Auditdienst Rijk
Ministerie van Financiën

-

Onderzoeksrapport
Interne Beheersing PVS stap 4.3.2 Innen

Definitief

Colofon

Titel	Interne Beheersing PVS stap 4.3.2 Innen
Uitgebracht aan	Hoofddirecteur Bedrijfsvoering en Directeur Onderwijsvolgers en Manager Innen
Datum	3 maart 2017
Kenmerk	2017-0000035997

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Samenvatting

DUO voert tussen 31 mei 2016 en medio juni 2016 de implementatie PVS van stap 4.3.2 voor SF Innen uit. Het voornemen is daarbij ook alle Innen-processen vast te leggen, vast te stellen en te publiceren in Mavim op het AO-portaal van DUO. Belangrijk onderdeel zijn de beheersmaatregelen voor de diverse processen.

De aanleiding voor dit onderzoek is gelegen in de omzetting van het systeem voor de bekostiging van instellingen naar een componentenstructuur in het verleden. Die omzetting heeft voor complicaties gezorgd qua aantoonbaarheid van de interne beheersingssystematiek voor de Algemene Rekenkamer. DUO wil dit voorkomen bij PVS. Een goede beheersing van processen is derhalve van invloed op de kwaliteit en het imago van DUO.

Naar aanleiding hiervan hebben de Hoofddirecteur Bedrijfsvoering DUO en de directeur Onderwijsvolgers aan ADR/Regio, in de rol van interne audit DUO, gevraagd inzicht te verstrekken in de voorgenomen beheersmaatregelen om, waar nodig, deze te verbeteren en er lering uit te trekken voor de toekomst.

Deze samenvatting geeft antwoord op een drietal onderzoeksvragen. Ons overallbeeld is:

Interne beheersing PVS verdient aandacht

In de rapportage zelf gaan we dieper in op de belangrijkste bevindingen. Dit doen we omwille van leesbaarheid niet meer per vraag maar geclusterd per item.

1. Welk proces heeft DUO ingericht om de gewenste controles/beheersmaatregelen vast te stellen en te implementeren? (subvraag: welke risico's onderkent DUO?)

Het beeld van beheersmaatregelen is fragmentarisch te noemen, er is geen centrale plek of document waar de beheersmaatregelen in totaliteit inzichtelijk zijn. DUO heeft geen proces ingericht om de beheersing vast te stellen en te implementeren. In een opgestelde risicoanalyse zijn kwaliteitseisen benoemd. De benoemde beheersmaatregelen lijken soms een eenmalig karakter te hebben en moeten deels nog geïmplementeerd worden.

2. Welke geprogrammeerde en handmatige controles/beheersmaatregelen heeft DUO ingebouwd die waarborgen dat het Inningsproces juist, tijdig, volledig en rechtmatig kan worden uitgevoerd? (subvraag: op welke manier zijn beheersmaatregelen aantoonbaar / inzichtelijk?)

Door het ontbreken van dit overkoepelend en centraal toegankelijk overzicht van beheersmaatregelen is het lastig om een volledig beeld te krijgen van de beschikbare beheersmaatregelen. Dit geldt niet alleen voor ADR maar kan vanuit managementoptiek niet anders zijn. De beheersmaatregelen zijn niet beschreven in procesbeschrijvingen. Ook is geen vastlegging gemaakt van de aanwezige applicationcontrols.
Met de conversie van WSF-oud naar SFS met stap 4.3.2 heeft DUO zelf vastgesteld dat de gegevens juist in SFS zijn verwerkt en dat de werking van het

SFS op dat moment juist is. Daarmee is niet geborgd dat de werking in de toekomst zo blijft.

Wij zien nog aandachtspunten op het gebied van:
- Applicationcontrols
- Changemanagement
- Medewerkersautorisaties inclusief functiescheidingen
- Logging en monitoring.

Toegang vanuit de externe omgeving met behulp van DigiD verloopt beheerst.

De hoge werkdruk bij de beheerders, als gevolg van nazorg op stap 4.3.2 en voorbereidingen op stap 5, en beperkte capaciteit van ketenmonitoring is van invloed op de kwaliteit van de interne beheersing. De kwaliteitscontrole, die daarnaast wordt uitgevoerd, staat in de kinderschoenen en moet nog verder ontwikkeld worden. De hulp van beheerders is hierbij noodzakelijk.
De hoge werkdruk vormt daardoor tevens een risico voor de uitvoering van controles alvorens te komen tot verantwoordingen. Met behulp van een track and trace ID is het mogelijk om individuele mutaties te volgen. Dit track and trace ID werkt overigens alleen binnen SFS. Hierdoor is niet duidelijk of er mutaties tussen wal en schip vallen. Een onderzoek van DUO naar de volledigheid van verwerking, waaronder track en trace, loopt nog.

3. Welke restrisico's kunnen worden onderkend en welk 'early warning' signalen voor verdere ontwikkeling en bouw richting DUO kunnen mogelijk worden afgegeven?

Het belangrijkste risico is dat, doordat de controle / beheersing niet sluitend is en er geen centraal totaalbeeld aanwezig is, de kans bestaat dat zaken tussen wal en schip vallen. Een mutatie komt wel binnen maar leidt niet of niet tijdig tot een juiste en volledige inning. Daarmee is de rechtmatigheid in het geding.

Een tweede risico ligt op het vlak van de vastlegging en aantoonbaarheid van de beheersmaatregelen. Op de huidige wijze is niet vast te stellen en niet aantoonbaar te maken dat het proces in control is. Dit heeft niet alleen interne consequenties, maar ook in de richting van de verantwoording en externe toezichthouders als de wettelijke accountant en de Algemene Rekenkamer die in opdracht van de Minister toezicht houden.

Belangrijke aanbeveling is dat de beheersmaatregelen in opzet en werking beter gedocumenteerd moeten worden en risicogericht ontworpen/bekeken dienen te worden op onderlinge samenhang en consistentie met als uitgangspunt "het geheel is meer dan de som der delen".

1 Beheersmaatregelen niet in Mavim beschreven

1.1 Procesbeschrijvingen in Mavim hebben hoog abstractieniveau

De procesbeschrijvingen bevatten vrijwel geen beschrijvingen van de beheersmaatregelen. De Adviseur AO bevestigde dit en ook de Manager sturing heeft dit niet weerlegd. Zo noemt de beschrijving "opstarten inningstermijn" de te doorlopen stappen bij de start van de inningstermijn. Daarbij is het doel te beslissen over alle mutaties in de inningsfase die mogelijk resulteren in een (herziening van een eerdere) inningsbeschikking. Niet duidelijk is hoe blijkt dat *alle* mutaties zijn betrokken.
Werkzaamheden worden of geautomatiseerd of door een Medewerker Klantbediening uitgevoerd. De beschrijving maakt niet duidelijk of er een 4-ogenprincipe is of dat een 2e medewerker verifieert.

1.2 Uit werkinstructies blijken geen beheersmaatregelen

De werkinstructies in de kennisbank gaan hier niet op in (zoeken op begrippen als "innen" en "opstarten inningsproces" hebben geen resultaat).

1.3 Risico's zijn in kaart gebracht

De risicoanalyse op het proces is van continue aard. De gebruikte kwaliteitseisen zijn tijdigheid, juistheid en betrouwbaarheid[1]. Als een studieschuld 3 dagen te laat wordt geïnd levert dat een positieve beoordeling op het aspect volledigheid op en een negatieve op het aspect tijdigheid.

Voor alle onderkende risico's geldt een "risico vermijden" strategie. Er zijn geen risico's die geheel worden geaccepteerd. De benoemde beheersmaatregelen lijken soms een eenmalig karakter te hebben, gericht op inrichting. Als voorbeelden:

- De autorisatiematrix is actueel en volledig doorgevoerd; Maatregel: matrix stap 4.3 is gevuld op basis van medewerkersprofielen. Onduidelijk is de bewaking op juiste, volledige en tijdige doorvoer van mutaties.
- Alle bedrijfsregels zijn actueel en worden juist ingevoerd; Maatregel: interpretatieverschillen in test worden gerepareerd. Continue cyclus inbedden in regulier change proces. Daarmee is niet duidelijk hoe dit nu daadwerkelijk is geborgd.
- Studieschulden worden tijdig geïnd; Maatregel: uitval in betaalproces moet tijdig worden gesignaleerd. DWH rapportage moet nog worden ontwikkeld. De maatregel is dus nog niet geïmplementeerd.

De risicoanalyse van Informatiebeveiliging en BCM signaleerde dat:

- Het track&trace mechanisme is nog niet volledig geïmplementeerd: de audittrail geeft geen informatie om eenduidig uit te sluiten dat alle aangevraagde transacties leiden het vooraf gedefinieerd einde.
- Bij descoping van stap 5 is schoning (=selectie en vernietiging) naar stap 6 verschoven. Deze valt zo buiten de programma scope wat kan leiden tot afstel. Zolang dit niet is geregeld is DUO niet compliant.

1 Betrouwbaarheid is vanuit auditperspectief: juistheid, volledigheid en tijdigheid

1.4 Requirements zijn gedocumenteerd

Requirements zijn in kaart gebracht en gedocumenteerd. Nog niet duidelijk is hoe geborgd is dat de requirements in tact blijven en hierop geen inbreuk plaatsvindt. De requirements zijn nog niet volledig ingericht. Een aantal zaken is nog in ontwikkeling of de goede werking er van moet nog worden vastgesteld. Wij verwachtten dat een proces is ingericht dat borgt dat de requirements juist en tijdig worden ingevoerd en dat er alleen geautoriseerde wijzigingen plaatsvinden. Dit proces hebben wij niet aangetroffen.

2 Conversie 4.3.2 goed verlopen

2.1 Functionaliteit SFS werkt op moment van conversie

DUO heeft gekozen voor een conversiestrategie waarbij de business rules "aan" staan, d.w.z. dat data in PVS wordt geplaatst zoals het in de normale situatie ook gaat. Voordeel hiervan is dat data correct en consistent in de doeldatabase terechtkomt. De aansluiting tussen de eindsituatie in ILS en de beginsituatie in SFS is gemaakt. Daarmee kan geconstateerd worden dat de functionaliteit in SFS op moment van conversie werkte.
Hieruit kan niet geconcludeerd worden dat de functionaliteit na de conversie blijvend geborgd is.

2.2 Relatief weinig uitval tijdens conversie

De conversie was gestructureerd opgezet en de resultaten waren zoals verwacht in de proefconversies. Er was relatief weinig uitval tijdens de conversie. De uitval die is opgetreden was vooraf bekend en was traceerbaar naar individuele gevallen.

3 Controles in automatiseringsomgeving voor verbetering vatbaar

3.1 Weinig zicht op applicationcontrols

Binnen PVS is geen eenvoudig toegankelijke beschrijving aanwezig van applicatiecontroles. In gesprekken is aangegeven dat er wel op diverse punten bepaalde validatiecontroles en andere checks zijn ingebouwd, maar dat deze niet op een centrale plek inzichtelijk zijn.

3.2 Medewerkerautorisaties ruim belegd

De PVS-WIKI bevat een autorisatiematrix die na afloop van de vorige conversie is opgeleverd. Wij hebben deze matrix vergeleken met de werkelijke inrichting van SFS en deze is niet in alle gevallen overeenkomstig. De procesregisseurs geven aan dat de autorisatiematrix nog niet bijgewerkt is. Naar aanleiding van de conversie zijn nog een aantal transacties/werkbakken toegevoegd aan rollen.

De beheerders hebben, gezien de inrichting SFS, de meeste rechten in de applicatie en ook meer dan strikt genomen noodzakelijk. Dit heeft volgens de procesregisseurs te maken met de opstartfase van SFS. In de toekomst zullen de rechten van de beheerders worden beperkt tot enkel beheertransacties. Alle productietransacties worden dan ingetrokken voor de beheerders. Een beheerder geeft aan dat onder de beheerders de mondelinge afspraak is gemaakt dat ze geen productiemutaties verrichten, maar dat hier niet extra op gecontroleerd wordt.

De afdeling Beveiliging heeft een overzicht opgeleverd met de verschillende autorisaties per medewerker waaruit blijkt dat aan een aantal rollen, naast losse autorisaties, ook functieprofielen zijn gekoppeld. Dit betekent dat alle medewerkers binnen dat profiel automatisch rechten verkrijgen in SFS. Uit een korte analyse blijkt dat er momenteel medewerkers rechten hebben in SFS die ze uit hoofde van hun functie niet hoeven te hebben.
De procesregisseur geeft aan hier naar te kijken. Aan de hand van het "overzicht medewerkers OVG" zal worden gecheckt of de autorisaties van medewerkers die geen toegang behoren te hebben ingetrokken kunnen worden.

3.3 Functiescheiding niet volledig

In SFS is functiescheiding op verschillende manieren ingericht:

- Ongeveer 80 à 90% van de aanvragen/wijzigingen verloopt als STP op basis van businessrules (bedrijfsregels) en zonder handmatige actie. Het Bedrijfsregelsteam stelt ze op in samenspraak met Beleid dat ze fiatteert voor de procesregisseurs om daarmee te voldoen aan geldende wet- en regelgeving.
- Het opvoeren en fiatteren van normen is belegd in twee aparte transacties. Wettelijke normen bepaalt het ministerie (vb. hoogte basisbedrag SF). Verder bestaan productiebesturingsnormen (bv. Hoe vaak draait een batch). Voor de laatste is minder controle nodig. Daarom willen de procesregisseurs deze soorten normen scheiden. Momenteel kan het opvoeren van normen plaatsvinden door de rollen Sturing en Beheer en het fiatteren door de rollen Sturing Specifiek en Beheer. Doordat Beheer beide transacties kan uitvoeren is functiescheiding niet in

zijn geheel van toepassing. Tevens zijn er twee medewerkers die zowel de rol Sturing als Sturing Specifiek hebben, waardoor ook hier de functiescheiding wordt doorbroken.

- Voor bepaalde financiële transacties (vb. uitbetalen grote bedragen) is tevens een 4-ogen controle ingesteld. Bij uitvoering van deze transacties komen de mutaties in de werkbak '4-ogen controle betalingsverkeer' terecht. Eén van de procesregisseurs geeft aan dat in theorie een medewerker zijn eigen mutatie zou kunnen fiatteren.

3.4 Changemanagement wijkt af van standaard DUO-wijze

Het changeproces specifiek bij PVS wijkt af van het gewone DUO-proces. PVS is opgepakt als een programma waarbij alle wijzigingen niet door beheer in de lijnorganisatie worden uitgevoerd, maar door de teams binnen het programma. Het changeproces is beschreven in een changemanagementstrategie, een werkinstructie en een sjabloon aan de hand waarvan wijzigingen kunnen worden aangevraagd.

Incidentenafhandeling

Incidenten worden (vanuit het onderhoudsbudget) via de lijn opgepakt evenals functionaliteiten die beter kunnen ("Improvement"). Grotere wijzigingen (zoals nieuwe opdrachten) pakt het programma op. Registratie van incidenten gaat in Topdesk. Zodra het een softwarewijzigingen/softwarevraag betreft wordt het overgezet naar Jira.

Normentabel

Het beheer van de normentabel gaat via het reguliere proces met een aparte fiatteringtransactie (met functiescheiding). Voor het wijzigen in de productie-omgeving (datamanipulatie) geldt de *mondelinge* afspraak dat de proceseigenaar alle wijzigingen goedkeurt en het akkoord vastlegt. Dit is in principe controleerbaar. Wij hebben niet vastgesteld of een controle is ingericht waarmee vastgesteld kan worden of dit daadwerkelijk en volledig gebeurt. De afspraken bij datamanipulaties zijn DUO breed.

Changes

Momenteel wordt gewerkt met een combinatie van DevOps en Prince 2. Dit vanwege het huidige onderscheid tussen programma en lijn. Er wordt naar toegewerkt dat ontwikkelde functionaliteiten na iedere sprint (3 weken) in productie worden genomen ("continuous delivery"). Dit kunnen zowel bugfixes als wijzigingen uit het releaseprogramma (stap 5) zijn. De zaken die op dat moment nog niet gebruikt worden (stap 5 specifiek) worden dan tot de grote implementatie van stap 5 "uit" gezet.

Testproces

Het testproces bestaat (in opzet) uit verschillende fases en wordt in zijn geheel vastgelegd in Jira:

- RIT (realisatie- en integratietest)
    - Gebeurt in de FAT-omgeving
    - Bij de integratietest worden alle wijzigingen van alle teams getest, waardoor wordt gekeken of de wijzigingen in de verschillende PVS applicaties in totaliteit correct zijn doorgevoerd.
    - Er worden ook dagelijks geautomatiseerde regressietesten op applicatieniveau uitgevoerd.
    - Alle PVS applicaties, het gegevensmagazijn en het portaal worden hierin getest.
    - Er wordt een functioneel akkoord gegeven door de productowner(s).
- GAT (Gebruikers Acceptatie Test)

    - Gebeurt in de GAT-omgeving.
    - Hierbij wordt ook meteen de BAT (beheer acceptatie test) getest.
    - Wordt uitgevoerd door de gebruikers.
- EXP (Exploitatietest)
    - Gebeurt in de EXP-omgeving.
    - Wordt uitgevoerd door Functioneel Beheer en Technisch applicatie Beheer, maar met name FB.
    - Hierbij worden ook hacktesten en performancetesten uitgevoerd, deze staat standaard opgenomen in het draaiboek en worden uitgevoerd indien noodzakelijk.
- PRD (Productie)
    - OPS en TAB zetten de nieuwste versie in productie.
    - Vrijgave wordt gegeven door de proceseigenaren.
    - Er wordt een productie acceptatie test uitgevoerd.

Testcriteria

Vooraf worden afspraken gemaakt over welke zaken als blokkerend kunnen worden gezien:

- Critical & blockers – moeten opgelost worden alvorens in productie wordt gedaan
- Major bevindingen – kunnen ook blokkerend zijn, maar minder zwaarwegend. Er moet dan wel een beeld gegeven worden wanneer deze zijn opgelost (zie ook 'Changes').

Bij een grote implementatie moet er ook fysiek getekend worden voor vrijgave naar productie. De werking van het testproces hebben wij niet vastgesteld.

3.5 Toegang door derden gecontroleerd

Studenten / scholieren hebben toegang tot SFS middels DigiD of SMS-verificatie. Dit proces verloopt gecontroleerd en leidt niet tot incidenten. Een jaarlijks onderzoek naar DigiD brengt geen extra risico's aan het licht.

3.6 Monitoring en logging behoeven aandacht

Vanuit Procescontrol hebben wij begrepen dat nog niet duidelijk is welke controles en of welke systeemlijsten er zijn in SFS. Uit de gesprekken komt het beeld naar voren dat de aandacht bij de tijdige in productiename lag en niet bij beheersmatige aandachtspunten als beheer, kwaliteit en monitoring.

Vanuit SFS wordt dagelijks een extractie in DWH gezet. Met behulp van de tool Disco wordt op basis van de logging informatie verzameld over de input, straight through processing (STP) en uitworp. Hierover wordt gerapporteerd.
Deze rapportage wordt gemaakt voor de doelgroep debiteuren, MBO 1&2, reisrecht MBO 18-.
Logging vindt plaats op performance, applicatie en proces. Logging vindt plaats bij Beheer.
Monitoring van error-queues schiet er soms bij in.

In SFS zijn verschillende "wekkers" ingebouwd. Hierover wordt gerapporteerd.

Zie ook onder Kwaliteitscontrole.

4 Kwaliteitscontrole is in oprichting

4.1 Kwaliteitscontrole wordt ontwikkeld

In opzet is kwaliteitscontrole belegd bij Procescontrol. Deze afdeling is gevraagd om een plan van aanpak voor de uit te voeren controles op te stellen dat inzicht moet geven in risicovolle transacties, te controleren aspecten en aantallen / percentages.
Omdat kwaliteitscontroles nog in ontwikkeling zijn, worden ze nog nauwelijks uitgevoerd. Op moment is niet bekend welke controles en/of welke systeemlijsten er zijn in SFS. De aparte controletransacties zoals die bestonden in de oude applicatie zijn nu niet ingebouwd.
Met monitoring moet er achter worden gekomen hoe SFS werkt. De controle wordt vooralsnog gericht op handmatige handelingen van de medewerker. Er is nu nog te weinig "uitworp" uit het geautomatiseerde proces om invulling te geven aan een controle.

5 Aandachtspunten bij verantwoording

5.1 Verantwoording / controles beïnvloed door werkdruk

Door medewerkers ketenmonitoring worden wekelijkse en maandelijkse rapportages opgeleverd. Hierbij wordt gebruik gemaakt van standaard rapportages van het BIC. De volledigheid en betrouwbaarheid van de gerapporteerde gegevens wordt door de medewerkers ketenmonitorig geverifieerd met behulp van queries, het gebruik van Disco en de error queues. Disco is gebaseerd op de proceslog.
Queries worden uitgevoerd door Beheer. Uit de gesprekken komt naar voren dat de werkdruk bij Beheer erg groot is. Hierdoor kan het voorkomen dat in de prioritering zaken niet tijdig uitgevoerd kunnen worden of vervallen. Daarnaast ligt het (politieke) accent bij PVS niet op beheer maar op het realiseren van functionaliteit op een vaste datum.

Ook bij ketenmonitoring is sprake van onderbezetting. Hierdoor hebben de medewerker hun handen vol aan de reguliere werkzaamheden en is er geen ruimte om te kijken naar verbetermogelijkheden of tooling.

5.2 Track and Trace is niet sluitend

Binnen DUO is de vraag gesteld of het mogelijk is om vast te stellen dat alle transacties goed en volledig tot output worden verwerkt. Deze vraag is nog niet positief beantwoord. Er zijn plaatsen in het proces waarbij de mogelijkheid bestaat dat transacties uit het zicht blijven ("blinde vlekken"). Er is nog niet aangetoond dat zaken zijn verdwenen. Nader onderzoek loopt nog.
Aan de hand van het geïmplementeerde track and trace ID is het mogelijk om individuele gevallen aan de hand van dit track and trace ID te volgen. Het track and trace werkt alleen zolang er geen interactie buiten SFS plaatsvindt. Op moment dat gegevens opnieuw worden aangeboden wordt een nieuw track and trace ID aangemaakt. De aansluiting met een "vorige track and trace ID" kan niet gemaakt worden.
De vraag hoe OVG zeker weet dat er geen zaken tussen wal en schip vallen kan (nog) niet beantwoord worden.

5.3 FPB-controles niet wezenlijk veranderd

De basis voor de controles van FPB is voor PVS/SFS is niet wezenlijk anders dan ten tijde van ILS. De ontvangsten via de bank, de koppeling aan het artikel en de mutaties op vordering debiteur is qua controle en grootboekinrichting vergelijkbaar met bijv. ILS. Bij PVS is de focus vanuit o.a. FPB dan ook geweest om de mutaties en standen en de basis voor de journalisering vanuit de "ruwe"gegevens vanaf start juist en volledig te krijgen. FPB is ook betrokken bij het analyse- en testproces. Er is een controlestelsel dat staat beschreven in procesbeschrijvingen en werkinstructies.

De aansluiting/controle bestaat uit:
- Ruwe gegevens SFS à Journalsering à FAS/FMS
- Ruwe gegevens/logging SFS à ETL/DWH à DWH rapportage

Belangrijk is dat DWH enkel managementinformatie genereert en geen financiële trigger heeft. Aansluitingen tussen DWH en FAS/FMS worden gemaakt, maar

daar zitten afwijkingen in door registratiedatum en rapportagedatum. FAS/FMS is de basis voor de jaarrekening, niet de gegevens uit DWH.

In opzet is vastgesteld dat FPB geen niet-financiële transacties kan uitvoeren in SFS.

6 Aanbevelingen en/of vervolgstappen

Gelet op het voorgaande is het evident dat de beheersmaatregelen verbeterd moeten worden. Het is van belang om zicht te hebben op het totale palet van beheersmaatregelen, zodat zekerheid bestaat dat het proces in control is en niets tussen wal en schip valt. Door de opzet van de beheersmaatregelen goed te documenteren is enerzijds bekend waar en hoe de controles worden uitgevoerd, en is anderzijds in geval van proceswijzigingen inzichtelijk wat de impact is voor de betreffende beheersmaatregelen.
Daarnaast is het van belang om de werking van de beheersmaatregelen aantoonbaar vast te leggen, zodat je kunt terugvallen op uitgevoerde controles. Bij calamiteiten is dan vast te stellen vanaf welk moment deze optreden of tot welk moment de calamiteit niet optrad. Zowel voor het afleggen van verantwoording (accountability), als voor de wettelijke accountant of de Algemene Rekenkamer is het van belang dat de werking van de beheersmaatregelen aantoonbaar is.

Concreet betekent dit dat:

- de beheersmaatregelen in opzet en werking beter gedocumenteerd moeten worden. Ze dienen daarbij tevens risicogericht ontworpen/bekeken te worden op onderlinge samenhang en consistentie met als uitgangspunt "het geheel is meer dan de som der delen";
- de te ruime autorisaties en overbrugging van functiescheiding zo snel als mogelijk te beperken;
- de beheerfunctie dusdanig in te richten dat deze niet alleen de monitorende taak kan uitvoeren maar ook de controletaak naar behoren kan faciliteren;
- de analyse naar de "witte vlekken" in het beheersproces te gebruiken om uitsluitsel te geven over de mate van volledigheid om het proces te volgen en over of het track & trace ID voldoende houvast biedt als maatregel bij externe uitwisselingsprocessen.

7 Verantwoording onderzoek

7.1 Werkzaamheden en afbakening

Het doel van het onderzoek is inzicht geven in de opzet van de getroffen beheersmaatregelen. Daarnaast wil DUO leerpunten uit dit traject halen.
Het onderzoek is hiermee niet gericht op het geven van zekerheid (Assurance).
Het object van onderzoek bestaat uit de stappen die zijn doorlopen om te komen tot het vaststellen van de gewenste implementatie van de te treffen beheersingsmaatregelen en de gekozen maatregelen zelf.

Het onderzoek is gebaseerd op de volgende onderzoeksvragen:

1. Welk proces heeft DUO ingericht om de gewenste controles/beheersmaatregelen vast te stellen en te implementeren? (subvraag: welke risico's onderkent DUO?)
2. Welke geprogrammeerde en handmatige controles/beheersmaatregelen heeft DUO ingebouwd die waarborgen dat het Inningsproces juist, tijdig, volledig en rechtmatig kan worden uitgevoerd? (subvraag: op welke manier zijn beheersmaatregelen aantoonbaar / inzichtelijk?)
3. Welke restrisico's kunnen worden onderkend en welk 'early warning' signalen voor verdere ontwikkeling en bouw richting DUO kunnen mogelijk worden afgegeven?

Onderzoeksaspecten betreffen:

- Inrichting van het Innenproces (w.o. applicatie controles);
- Onderzoek en (impact)analyse om te komen tot gewenste beheersmaatregelen;
- Implementatie van de beheersmaatregelen.

Om te kunnen voorzien in een juist, volledig en tijdig inningsproces en risico's te beperken dienen beheersmaatregelen ingericht te worden die dit waarborgen. De volgende onderdelen zijn van belang:

- Uitgevoerde risicoanalyse
- Invoeren en up-to-date zijn van Business Rules
- Wijzigingen tabellen (i.h.k.v. grondslagen)
- Handmatige mutaties
- Autorisaties
- Wisselwerking proces Innen en proces Toekennen
- Opleiding en instructie medewerkers
- Misbruik en oneigenlijk gebruik (M&O)
- Geprogrammeerde controles
- Logging en monitoring

Het onderzoek richt zich op de opzet van de beheersmaatregelen van het proces Innen in stap 4.3.2 van PVS. Ook worden de applicatiecontroles tot de scope gerekend. Buiten deze scope vallen:

- Bestaan en werking van de maatregelen;
- De conversie van de oude naar de nieuwe applicatie;
- De technische/infrastructurele maatregelen (de zgn. general IT-controls);
- De kwaliteit van inhoud en omzetting van wet-en regelgeving;
- Projectbesturing en projectkosten.

Wij hebben procesbeschrijvingen en werkinstructies bestudeerd. Vervolgens hebben wij diverse medewerkers gesproken om te achterhalen welke beheersmaatregelen zijn geïmplementeerd. Dit heeft meer doorlooptijd gekost dan aanvankelijk verwacht.

7.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd.

7.3 Verspreiding rapport

De opdrachtgever, Hoofddirecteur Bedrijfsvoering en Directeur Onderwijsvolgers, zijn eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de 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 de website.

8 Ondertekening

Groningen, 3 maart 2017

Auditmanager ADR-Regio

Bijlage: managementreactie

DEFINITIEF
ADR

Directie
OVG
Afdeling
Sturing
Datum
15-2-2017
Bijlagen

memo

Managementreactie op Onderzoeksrapport interne beheersing PVS stap 4.3.2 d.d. 7 november 2016

Hierbij ontvangt u de managementreactie op het onderzoeksrapport interne beheersing PVS dat is uitgevoerd op stap 4.3.2.

Algemene reactie
Het beeld dat het onderzoeksrapport oproept is dat de interne beheersing fragmentarisch is en dat het daarom moeilijk is het volledige beeld op te bouwen van de beschikbare beheersmaatregelen. Aangegeven wordt dat de druk op de beheerorganisatie in de overgangsfase van de ontwikkeling en afronding van het programma en het beheren en beheersen van hetgeen al in productie staat van invloed is op de kwaliteit van de beheersing.

DUO herkent het beeld van de druk op de beheerorganisatie in de combinatie van beheer en afronding van het programma en onderkent dat er op de interne beheersing nog een aantal stappen te zetten zijn. Tegelijkertijd is DUO van mening dat er meer is ingericht op de interne beheersing dan naar boven is gekomen ten tijde van het onderzoek. De betrokken kennishouders die geselecteerd zijn op basis van de onderzoeksvraag verdient aandacht bij de onderzoeken in de toekomst in verband met de spreiding van kennis over meerdere specialismen.

DUO heeft het rapport ter harte genomen door via een additioneel eigen onderzoek de beheersmaatregelen te inventariseren en inzichtelijk te maken en 'witte vlekken' in kaart te brengen zodat verdere maatregelen genomen kunnen worden. Resultaten van dit onderzoek zijn gedeeld en besproken in een workshop op 6 februari met alle direct betrokkenen en in aanwezigheid van de IAD en ADR. Dit om een volledig beeld (inzage en nuance) te geven op de stand van zaken en aanbevelingen en 'early warnings' uit het rapport. Voor DUO zijn de gepresenteerde resultaten tijdens deze workshop bepalend voor het verder op orde krijgen van de interne beheersing.

In deze managementreactie wordt ingegaan op individuele bevindingen uit uw rapport en de aanbevelingen die zijn gedaan.

Opvolging van bevindingen

Het abstractieniveau van de procesbeschrijvingen in Mavim:

De procesbeschrijvingen van DUO in Mavim voldoen aan de richtlijnen voor het opstellen van AO van FEZ OCW. Daarmee voldoen wij aan de norm die DUO zichzelf gesteld heeft. Op detailniveau gaat DUO een stap verder omdat vanuit de procesbeschrijvingen in Mavim doorgelinkt wordt naar de detailbeschrijvingen in Magicdraw. Omdat voldoen aan een norm nooit een doel op zich kan zijn, gaat DUO de komende tijd de waardering van de SFS-gerelateerde procesbeschrijvingen in Mavim verder laten onderzoeken. De uitkomsten van dat onderzoek willen we gebruiken om de procesbeschrijvingen -zo nodig- nog meer te verbeteren.

Vastlegging van het 4-ogenprincipe:

Voor SFS is op grond van een risicoafweging per medewerkershandeling in het SFS-systeem bepaald of deze een 4-ogenprincipe vereist. Dit kenmerk leggen we vast bij de medewerkershandelingen waarbij dit wel wordt vereist. Ligt vast in de ontwerpen van PVS en wordt door vertaald naar de autorisatiematrix.

Beschrijvingen van beheersmaatregelen:

Het klopt dat Mavim en de Kennisbank nauwelijks beschrijvingen van beheersmaatregelen bevatten. Wel worden beheersmaatregelen beschreven op diverse wiki's. Door de huidige mate van verandering in de DUO-organisatie, beheerinrichting, gebruikersorgaan en de middelen, vinden wij wiki's, zeker op dit moment, vanwege de laagdrempeligheid, één van de juiste plekken om beheersmaatregelen vast te leggen. Deze beschrijvingen zijn, voor de bedoelde doelgroep, zelfstandig leesbaar.
Wij geven de beheerteams de verantwoordelijkheid om te borgen dat nieuwe beheersmaatregelen op de wiki's worden geplaatst, en dat bestaande beschrijvingen actueel worden gehouden.
Wij laten onderzoeken of er ook op andere plaatsen beheersmaatregelen worden vastgelegd. Afhankelijk van de uitkomst van dat onderzoek zullen we vervolgacties uitzetten die moeten leiden tot bereikbaarheid van gepubliceerde beheersmaatregelen.

Bewaking op de autorisatiematrix:

Voor de bestaande SFS-lijnorganisatie bewaakt het BAT de autorisaties. Er bestaat een autorisatieprotocol en er wordt aangesloten op bestaande afspraken met ICT Autorisaties; informatie hierover is gepubliceerd op de wiki. Hiermee zorgen we ervoor dat alleen op een afgesproken manier wijzigingen in de toegekende autorisaties worden uitgevoerd.
We hebben het BAT gevraagd ook afspraken te maken en vast te leggen die ertoe leiden dat het programma op de hoogte wordt gesteld van relevante, vanuit de lijnorganisatie geïnitieerde wijzigingen op de autorisatiematrix.
Wij hebben naar aanleiding van uw bevinding het SFS BAT-team gevraagd het proces, waar deze afspraken onderdeel van uitmaken, te beschrijven en vast te leggen. Hiermee hebben we vanuit de lijn volgens ons afspraken over een bewaking op de autorisatiematrix in opzet ingericht.
We hebben daarnaast de procesregisseurs gevraagd van het programma te eisen dat impact van wijzigingen vanuit het programma op de autorisatiematrix wordt benoemd in de *release notes*, en dat, in voorkomende gevallen, de gewijzigde autorisatiematrix releasematig wordt opgeleverd.
Hiermee wordt de bewaking op de autorisatiematrix, voor de wijzigingen

vanuit het programma, onderdeel van het normale PVS-releaseproces.

Onduidelijkheid omtrent het borgen van het inbedden van bedrijfsregels in het reguliere change proces:
De manager Expertisecentrum/bedrijfsregelteam heeft al een situatieanalyse opgestart waarmee we deze bevinding willen wegnemen. Wij verwachten dat dit medio april 2017 tot resultaat zal leiden. Wij zullen er op toe zien dat hiermee de bedrijfsregelfunctie wordt ingebed in het wijzigingsproces

DWH-rapportages zorgt voor uitval in het betaalproces:
DWH-rapportages waar DUO om heeft gevraagd zijn ontwikkeld door DWH PVS. We hebben daarbij niet gevraagd om een DWH-rapportage voor het signaleren van uitval bij betalingen. Wij verwachten dat het signaleren van uitval in het betaalproces niet via DWH-rapportage (achteraf) maar "direct" plaatsvindt door de bewaking van het betaalproces zelf. Dit proces is beschreven en geborgd in de procesgang van het Payment Service Centre (PSC).

Afwijkingen aansluiting DWH en FAS/FMS:
Nader onderzoekt leert dat er geen onverklaarbare verschillen meer zitten tussen DWH en FAS/FMS. Deze informatie hebben wij ondertussen ook met u gedeeld.

Het ontbreken van een proces dat borgt dat de requirements juist en tijdig worden ingevoerd en dat er alleen geautoriseerde wijzigingen plaatsvinden:
Er zijn meerdere bronnen vanwaar, in het kader van PVS en SFS, requirements gesteld worden. Vanuit de opdrachtgever OCW, en vanuit de eigen DUO-organisatie.
Volgens ons is er wel degelijk een proces ingericht dat ertoe leidt dat de stakeholder OCW kan vaststellen dat de OCW-requirements juist zijn geïmplementeerd. Vanuit het productownerschap van PVS wordt hierover met OCW afgestemd, zodanig dat eventuele wijzigingen op requirements, of op de implementatie daarvan, worden gedocumenteerd en geaccordeerd door OCW.
Een beschrijving van dit proces is niet aanwezig; hiertoe hebben wij ondertussen opdracht gegeven.
De borging van de requirements van de eigen DUO-organisatie vindt plaats in het toets- en testtraject (zoals door uzelf beschreven in paragraaf 3.4 van uw rapport). Dit is een proces dat voor elke oplevering wordt doorlopen. Wij hebben ondertussen wel vastgesteld dat de relatie tussen testscenario's en de requirements niet evident is; wij laten onderzoeken hoe we dit kunnen verbeteren.
De verantwoordelijkheid van de blijvende borging van de requirements is voorts geborgd in de rol van de product owners en de procesregisseurs. Wij zullen in de rolbeschrijving deze verantwoordelijkheid duidelijk benoemen.

Blijvende borging van de functionaliteit:
De blijvend juiste werking van SFS is geborgd in de aansluiting tussen gevraagde werking (functionele en niet-functionele requirements), de juiste uitwerking daarvan in ontwerp (FO's of Use Cases, bedrijfsregelontwerp, sjablonen), de uitwerking daarvan in software (programmatuur en bedrijfsregels) en handmatige handelingen (AO, werkinstructies), de vaststelling van de juiste werking en bruikbaarheid daarvan tijdens het toets- en testproces, én de diverse controles

gedurende de productiefase van het systeem. Deze voortbrengingsketen borgt de juiste, afgesproken functionaliteit. In de rol van de Product Owners ligt de verantwoordelijkheid besloten dat in de toekomst requirements geborgd blijven; hiermee wordt naar onze mening de functionaliteit geborgd.

Applicatiecontroles:
Voor PVS/SFS worden (in elk geval een deel van) de beschrijvingen van applicatiecontroles gebaseerd op het gegevenswoordenboek, en vastgelegd in MagicDraw. Op grond van het Gegevenswoordenboek en het services- en berichtenboek worden in het ontwerp in MagicDraw application controles ingevoegd; vanuit MagicDraw worden hiervan xsd's (die de gegevensdefinitie en validatie bevatten) gegenereerd die in de software worden opgenomen.
Volgens ons zijn dit toegankelijke beschrijvingen, op centrale plekken. We laten op dit moment onderzoeken of applicatiecontroles waarvoor een functioneel proces nodig is, in het ontwerp ervan een kenmerk kan worden meegegeven waaruit blijkt dat het een applicatiecontrole is.

Monitoring van error-queues schiet er soms bij in:
Momenteel is in het team "Voorbereiding" hier de nodige aandacht voor. Wekelijks worden errorqueues geanalyseerd en worden herstelacties bepaald. Veelal betekent dit dat de oorzaak van de error in de werking van de software wordt weggenomen, waarna de berichten op de errorqueues opnieuw ter verwerking worden aangeboden, en dus verwerkt worden.

Het is van belang dat z.s.m. de bewaking en kennis van het uitlezen en duiden van deze queues worden overgedragen naar de lijnorganisatie van DUO. Deze overdracht van kennis vindt momenteel plaats.

Functiescheiding:
Functiescheiding tussen ontwikkelaars en beheerders lijken contrair op de doelstelling van BusDevOps waarbij het juist de bedoeling is dat ontwikkelaars en beheerders bij dezelfde applicaties en omgevingen kunnen om zo de voortbrenging en ontwikkeldynamiek te bespoedigen. De ontwikkelingen op het gebied van DevOps vergen ons inziens aanpassing van het aurorisatiebeleid van Informatiebeveiliging. We hebben in het verleden Informatiebeveiliging gevraagd hun autorisatiebeleid aan te passen en ons te ondersteunen bij de doorvoering hiervan. Dit heeft onvoldoende voortgang. We zullen daarom opnieuw bij Informatiebeveiliging aandringen op aanpassing van het beleid.
Dit issue is overigens niet enkel een PVS issue maar speelt DUO-breed en ongetwijfeld ook bij andere organisaties.

DUO onderzoekt hoe andere partijen met deze problematiek omgaan en wil op basis daarvan een richtlijn bepalen.

Conclusie
Wij stellen vast dat de interne beheersing op SFS aan scherpte kan winnen. In de behandeling per bevinding heb ik nuance aan willen brengen in de bevindingen van het onderzoeksrapport en daar waar nodig te treffen maatregelen aan te kondigen. Hiermee is het probleem van de fragmentarisch beschikbare informatie nog niet opgelost. We zullen daarom ons eigen onderzoek vervolgen en tevens de wel beschikbare informatie op een eenduidige manier ontsluiten zodat deze voor alle

betrokkenen toegankelijk is en zelfstandig leesbaar. Daarnaast zijn wij voornemens om het bij uw onderzoeksrapport gehanteerde raamwerk te benutten om ook de witte vlekken, die niet direct in dit onderzoek tot uiting zijn gekomen, op de juiste manier van maatregelen te voorzien.

Met vriendelijke groet,

Namens Directeur Onderwijsvolgers,
Manager Sturing Studiefinanciering

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