien van functiescheiding en vier-ogenprincipe is niets beschreven.

[2] Instroom betreft nieuwe medewerkers, doorstroom betreft medewerkers die (tijdelijk) intern van functie veranderen, uitstroom betreft medewerkers die uit dienst gaan.

3 Risicoafweging (BIO 9.2.2.2)

Norm: op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven (BIO 9.2.2.2).

Norm: functiescheidingsvereisten zijn opgenomen in de autorisatiematrix (DUO voorschrift Autorisatiematrices).

3.1 Risico's zijn niet beschreven

Het idee heerst binnen OVG dat een risicoanalyse is uitgevoerd op het gebied van functiescheiding. Er is echter geen document waaruit specifieke risico's ten aanzien van functiescheiding blijken. Er is voor OVG een risicoanalyse uitgevoerd, maar die bevat geen aspecten met betrekking tot functiescheiding (bron: controlematrices[3]). Indien een bedrijfssysteem als bedrijfskritisch is betiteld, dan worden alle onderliggende processen en systemen als bedrijfskritisch gezien. Alle systeemautorisaties zijn daarmee als bedrijfskritisch aangemerkt.

In het DUO voorschrift Autorisatiematrices 0.9.4 is beschreven dat een belangrijk onderdeel bij het geven van autorisaties het bepalen van kritieke autorisaties is, en vervolgens het bepalen van onverenigbare autorisaties, de zogenaamde rol-/functieconflicten. Een bekend voorbeeld is dat de persoon die het rekeningnummer mag wijzigen geen betalingen mag doorvoeren/accorderen.

3.2 Periodieke controles zijn in ontwikkeling

Door het ontbreken van een risicoanalyse en duidelijk gedefinieerde risico's is het lastig om te spreken van periodieke controles. Waarop controleer je, als er geen risico's zijn bepaald. Controles zijn in ontwikkeling. Een risicoanalyse kan helpen om de benodigde beheersmaatregelen te bepalen.
De systeemcontrole op kritische systemen zal vier keer per jaar worden uitgevoerd. De resource-eigenaren beoordelen daarbij of de persoon binnen de scope van de autorisatie past. Er wordt dus vanuit de rol naar de persoon gekeken, maar andersom ook: "deze persoon heeft deze rollen". Dit laatste doen de manager en de rolbeheerder, tevens vier keer per jaar. Beide personen moeten de check uitvoeren en bevestigen. De manager en rolbeheerder kunnen echter dezelfde persoon zijn. Het lijnmanagement speelt derhalve een belangrijke rol in de controle, omdat zij periodiek de toegekende autorisaties monitoren.

3.3 Autorisatiematrices geven slechts onderscheid in rollen

Uit de autorisatiematrix blijkt welke rollen bij welke functie horen. Wat je niet kunt zien is of er medewerkers zijn met meerdere rollen.
De taken die vallen onder de rollen en die eventueel conflicterend zijn, blijken niet uit de matrix. Het is niet altijd duidelijk wat die taken precies inhouden (en dus ook niet welke conflicterend zijn).
Er is geconstateerd dat Arbitrair beslissen samenvalt met de rol SFS productie toekennen. Een medewerker productie Toekennen kan hierdoor ook Arbitrair

[3] Controlematrix Toekennen versie 1.0 en Controlematrix Innen 2020 versie 1.0 dd 13-10-2020.

beslissen. De achterliggende gedachte dat één proces niet in handen mag zijn van één persoon blijkt hier niet uit.
Splitsen van Toekennen en Innen bij medewerkers Klantbediening wil DUO bewust niet toepassen. Het risico bestaat dat er onterecht toekenningen worden gedaan, waarbij de schuld/vereiste terugbetalingen worden kwijtgescholden/afgeboekt, ofwel dat er onterecht gelden wegvloeien. Het bedienen van de klant heeft hier voor DUO prioriteit boven functiescheiding.

De trajecten POK, Werk aan Uitvoering en de bevindingen van de Tijdelijke Commissie Uitvoering hebben geleid tot extra aandacht voor de uitvoering. In de zomer van 2021 is door het kerndepartement van OCW en DUO besloten om een gezamenlijke aanpak rondom maatwerk omtrent studiefinanciering op te stellen. DUO wil (nieuwe) mogelijkheden benutten om meer rekening te houden met persoonlijke situaties van klanten. Dit vraagt een zekere ruimte in handelingsbevoegdheid van medewerkers, hetgeen consequenties zal hebben voor functiescheiding.

Soms is van autorisaties niet duidelijk wat ermee bedoeld wordt. De autorisatie "werkbakken" is daar een voorbeeld van.

Opvoeren van normen en het fiatteren van normen is in één hand in het geval van de rol SFS-Sturing Specialist. Hier is voor gekozen omdat het anders IT-technisch niet werkt. Dit is uit controle technisch oogpunt niet wenselijk.

In Layer7 kan de scheiding worden afgedwongen en/of inzichtelijk worden gemaakt dat er sprake is van conflicterende situaties.

4 Koppelvlakken

Norm: van in autorisatiesmatrices opgenomen koppelvlakken moet bepaald zijn welke autorisaties een functiescheidingsconflict opleveren tussen de gekoppelde resources (DUO-voorschrift Autorisatiematrices).

Er is geconstateerd dat functiescheidingsvereisten zijn opgenomen in de autorisatiematrix (DUO-voorschrift Autorisatiematrices).

4.1 Scheiding in/tussen systemen/applicaties is aangebracht

Er is functiescheiding binnen de applicaties, over de afdelingen heen, over de directies heen en op transactieniveau. Deze functiescheiding wordt "veroorzaakt" doordat er in principe verschillende teams zijn per afdeling. Het is niet zo dat er afdeling-/applicatie-overstijgend conflicterende rollen worden geïdentificeerd, want de autorisatiematrices worden opgesteld per applicatie. Met de implementatie van Layer7 zullen betreffende conflicterende situaties worden geïdentificeerd.

Vroeger zat alle data m.b.t. studiefinanciering in 1 systeem en was het voor alle afdelingen en directies toegankelijk. Nu is dat anders. SFS maakt gebruik van gegevens uit registers van de directie RNE. Alleen voor zaken die niet in registers van RNE staan is er binnen de directie OVG een eigen Klantopgaveregister. De afdelingen en directies kunnen dus niet beschikken over gegevens uit de registers die niet bij hun functies horen. RNE kan muteren in de basisregisters, dat kan OVG niet zelf doen.

4.2 Autorisatiematrices geven geen inzicht in koppelvlak conflicten

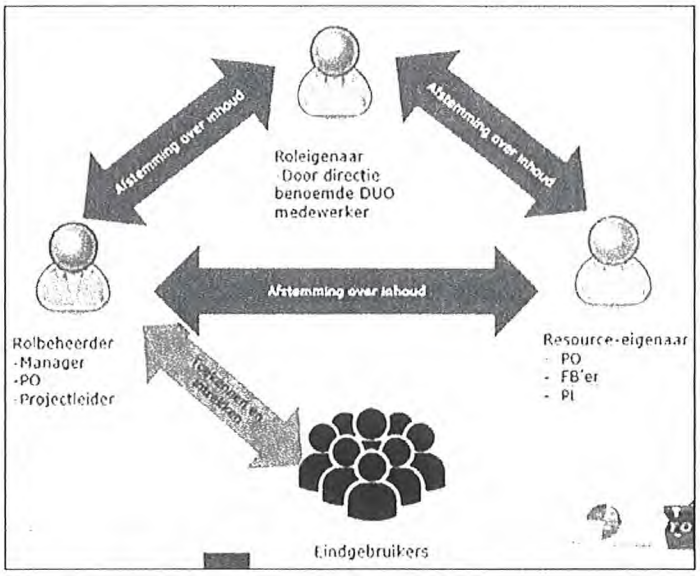
Uit de autorisatiematrix blijkt welke autorisaties bij welke rollen horen. Uit de autorisatiematrix blijkt niet of er sprake is van koppelvlakken en eventuele conflicten. De autorisatiematrices zijn role-based ingericht. Per rol wordt gekeken welke autorisaties daarbij horen.

5 Mandaatregister (BIO 9.2.2.3)

Norm: er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten (BIO 9.2.2.3).

5.1 Toekennen autorisaties belegd in driehoek resource-eigenaar, roleigenaar en rolbeheerder

Er is een actueel mandaatregister, al gaat dat meer over het autoriseren van betalingen. In dit mandaatregister is niet vastgelegd wie de bevoegdheid heeft om autorisaties te verlenen.
Het toekennen van autorisaties/verlenen van toegangsrechten is belegd in de driehoek resource-eigenaar, roleigenaar en rolbeheerder. Dit blijkt verder niet uit de autorisatiematrix, terwijl het wel van belang is, aangezien het rollen betreft van medewerkers. Met de implementatie van Layer7 zal dit nadrukkelijker tot uiting komen.
De rolbeheerder kent de rollen toe en mag deze intrekken. De rolbeheerder gaat periodiek controles uitvoeren op de koppeling tussen de rol en de eindgebruiker (conform onderstaande plaatje).
De roleigenaar zorgt voor de wijzigingen in de rol. Dit doet hij op verzoek van de rolbeheerder, (de manager, de product owner, projectleider(zie plaatje)) of resource-eigenaar.
De resource-eigenaar stelt de autorisaties beschikbaar om op te nemen in de rollen in het doelsysteem. De resource-eigenaar gaat periodieke controles uitvoeren op de autorisaties in het doelsysteem en de daarop gebouwde rollen.



5.2 Logging vindt plaats, monitoring is in ontwikkeling

Uit gesprekken blijkt dat alle mutatie-handelingen van medewerkers gelogd worden. Raadpleeg-handelingen worden niet gelogd. Of er vervolgens ook iets met die logging gedaan wordt is niet helemaal duidelijk. Managers geven aan dat de logging gecontroleerd wordt, maar wij hebben niemand gesproken die dat daadwerkelijk structureel doet. Incidenteel wordt de logging bekeken. Aan de hand van signalen wordt er dan naar de logging gekeken. Wat de eventuele norm voor beoordeling is, is niet duidelijk.

6 Beoordeling toegangsrechten (BIO 9.2.5)

Norm: eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen (BIO 9.2.5).

6.1 Operationeel management beoordeelt toegangsrechten. Periodiciteit wisselt

Het is de verantwoordelijkheid van de manager om het overzicht van autorisaties actueel te houden, want die overziet wie er nog in de betreffende rol werken/wie er weg gaan.

Een keer per kwartaal krijgen de managers een overzicht van welke medewerkers welke rol hebben. De manager moet hierop reageren en wordt waar nodig gerappelleerd.
In Layer 7 zullen de taken van de driehoek ook ingeregeld worden in de tooling voor elk systeem.

De logging vormt de basis voor rapportages. DUO is van plan om in Layer7 in te regelen dat beheerders een notificatie krijgen wanneer een medewerker probeert autorisaties aan zichzelf toe te kennen/te wijzigen. Deze notificatie moeten de beheerders controleren en indien nodig acties op nemen.

7 Overige bevindingen

7.1 Algemeen beeld onder medewerkers

Autorisatiebeheer
Over het algemeen wordt de huidige toepassing van functiescheiding door de medewerkers niet als risicovol beschouwd. In het verleden heeft de ADR bevindingen gerapporteerd ten aanzien van het stapelen van autorisaties, doordat oude autorisatierollen niet werden ingetrokken in het geval van een nieuwe functie. Inmiddels heeft er binnen het autorisatiebeheer een opschoonactie plaatsgevonden en is het Role Based Access Control (RBAC) project gestart. Daarnaast gaf Procescontrol aan dat uit hun onderzoeken is gebleken dat functiescheiding binnen processen goed geborgd is. Het heersende beeld onder medewerkers is daardoor dat het autorisatiebeheer overwegend schoon en sluitend is geworden, en daarmee ook de toepassing van functiescheiding. Er zijn binnen DUO nog steeds veel autorisaties toebedeeld, maar dit wordt niet gezien als een risico, omdat alle handelingen gelogd worden. De medewerkers zijn daarbij van mening dat men moet kunnen vertrouwen op de autorisatieprofielen, de controles door managers en de eed/belofte die de medewerkers hebben afgelegd.

Volledige borging van functiescheiding een illusie
Gedurende dit onderzoek kwam naar voren dat medewerkers een volledige borging van functiescheiding als een illusie beschouwen, omdat handmatige handelingen onvermijdelijk zijn. Aangezien het hierbij maatwerk op individueel niveau betreft, moeten er soms extra autorisaties toegekend worden. Bij het toekennen van deze autorisaties wordt gecontroleerd of functiescheiding nog geborgd is. Aangezien alle activiteiten worden gelogd wordt dit niet als risico gezien, omdat ze herleidbaar zijn tot de betreffende medewerker.

Volledige borging van functiescheiding onwenselijk
Medewerkers gaven de indruk functiescheiding een zwaar middel te vinden en tot op zekere hoogte onwenselijk. Functiescheiding conflicteert namelijk met DUO's principe van integrale klantafhandeling, waarbij een medewerker SK een klant volledig moet kunnen bedienen. Ook is de beleving dat functiescheiding *agile* werken tegengaat in het geval van nieuwe projecten, wat als frustrerend wordt ervaren door medewerkers. Tot slot wordt een volledige borging van functiescheiding onwenselijk geacht om financiële redenen. Een voorbeeld hierbij is het muteren van rekeningnummers van klanten. In theorie is het mogelijk dat een medewerker zijn eigen rekeningnummer invoert en accordeert. In de praktijk zal dit echter opvallen, omdat de klant contact op zal nemen met DUO zodra deze opmerkt dat hij of zij geen geld heeft ontvangen. Het volledig inregelen van functiescheiding binnen dit proces zou veel benodigde man-uren en daarmee geld kosten. Deze kosten zouden volgens de medewerkers disproportioneel zijn ten opzichte van het respectievelijke risico.

7.2 Handelsperspectieven volgens medewerkers

De medewerkers met wie wij hebben gesproken hebben verschillende handelsperspectieven benoemd om de toepassing van functiescheiding binnen OVG te verbeteren.

Mitigeren van technische belemmeringen
Volgens de planning zou Layer7 aan het eind van dit jaar volledig functioneel moeten zijn voor OVG, maar in de praktijk is de verwachting dat dit voor 80% het geval zal zijn. Role-mining blijkt namelijk veel werk te zijn. OVG is pionier wat betreft de implementatie van Layer7, dus kost het opdoen van gebruikerservaring en het oplossen van bugs veel tijd. Inmiddels zitten de functierollen van OVG in Layer7. Een probleem doet zich voor binnen de rol "Productie sturing specifiek". De product owner krijgt autorisatie tot zowel het opvoeren van normen als het fiatteren daarvan. Deze autorisaties zijn aan elkaar gekoppeld, omdat het anders IT-technisch niet functioneert. Een medewerker kan namelijk alleen bij de functie van het fiatteren komen wanneer diegene ook de opvoerautorisatie heeft. Dit probleem is nog niet verholpen in verband met andere, meer urgente taken. Het risico wordt door het management nog niet onderkend, waardoor acties uitblijven.

Afdeling overstijgend identificeren van conflicterende rollen
Momenteel wordt vooral op afdelingsniveau of op applicatieniveau naar autorisaties gekeken. Medewerkers hebben aangegeven behoefte te hebben aan een afdeling- en applicatie overstijgende benadering in het identificeren van conflicterende rollen. Een groot aantal medewerkers kan namelijk zowel toekennen als innen, aangezien zij taken hebben op beide vlakken. Hiertoe zouden gesprekken tussen analisten van verschillende afdelingen gefaciliteerd moeten worden. Deze situatie is bekend bij het management en wordt acceptabel geacht. Controletechnisch is het beter om toekennen en innen van elkaar gescheiden te houden.

Verscherpen beheersing functiescheiding
Volgens medewerkers zou de beheersing van functiescheiding verscherpt kunnen worden door het monitoren van rollen te standaardiseren. Ook het kritisch beoordelen of bepaalde autorisaties noodzakelijk zijn voor het uitoefenen van een functie zou een verscherping zijn. Daarnaast is het mogelijk om met ontheffingen te werken, wanneer het beleid niet strookt met het belang van de afhandeling. Momenteel zijn er veel ontheffingen verleend, waardoor een ontwikkelaar bijvoorbeeld raadpleegautorisaties heeft in de productieomgeving. Bij de beoordeling van de periodieke overzichten van autorisaties door het (lijn)managament, wordt gecontroleerd of de ontheffingen nog terecht zijn. Gedurende het onderzoek is genoemd dat werken met ontheffingen binnen Devops-teams de huidige gang van zaken is, hoewel op alle ontheffingen een explainer zit ter toelichting. Ook is er een mogelijkheid tot een autorisatieswitch, waarbij een ontwikkelrol afgesloten kan worden om in een andere rol verder te kunnen. Dit wordt door de medewerkers onwenselijk geacht. Er is een vier-ogencontrole ontwikkeld voor autorisatieswitches, maar deze is nog niet in productie genomen.

Verhelderen onderliggend beleid
De medewerkers gaven aan behoefte te hebben aan een betere vertaling van het AO-beleid van OCW naar DUO, waarbij invulling wordt gegeven aan kaderstelling en op welke manier deze kaders worden getoetst. Daarnaast zouden de medewerkers graag zien dat business rules ten aanzien van functiescheiding worden vastgelegd in de autorisatiematrices.

7.3 Overige opvallendheden

Daarnaast zijn ons gedurende het onderzoek een aantal zaken opgevallen.

Autorisatiematrix in Excel
De autorisatiematrix is gemaakt en in bewerking in de vorm van een Excelbestand. Hierdoor zouden medewerkers ongezien zaken kunnen wijzigen. Dit bestand staat weliswaar opgeslagen op een schijf waar alleen bevoegde medewerkers toegang tot hebben, maar is niet beveiligd middels een wachtwoord. Bovendien kunnen mutaties niet worden gelogd via dit medium.

Benadering vanuit IST-situatie
Wanneer de bestaande functiescheiding tussen bepaalde rollen goed is bevonden door DUO, wordt deze overgenomen in de autorisatiematrix en Layer7. Deze beoordeling vindt plaats op basis van ervaring, maar concrete randvoorwaarden zijn hierbij niet geformuleerd. Het uitgangspunt bij het inrichten en vullen van de autorisatiematrix lijkt dus het bepalen van hetgeen behouden moet blijven, in plaats van dat er vanuit een nul-situatie opnieuw wordt opgebouwd. Een ander uitgangspunt hierbij lijkt te zijn dat DUO voorzichtig is in het wegnemen van autorisaties. DUO acht het namelijk een veel groter risico dat een medewerker te weinig autorisaties heeft dan te veel, waardoor diegene zijn werk niet kan doen.

Geen eenduidige invulling functierollen
Er is geen eenduidige onderscheidende invulling van bepaalde functies. Een product owner is bijvoorbeeld soms resource eigenaar, maar soms ook niet. Daarnaast kan een product owner ook proces eigenaar zijn, wat met name voorkomt bij product owners binnen OVG. Bij systeemcontroles op kritische processen controleren de manager en rolbeheerder samen of de toegekende rollen aan de individuele medewerkers rechtmatig zijn. De manager en rolbeheerder kunnen echter dezelfde persoon zijn. Door het gebrek aan een eenduidige en onderscheidende invulling van een functie is functiescheiding dus lastig te borgen.
Tijdens het onderzoek werd duidelijk dat het verschil tussen functierollen soms niet helemaal zuiver is, waardoor autorisaties onterecht meekomen. De rol "Productie Algemeen" geeft basis muteerrechten, waardoor een medewerker Vorderingen kan muteren. Deze autorisatie is dus niet alleen toebedeeld aan Innen-medewerkers maar, in het kader van functiescheiding ongewild en ongewenst, ook aan medewerkers buiten Innen.

Verwarrende terminologie
In de autorisatiematrix staan een aantal termen die verwarring kunnen oproepen. Zo wordt de term "productie" veelvuldig gebruikt, terwijl deze rol ook bestaat in de ontwikkelomgeving. Ook "Rekening mutaties" kan geïnterpreteerd worden als een autorisatie tot het muteren van rekeningen, terwijl het in werkelijkheid een raadpleegfunctie betreft. Hoewel verantwoordelijken voor de autorisatiematrix zich bewust zijn van deze verwarrende terminologie, is daar nog geen verandering in aangebracht.

Onduidelijkheid in beheer autorisatiematrix
De ADR heeft de indruk dat er soms onduidelijkheden bestaan ten aanzien van het beheer van de autorisatiematrix. Alle product owners van SFS staan in de matrix vermeld als zijnde tekenbevoegd, terwijl zijzelf het beeld schetsten alleen een raadpleegautorisatie daarin te hebben. Ook werd door medewerkers verondersteld dat de autorisatiematrix naast SFS tevens de autorisaties van ABL bevatte, maar dit blijkt niet het geval te zijn. Bij het opvragen van de autorisatiematrix voor ABL verwezen medewerkers ons naar collega's, die ons weer naar andere collega's verwezen. Het is niet duidelijk wie verantwoordelijk is voor het beheer van de autorisatiematrix ABL.

Geen aansluiting tussen autorisatiematrix en functiegebouw
De hoofdprocessen in de autorisatiematrix komen niet overeen met de hoofdprocessen zoals gepresenteerd in het functiegebouw. De medewerkers hebben aangegeven dat dit functiegebouw is gemaakt in Den Haag en niet aansluit op de werkelijke processen. In het functiegebouw worden alle rollen binnen schaal 6 tot schaal 11 met de generieke rol "medewerker adviseur behandelen" aangeduid, wat niet overeenkomt met de werkelijkheid. Een nadere specificatie van de rollen o.b.v. de werkelijke processen ontbreekt.

8 Aanbevelingen en/of vervolgstappen

Beschrijf de opzet van functiescheiding
Het is belangrijk om de opzet van functiescheiding goed te beschrijven. Iedereen moet weten wat er bedoeld wordt en binnen welke kaders zaken uitgevoerd kunnen worden. Strategisch: duidelijk moet zijn waarom functiescheiding van belang is en wat de minimale eisen zijn. Tactisch/operationeel: duidelijk moet zijn wat het concreet inhoudt en wat wel/niet mag in het kader van functiescheiding. Conflicterende rollen moeten duidelijker uit de autorisatiematrix blijken.

Implementeer Layer7 zoals initieel bedacht
Layer7 is een bruikbaar middel om functiescheiding te borgen. De gewenste functiescheiding kan worden aangebracht en vervolgens worden gemonitord. Maak deze ontwikkeling af binnen een afgesproken tijdspad. Doe hierin geen concessies, omdat dat sneller of goedkoper moet. Kwaliteit moet voorop staan.

Definieer functies/rollen eenduidig
De ene functie is de andere niet, ondanks dat functies gelijk lijken.
De autorisaties van de product owner SFS zijn niet gelijk aan die van de product owner ABL. Niet alle product owners zijn resourcemanager. Leg in een mandaatregister vast wie de bevoegdheid heeft om autorisaties te verlenen.

Voer een risicoanalyse uit en leg deze vast
Na uitvoering van een risicoanalyse is bekend waar de risico's op het gebied van functiescheiding zitten. Vervolgens kunnen op basis van de geïdentificeerde risico's beheersmaatregelen, waaronder periodieke controles, worden ingericht.

Monitor de logging
Het vastleggen van de logging is een eerste stap. Een tweede stap die hierop aansluit is het periodiek monitoren van de logging. Momenteel vindt monitoring op ad hoc basis / incidenteel plaats. Monitor de logging periodiek op structurele wijze.

Management moet rol pakken
Management blijft een belangrijke rol houden in het toekennen en intrekken van autorisaties. Autorisaties moeten tijdig worden verstrekt en weer worden ingetrokken.
Het management dient initiatief te nemen bij periodieke controles.

9 Verantwoording onderzoek

9.1 Werkzaamheden en afbakening

Werkzaamheden
Ten behoeve van dit onderzoek hebben we de volgende werkzaamheden uitgevoerd:

1. We hebben interviews gehouden met relevante functionarissen binnen OVG. De geïnterviewden zijn product owners en managers binnen SFS en ABL, alsmede projectmanagers van het project Autorisatiebeheer Blijvend in Control en een procescontroller. De te interviewen personen zijn onder andere door de opdrachtverstrekker aangegeven, maar zijn ook gedurende het onderzoek bepaald aan de hand van doorverwijzingen door de geïnterviewden. Van de interviews hebben wij verslagen opgesteld, welke zijn teruggekoppeld voor hoor en wederhoor.
2. Waar van toepassing hebben wij kennisgenomen van documenten ter ondersteuning van de bij de interviews verstrekte informatie, zoals de voor SFS opgestelde autorisatiematrix.
3. De informatie die in de interviews en documentatie is verzameld is gebruikt voor de analyse, ten behoeve van de beantwoording van de subvragen en de formulering van de handelsperspectieven in hoofdstuk 8.
4. Het conceptrapport met de resultaten van het onderzoek is eerst met besproken, voordat het definitieve rapport is uitgebracht aan de opdrachtgever Wim Westerbeek. Dit is conform de overeengekomen werkzaamheden in de opdrachtbevestiging. De afbakening in de opdrachtbevestiging zoals vermeld in paragraaf 2.3 is aangehouden.

Wijziging ten opzichte van de opdrachtbevestiging
In tegenstelling tot subvraag 8 in paragraaf 2.2 van de opdrachtbevestiging hebben we niet onderzocht of functiescheiding blijkt in Layer7. Dit is ten gevolge van het feit dat Layer7 nog niet operationeel is. We hebben ons daarom beperkt tot hetgeen verteld is gedurende de interviews ten aanzien van de geplande functionaliteiten van Layer7, alsmede het analyseren van de autorisatiematrix. De autorisatiematrix zal namelijk één op één overgenomen worden in Layer7. De andere subvragen uit paragraaf 2.2 zijn wel aangehouden conform de opdrachtbevestiging.

9.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

9.3 Verspreiding rapport

De opdrachtgever, Hoofddirecteur Financiën & Services DUO, Dhr. Wim Westerbeek, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op www.rijksoverheid.nl.

10 Ondertekening

Groningen, 31 oktober 2021

Auditmanager
Auditdienst Rijk

Bijlage: managementreactie

Zie volgende pagina.

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Directie
OVG en CIO

Afdeling
MT-OVG en CIO

Contactpersoon

Datum
31 oktober 2021

Bijlagen
-

memo

Managementreactie rapportage functiescheiding OVG Toekennen

Beste

Allereerst onze dank voor het verrichte onderzoek en de geschetste aanbevelingen. De resultaten van het onderzoek laat zien dat DUO al veel heeft bereikt op het terrein van het beheersen van autorisaties en de implementatie van de nieuwe RBAC-werkwijze. We zijn er echter nog niet helemaal waar het gaat om het geborgd hebben van de noodzakelijke functiescheiding. De verzameling aan te verstrekken autorisatie mogen niet het volledig en juist scheiden van de functies doorbreken. DUO verwacht dat genoemde nog op te lossen issues niet specifiek zijn voor het onderzoeksgebied van de product/dienst SF toekennen en gaat DUO breed maatregelen treffen om volledig in-control te zijn.

De conclusie uit het rapport zijnde "Functiescheiding is in de praktijk geborgd echter de onderliggende visie, het beleid en de AO waar de functiescheiding is beschreven ontbreken" is herkenbaar doch ook opmerkelijk. Het geeft aan dat we wel het belang onderkennen, daar ook daadwerkelijk maatregelen op treffen echter dat we die niet aantoonbaar in de opzet hebben beschreven.

Het onderzoek geeft ons concrete houvast om vervolgstappen te zetten. In de onderstaande tabel is opgenomen wat doe in welke mate doet met de aanbevelingen:

Nr.	*Aanbeveling*	*Opvolging*	*Wanneer/ Wie*
1	Beschrijf de opzet van functiescheiding	*Nieuwe versie AO-beleid OCW/DUO*	*Gereed: 2021/11/30 @Procescontrol*
2	Implementeer RBAC zoals bedacht/ definieer rollen eenduidig:		
2a	*Borg dat de 3 nieuwe rollen ook door 3 verschillende personen worden uitgevoerd*	*Aanscherpen voorschrift en uitdragen*	*Gereed: 2022-06-30 @Management*
3	Voer een risicoanalyse uit:		
3a	*Voorkom dat door het principe van integrale klantafhandeling door 1 medewerker de minimaal benodigde functiescheiding*	*Nieuwe versie AO-beleid OCW/DUO*	*Zie 1*

	bij risicovolle taken niet wordt doorbroken		
		Risicoanalyse per product/dienst	*Gereed: uiterlijk 2023-12-31 afhankelijk van schema herijking @(product)Management*
4	Management moet rol pakken:		
4a	*Voorkom een zodanige stapeling van autorisaties a.g.v. verschillende rollen die een medewerker uitvoert dat hij/zij waarde kan onttrekken aan de onderneming*	*Nieuw voorschrift op-/vaststellen*	*Gereed: 2022/02/28 @CISO/IB*
		Controlelijst realiseren m.b.v. L7	*Gereed: 2022/06/30 @Project AB in-control*
		Controleren en bijsturen 1e lijn	*Gereed: 2022/12/31 @Management*
4b	*Monitor periodiek de functionele logging*	*Nieuw voorschrift op-/vaststellen*	*Gereed: 2022/02/28 @CISO/IB*
		Controlelijst realiseren	*Gereed: 2022/06/30 @Project AB in-control*
		Controleren en bijsturen 1e lijn	*Gereed: 2022/12/31 @Management*
4c	*Ontheffingen om een functiescheiding te doorbreken vindt niet via het formele proces plaats*	*Bijsturen dat voor ontheffingen Topdesk wordt gebruikt*	*Gereed: 2021/12/31 @Management*
		Ontheffingen functionaliteiten in Teamapp z.s.m. uitzetten	*Gereed: 2021/12/31 @mBV/Bicc*
5	Overige:		
5a	*Niet alle autorisaties zijn zelf verklarend; bv: "Werkbakken"*	*Wijzig de autorisatie in een zelf verklarende term*	*Gereed: 2022/06/30 @Roleigenaar OVG*
5b	*Herstel foutief werkende functionaliteit m.b.t. wijzigen en fiatteren van normen*	*Zorg ervoor dat als de autorisatie van degene die wijzigt gescheiden is van degene die fiatteert, dat de applicatie dit ook borgt.*	*Gereed: 2022/06/30 @PO OVG*
5c	*Nagenoeg alle medewerkers bij OVG/toekennen zijn geautoriseerd om te mogen raadplegen*	*Herijk de gedefinieerde rollen en bijbehorende autorisaties*	*Gereed: 2022/12/31 @Roleigenaar OVG*
5d	*Autorisatiematrices worden opgesteld in Excel;*	*Deze werkwijze passen we niet aan; de Excel*	*N.v.t.*

	wijzigingen zijn daardoor niet te volgen	*sheets worden op een specifieke plaats beheerd*	
5e	*Ontbreken aansluiting functies in functiehuis en rollen*	*Deze werkwijze passen we niet aan; bewuste keuze om deze te ontkoppelen; de formele functies in de P-administratie sluiten niet altijd aan op de werkelijke situatie*	*N.v.t.*

Besluitvorming over de opvolging vindt plaats via de lopende stuurgroep Autorisatiebeheer in-control naar het DO/sponsorgroep Autorisatiebeheer in-control. Een deel van de aanbevelingen betreffen te ondernemen acties in de lijn, Het monitoren van de opvolging van de aanbevelingen geschiedt langs de reguliere P&C cyclus.

Met vriendelijke groeten,

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00