Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport Integriteitsmaatregelen Print- en Couverteerstraat DUO

Colofon

Titel	Integriteitsmaatregelen Print- en couverteerstraat DUO
Uitgebracht aan	De opdrachtgever van het onderzoek, de hoofddirecteur DUO,
Datum	16 maart 2023
Kenmerk	2023-0000078305
Referentienummer	2021-OCW-031

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

(Management)samenvatting

De ADR heeft op verzoek van DUO een onderzoek uitgevoerd naar de integriteitsmaatregelen gericht op de Print- en couverteerstraat binnen DUO. In deze managementsamenvatting geven wij antwoord op drie onderzoeksvragen. De onderzoeksvragen hebben betrekking op het ontwerp en daadwerkelijk aanwezig zijn van een risicomanagementsysteem binnen de Print- en couverteerstraat van DUO. Respectievelijk: het onderkennen van risico's (onderzoeksvraag 1), het treffen van passende maatregelen (onderzoeksvraag 2) en governancemaatregelen gericht op de borging van de integriteit en vertrouwelijkheid van de gegevens en tenslotte het onderkennen van restrisico's (onderzoeksvraag 3). Voor een beschrijving van de onderzoeksvragen verwijzen wij naar paragraaf 1.2.

Eerst geven wij een korte toelichting op de Print- en couverteerstraat.

Het print- en couverteerproces bestaat uit een gegevensstroom waarbij data o.a. wordt ontvangen, opgeslagen, samen met andere data wordt gebundeld in een batch en voor printen wordt aangeboden, geprint, in enveloppen gedaan en aan PostNL overgedragen. DUO noemt dit het 'gesloten systeem'. In dit rapport noemen wij dit ook de Print- en couverteerstraat in enge zin. Het betreft niet één technisch systeem maar diverse systemen die middels koppelpunten zijn gekoppeld. In het 'gesloten systeem' wordt gesteund op allerlei (ondersteunende) processen, componenten en software zowel gericht op de verwerking zelf als op de communicatie. Bijvoorbeeld logische toegangsbeveiliging of changemanagement. In dit rapport noemen wij dit de Print- en couverteerstraat in brede zin.

Een gestructureerd en compleet risicomanagementproces ontbreekt

De Print- en couverteerstraat is in hoge mate geautomatiseerd en gemechaniseerd[1]. De werkzaamheden van de Print- en couverteerstraat kunnen ter plaatse door (minimaal) twee medewerkers worden uitgevoerd. Er is snel onderling contact tussen de medewerkers en de manager en bij vragen en problemen weet men elkaar makkelijk te vinden.

Een risicoanalyse van zowel de werkzaamheden gericht op het printen en couverten van ontvangen opdrachten (in enge zin) als de ondersteunende processen, componenten, zoals logische toegangsbeveiliging en changemanagement ontbreekt. Dergelijke ondersteunende processen kunnen invloed hebben op de integriteit van de Print- en couverteerstraat.

Ook ontbreekt een gestructureerde uitwerking van de risico's in concrete maatregelen, acceptatie van restrisico's en ontbreekt een inbedding van maatregelen die zijn aangetroffen in een risicomanagementsysteem. Er is een document aanwezig ("printen en couverteren (PDF-to-print)") waarin maatregelen op geaggregeerd niveau zijn beschreven maar een verdere concrete uitwerking, de relatie met risico-inschattingen en informatie over het daadwerkelijk naleven ervan ontbreekt. In servicelevel agreement (SLA) tussen en DUO is aangegeven dat de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG) van toepassing zijn maar hiervan hebben wij intern binnen DUO geen gestructureerde uitwerkingen in maatregelen en rapportages over daadwerkelijke naleving daarvan binnen de Print- en couverteerstraat aangetroffen.

[1] Voor een beschrijving wordt verwezen naar bijlagen 1 en 2 van dit rapport.

Dit betekent niet dat DUO géén maatregelen heeft getroffen gericht op de integriteit van de Print- en couverteerstraat. Wij hebben tijdens het onderzoek diverse controlemaatregelen aangetroffen, bijvoorbeeld de kwaliteitscontrole op prints. De aangetroffen maatregelen richten zich met name op de Print- en couverteerstraat zelf (in enge zin[2]).

Ten aanzien van onderzoeksvraag 3[3] hebben wij weinig borgingsmaatregelen aangetroffen. Wij hebben gezien dat er rapportages worden opgeleverd vanuit de Print- en couverteerstraat gericht op bijvoorbeeld verwerkte aantallen en op uitval bij het printen. Er ontbreken rapportages die zich richten op het daadwerkelijk beheersen van integriteitsrisico's en het naleven van integriteitsmaatregelen. Tijdens het onderzoek is door DUO aangegeven dat deze in ontwikkeling zijn.

In hoofdstuk 2 geven wij een nadere toelichting op de belangrijkste bevindingen uit het onderzoek. Voor een nader toelichting op het onderzoek verwijzen wij naar hoofdstuk 3. In bijlage 1 en 2 geven wij een korte beschrijving en een schematische weergave van de print en couverteerstraat.

Aanbeveling

Het risico doet zich voor dat er niet voldoende maatregelen zijn getroffen om de integriteitsrisico's in voldoende mate te mitigeren of dat niet (tijdig) inzicht is in de daadwerkelijke beheersing van risico's en als gevolg daarvan, indien nodig, compenserende maatregelen niet (tijdig) worden getroffen. Het ontbreken van een gestructureerd risicomanagementproces heeft ook gevolgen voor de continuïteit van de processen. Bij vertrek van een medewerker wordt het risico gelopen dat tevens veel kennis over risico's en de beheersing ervan verdwijnt.

Wij bevelen DUO aan om een gestructureerd risico-managementproces gericht op de integriteit van de Print- en couverteerstraat (in brede zin) in te richten. Door dit in te richten wordt inzicht verkregen in de daadwerkelijke risico's, borging van de implementatie en naleving van de gewenste integriteitsmaatregelen. Dit biedt tevens een goede basis om hierover verantwoording af te leggen.

---

[2] Zie voor een beschrijving daarvan de inleidende tekst van deze (management)samenvatting

[3] Voor en beschrijving van de vraag wordt verwezen naar paragraaf 1.3

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

De aanleiding voor het onderzoek is enerzijds dat DUO een nieuwe printstraat heeft gerealiseerd en anderzijds dat zich een probleem heeft voorgedaan in 2020. Er is gebleken dat te printen gegevens zijn kwijtgeraakt in een koppelpunt, . Aangegeven is dat de gegevens zijn teruggevonden en het probleem is opgelost. In het print- en couverteerproces wordt gebruik gemaakt van meer koppelpunten en servers.
DUO vraagt zich af of de integriteitsmaatregelen aan de kant van DUO goed zijn ingericht. Zijn hierin nog risico's te onderkennen en/of zijn er nog aandachtspunten? En zo ja, kunnen er maatregelen worden getroffen om deze risico's te mitigeren? Voor een verdere toelichting wordt verwezen naar de opdrachtbevestiging 2022-0000055872.

De Hoofddirecteur DUO is opdrachtgever van het onderzoek. De opdrachtgever wenst een rapport van bevindingen te ontvangen op een aantal specifieke onderwerpen om zelf conclusies te trekken en indien gewenst verbetermaatregelen te treffen. De opdracht heeft alleen betrekking op feitelijke bevindingen en dit rapport bevat om die reden geen oordeel en/of conclusies.

1.2 Doelstelling en onderzoeksvragen

Doel van het onderzoek is om inzicht te geven in de door DUO getroffen maatregelen gericht op het borgen van de integriteit van het print- en couverteerproces binnen DUO.

In de opdrachtbevestiging zijn drie onderzoeksvragen opgenomen:

Onderzoeksvraag 1: Welke risico's onderkent DUO gericht op het borgen van de integriteit en vertrouwelijkheid van de datastroom vanaf ontvangst van een printopdracht tot het aanleveren van geprinte documenten in een enveloppe aan PostNL?
Onderzoeksvraag 2: Welke maatregelen heeft DUO getroffen om de geconstateerde risico's te mitigeren en zijn t.o.v. het onderzoekskader nog restrisico's te onderkennen?
Onderzoeksvraag 3: Welke governancemaatregelen zijn getroffen rond het proces gericht op de borging van de integriteit en vertrouwelijkheid van de gegevens en zijn t.o.v. het onderzoekskader nog restrisico's te onderkennen?

1.3 Afbakening

In het kader van het onderzoek worden de volgende onderzoeksobjecten onderkend:

1. De integriteitsmaatregelen gericht op de datastroom en fysieke stroom van ontvangst van de data tot en met de verwerking door het printproces en het aanbieden van de enveloppen aan PostNL.
2. De inrichting en het bestaan van de toegangsbeveiliging tot (data op) de koppelpunten en belangrijke bestanden gericht op de integriteit en vertrouwelijkheid van de data.

3. De inrichting en het bestaan van changemanagement op software dat wordt gebruikt in de print en couverteerstraat.
4. Afspraken en verantwoordingen binnen de keten met ketenpartners gericht op de integriteitsmaatregelen en de naleving ervan.
5. Inrichting en het bestaan van de governancemaatregelen gericht op het voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) voor de betrokken technische componenten, bestanden en software in het print- en couverteerproces. Het gebruik van generieke componenten, zoals e-mail wordt niet meegenomen in het onderzoek.
6. Inrichting en het bestaan van de governancemaatregelen gericht op het voldoen aan de AVG met betrekking tot verwerkingen van persoonsgegevens. De generieke componenten worden niet meegenomen in het onderzoek.

Het print- en couverteerproces is afgebakend tot DUO: van de door DUO (middels het koppelvlak tussen en DUO) ontvangen data tot de aanlevering van brieven aan PostNL. De aansluiting van op het koppelvlak met DUO maakt geen onderdeel uit van het onderzoek omdat dit onder verantwoordelijkheid van valt. De maatregelen gericht op aansluiting van de data ontvangen door DUO op de data aangeleverd door de opdrachtgever wel, evenals de controle op de aansluiting van de aangeboden en ontvangen enveloppen door PostNL. De (interne) processen binnen of PostNL vallen niet binnen de scope. Verdere uitbestedingen door DUO is niet in het onderzoek meegenomen. De governancemaatregelen gericht op de integriteit en vertrouwelijkheid bij uitbesteding van werkzaamheden door DUO aan andere partijen in de keten maken wel deel uit van het onderzoek voor zover weergegeven in de figuren 1, 2 en 3 in bijlage 2 van dit rapport. Voor een nadere toelichting en weergave van het onderzoekskader wordt verwezen naar de opdrachtbevestiging 2022-0000055872.

2 Bevindingen

De drie onderzoeksvragen (zie 1.2) liggen in elkaars verlengde. In dit hoofdstuk geven wij de belangrijkste bevindingen weer in de volgorde van de onderzoeksvragen. Paragraaf 2.1 geeft een overkoepelende bevinding die betrekking heeft op alle drie onderzoeksvragen. We sluiten af met een algemene bevinding (2.7). Hieronder geven wij de relatie van de belangrijkste bevindingen met de onderzoeksvragen:

- Onderzoeksvraag 1: 2.2
- Onderzoeksvraag 2: 2.3 en 2.4
- Onderzoeksvraag 3: 2.5 en 2.6

2.1 Een gestructureerd en compleet risicomanagementproces ontbreekt

Het onderzoek richt zich op de integriteitsmaatregelen van en rond de Print- en couverteerstraat binnen DUO. Om een goed beeld te krijgen van de beheersing van de risico's en effectiviteit van de getroffen maatregelen is het van belang dat DUO het risicomanagement heeft ingericht. Wij hebben geen gestructureerde (en expliciete) risicoanalyse en geen gestructureerd en compleet risicomanagementproces aangetroffen binnen DUO.

Het was bij betrokken medewerkers van DUO niet duidelijk of een risicoanalyse is uitgevoerd. Uiteindelijk bleek er geen complete risicoanalyse aanwezig te zijn. Op onderdelen hebben we documenten aangetroffen, bijvoorbeeld een risicoanalyse gericht op invoering van de Rijkspas (en een document van de evaluatie van een probleem. Wij hebben geen informatie aangetroffen gericht op het vaststellen van de risicoanalyse (en risk appetite/restrisico's).
In afspraken is aangegeven dat de BIO van toepassing is. Er ontbreekt een analyse of de BIO een voldoende beveiligingsniveau biedt bijvoorbeeld t.a.v. de categorieën persoonsgegevens die worden verwerkt.

Een gestructureerde uitwerking van de BIO en AVG in concrete maatregelen en controles (die gezien de situatie van de Print- en couverteerstraat minimaal noodzakelijk zijn) en welke restrisico's worden geaccepteerd is niet aangetroffen. Er is een beschrijving (document "printen en couverteren (PDF-to-print)", versie 1.1, concept) van het print- en couverteerproces waarin controlemaatregelen op geaggregeerd niveau zijn genoemd. Ook liggen er afspraken over het uitvoeren van hacktests om de veiligheid van de digitale infrastructuur te constateren. Hierbij ontbreken vaak (gestructureerde) onderliggende beschrijvingen en uitwerkingen van deze controles, of en op welke wijze deze worden vastgesteld en/of de maatregelen worden nageleefd (daadwerkelijke uitvoering van controles/maatregelen). Ook ontbreken maatregelen gericht op het opleveren van betrouwbare rapportages over het naleven van deze maatregelen. Daarnaast ontbreekt er een relatie tussen de maatregelen en risico-inschattingen.

Tevens missen we maatregelen gericht op het meten en beheersing van het daadwerkelijk naleven van integriteitsmaatregelen en controles en de rol van interne (en externe) audits hierbij.

Het besluitvormingsproces gericht op risico's, maatregelen, accepteren restrisico's en de terugkerende cyclus op basis van het daadwerkelijk naleven ervan, de resultaten en afstemming hiervan met opdrachtgevers, ontbreekt.

2.2 Inzicht in de mogelijkheden het gesloten systeem te beïnvloeden en de beheersing daarvan ontbreekt deels

De procesbeschrijving '"printen en couverteren (PDF-to-print)"' en een bezoek ter plaatse heeft inzicht gegeven in werkzaamheden in de Print- en couverteerstraat tot en met de overdracht van brieven aan PostNL. Voor een nadere beschrijving van het proces verwijzen wij naar de bijlagen 1 en 2 van dit rapport. Tijdens het onderzoek is aangegeven dat de Print- en couverteerstraat een gesloten systeem is en dat daarop qua integriteitsmaatregelen wordt gesteund. Daarmee levert de opdrachtgever print- en couverteer opdrachten (hierna: opdracht) aan en met minimale menselijke handelingen worden deze door DUO samengebundeld in een te printen batch, uitgeprint, gecouverteerd en aangeboden aan PostNL. Daarbij hebben wij gezien dat door de printer kwaliteitscontrole plaatsvindt op de prints en bij uitval een nieuwe te printen opdracht wordt aangemaakt. Maatregelen zijn met name gericht op de integriteit van de print(opdrachten). Naast kwaliteitscontrole op de prints vindt ook rapportage over o.a. aantallen plaats richting de opdrachtgever. Hieronder benoemen wij in relatie tot het gesloten systeem twee bevindingen. Er is geen documentatie waaruit op gestructureerde wijze blijkt welke mogelijkheden er zijn om het gesloten systeem te beïnvloeden en welke mitigerende maatregelen zijn getroffen. Een nadere toelichting geven wij in 2.2.1 en 2.2.2

2.2.1 Afhankelijkheid van menselijk handelen binnen het "gesloten systeem"

Binnen het gesloten systeem vinden ook handmatige handelingen plaats. Bijvoorbeeld het samenvoegen van printopdrachten tot batches, het opstarten van print-jobs, uitvoeren van controle op uitval, het opnieuw printen van uitval, klaarzetten van het papier, gebruik van de juiste enveloppen en het laten vernietigen van prints die niet aan de gewenste kwaliteit voldoen. Er is een procesbeschrijving '"printen en couverteren (PDF-to-print)"' aanwezig. Dit is een beschrijving op geabstraheerd niveau, wij hebben geen documentatie ontvangen waarin dit op gestructureerde wijze is uitgewerkt in concrete maatregelen en controles die hiervoor zijn getroffen. We hebben tijdens een bezoek ter plaatse geconstateerd dat er binnen de Print- en couverteerstraat aandacht is voor het treffen van maatregelen om het risico op fouten of problemen te minimaliseren. Zo wordt het logo van de organisatie op het papier geprint om de kans op het gebruik van het verkeerde (logo)papier te vermijden. Ook zijn er maatregelen getroffen dat onbevoegden niet ongeautoriseerd (door middel van fysieke toegangsbeveiliging middels pasjes) en ongemerkt (achterdeur, middels een sluis) naar binnen kunnen komen. Wegens het ontbreken van documentatie is het voor ons niet inzichtelijk geworden welke handmatige ingrijpen op het systeem mogelijk zijn door de medewerkers en voor welke acties autorisatie noodzakelijk is door de manager en welke acties zij zelf mogen uitvoeren. Hierdoor is het ook onduidelijk is op welke wijze wordt geconstateerd dat autorisatie en maatregelen worden nageleefd. Tijdens ons bezoek bleek dat het een hele kleinschalige omgeving is waarin veel direct contact is tussen de medewerkers en de manager en dat het voor de medewerkers wel duidelijk is welke handelingen zij kunnen of mogen uitvoeren.

2.2.2 Afhankelijkheid van de werking van het "gesloten systeem" van componenten en andere processen

In het "gesloten systeem" wordt gebruik gemaakt van allerlei processen, componenten, softwarecomponenten zowel gericht op de verwerking zelf als op de communicatie. Voor een toelichting verwijzen wij naar bijlage 2. Instellingen, autorisaties en het gebruik van dergelijke processen en componenten kunnen invloed hebben op de juiste werking van de Print- en couverteerstraat, de integriteit, maar ook op de vertrouwelijkheid van de gegevens die worden verwerkt. In het onderzoek is de fysieke en logische toegangsbeveiliging (en het verlenen van autorisaties, het gebruik ervan en het intrekken ervan) en changemanagement (het ongewijzigd blijven en alleen beheerst doorvoeren van wijzigingen in onder andere componenten, software) onderzocht. Beheersing van deze processen is nodig om zekerheid te hebben over het functioneren of te kunnen borgen dat de Print- en

couverteerstraat en de componenten waarvan zij gebruik maakt blijven functioneren zoals gewenst en om te voldoen aan de gemaakte afspraken ten aanzien van informatiebeveiliging en privacy en om tijdig mogelijke problemen te constateren.

Een goede beheersing van de werking van het gesloten systeem vraagt om een breed inzicht in de risico's die zich voor kunnen doen. Voor onze bevindingen t.a.v. de risicoanalyse en het risicomanagementproces wordt verwezen naar paragraaf 2.1.

2.3 Gestructureerd overzicht van AVG-maatregelen binnen DUO en inbedding in risicomanagementproces ontbreekt

Er is een verwerkersovereenkomst tussen en DUO. Uit een bijlage bij deze verwerkersovereenkomst blijkt dat de verantwoordelijke is en de grondslag van de gegevensverwerking is aangegeven. In het document is tevens een aantal onderwerpen genoemd. Bijvoorbeeld:

- Verklaring Omtrent Gedrag Natuurlijke Personen (VOG NP), ambtseed/-gelofte.
- Inlogcodes en toegangsbadges.
- Niet verzonden printwerk wordt op een veilige wijze vernietigd, alle bestanden worden verwijderd na ten hoogste 60 dagen.
- Regelmatig uitvoeren van een hacktest.
- Afspraken over het melden van inbreuken in verband met persoonsgegevens.

Onduidelijk is op welke wijze deze onderwerpen binnen DUO zijn uitgewerkt in procedures en maatregelen en zijn ingebed in het risicomanagementproces binnen DUO. Wij hebben hiervan geen gestructureerde uitwerking ontvangen. Ook niet over de wijze waarop hierover afstemming plaatsvindt met de opdrachtgever. Wij hebben geen Data Protection Impact Assessment (DPIA) ontvangen. Het opstellen ervan ligt bij de verantwoordelijke, valt buiten de scope van het onderzoek.

2.4 Toegangsrechten lijken soms heel ruim en zijn niet altijd te herleiden naar een persoon

Uit gesprekken en ontvangen documenten blijkt dat er binnen DUO gebruik wordt gemaakt van toegangsbeveiliging. Middels een rol worden autorisaties toegekend aan medewerkers. De rol die een medewerker krijgt bepaalt tot welke onderdelen (resources) een medeweker toegang heeft en wat de medewerker mag doen. Ook is er aandacht voor identity-management. Op een WIKI-pagina is aangegeven dat de verantwoordelijkheid dat medewerkers niet meer autorisaties hebben dan ze voor hun werk nodig hebben bij de manager is belegd; "die check doet de manager 4 x per jaar via de attestaties, maar ook wanneer een nieuwe medewerker aan de slag gaat, van functie wijzigt of vertrekt". Wegens het ontbreken van documentatie is het niet duidelijk of dit voor alle componenten geldt. In een mail is aangegeven dat er autorisatiematrices zijn voor en dat die elk jaar worden gecontroleerd door de manager printstraat. Door het ontbreken van vastleggingen is het niet duidelijk welke controles worden uitgevoerd en de inbedding daarvan in het risicomanagementproces. Voor onze bevindingen t.a.v. de risicoanalyse en het risicomanagementproces wordt verwezen naar paragraaf 2.1.

Ten aanzien van de fysieke toegangsbeveiliging maakt de Print- en couverteerstraat gebuikt van de Rijkspas die is ingevoerd voor toegang tot de fysieke locatie Er is een risicoanalyse aanwezig die is opgesteld voorafgaand aan de implementatie ervan. Wij hebben informatie ontvangen over de logische toegangsbeveiliging van een aantal componenten die gebruikt worden binnen de Print- en couverteerstraat. Hieruit blijkt dat er op deze componenten een systeem van logische toegangsbeveiliging is ingericht. Uit ontvangen documenten en overzichten uit componenten blijkt dat een rol (en daarmee autorisaties) niet altijd te koppelen is aan een persoon omdat gebruik wordt gemaakt van generieke

accounts. Er zijn situaties waarin dit logisch lijkt bijvoorbeeld het verlenen van fysieke toegang aan een eenmalige bezoeker of in geval van beheerdersaccount, dat verplicht in het systeem aanwezig is. Het lijkt het erop dat er meer van dergelijke accounts aanwezig zijn en dat bijvoorbeeld veel medewerkers geautoriseerd zijn voor toegang tot een generiek beheerdersaccount. Voor detailbevindingen verwijzen wij naar de bevindingenmatrix. Uitgangspunt zou moeten zijn het zo min mogelijk gebruikmaken van niet naar een persoon herleidbare accounts. Daarnaast vragen generieke accounts om compenserende (controle)maatregelen gericht op het verstrekken en gebruik ervan. Uit een ontvangen document blijkt dat er een controle is beschreven (het dagelijks veranderen van Admin wachtwoorden en het blokkeren van toegang zodra je komt te vervallen uit de betreffende autorisatiegroep) maar we hebben niet kunnen vaststellen dat dit voor alle componenten geldt. Tevens is geen informatie ontvangen over de wijze waarop toegang tot generieke accounts en het gebruik ervan worden beheerst en hoe geborgd wordt dat alleen medewerkers waarvoor het noodzakelijk is, daadwerkelijk toegang hebben tot de betreffende generieke account en er op een beheerste wijze gebruik van maken. Het is niet bekend of logging en controle plaatsvindt op het gebruik van generieke accounts en de beheerdersactiviteiten w.o. het toekennen en wijzigen van wachtwoorden. Ook is niet uitgewerkt hoe wordt geborgd dat autorisaties tijdig worden ingetrokken. Uit een ontvangen actueel overzicht van autorisaties in blijkt dat ten opzichte van een eerder ontvangen versie de autorisatie van toegang tot een generiek account sterk is beperkt. Daaruit blijkt dat er controle plaatsvindt.

Bij ons bezoek ter plaatse valt op dat de servers in de ruimte van de Print- en couverteerstraat staan. Een serverruimte zou aan allerlei eisen moeten voldoen. Bijvoorbeeld gericht op klimaatbeheersing, brandpreventie en brandvertragende maatregelen, maatregelen gericht op wateroverlast, back-up, recovery en voldoende afscherming vanaf buitenaf. Dit hebben wij niet onderzocht omdat dit buiten de scope van de opdracht valt.

2.5 Rapportages over het naleven van integriteitsmaatregelen zijn in ontwikkeling

2.5.1 Er zijn rapportages aanwezig met aantallen printen en couverteren

In de Print- en couverteerstraat zelf worden meta gegevens, bijvoorbeeld aantallen, vastgelegd en vindt controle plaats bijvoorbeeld op de kwaliteit van een print en wordt tussen partijen en/of componenten meta-informatie uitgewisseld. Voor een beschrijving verwijzen wij naar bijlagen 1 en 2. Aangegeven is dat DUO maandelijks een maandrapportage oplevert. Dit betreft een maandrapportage (Excel-overzicht) uit Dit overzicht hebben wij ontvangen. Op verschillende tabbladen is informatie weergegeven over aantallen en totalen. Het is onduidelijk wat met het overzicht wordt gedaan. Dit is niet toegelicht. Wij hebben een KPI-rapportage ontvangen (zie paragraaf 2.5.2). DUO gebruikt Topdesk voor de registratie van onder andere incidenten en daaruit worden rapportages opgeleverd. Aangegeven is dat ten behoeve van het 2-maandelijkse overleg met overzichten worden verstrekt.

2.5.2 Er zijn KPI-rapportages aanwezig

Wij hebben een door DUO opgestelde KPI-rapportage over maart en april 2022 ontvangen dat betrekking heeft op 3 van de 4 prestatie-indicatoren waarover in de SLA tussen en DUO afspraken zijn gemaakt: volledigheid, tijdigheid en afdrukkwaliteit. De KPI "betrouwbaarheid" ontbreekt. Uit het document blijkt dat de drie KPI's 100% zijn behaald. Onduidelijk is op welke brongegevens de rapportage is gebaseerd en op welke wijze de berekeningen zijn gemaakt. Tevens is onduidelijk welke (onafhankelijke) controles op de juistheid, volledigheid en controleerbaarheid van de rapportage zijn uitgevoerd. In de rapportage is aangegeven dat er geen verstoringen zijn geweest. Het is niet duidelijk wat in de KPI-rapportage onder een "verstoring" wordt verstaan. In de KPI-rapportage is geen relatie gelegd met de drie escalatieniveau 's beschreven in de SLA tussen en DUO. In een interview is

aangegeven dat alleen belangrijke verstoringen/incidenten worden genoemd. Het is niet duidelijk wie dit bepaalt en op basis waarvan. In een overzicht met incidenten januari-april 2022 zijn 44 incidenten weergegeven. Incidenten met de volgende meldingen worden in dit overzicht vaak genoemd: "printjob vastgelopen" of "vastloper in OM-variant" of "ontbrekende ontvangstbevestigingen" of "problemen met Bij één opmerking is weergegeven " en issue bij We hebben een document ontvangen "Evaluatie incident 1 september". Hieruit blijkt dat er een evaluatie van een incident heeft plaatsgevonden. Dit betreft een chronologische opsomming van alle voorvallen/acties ten aanzien van een incident met waardoor de printopdrachten niet bij de printer komen. Onduidelijk is wat de oorzaak van het incident is en op welke wijze dit in de toekomst wordt voorkomen. Onduidelijk is wie daarbij aanwezig zijn geweest en of dit is afgestemd binnen de organisatie en met . Ook is onduidelijk in welke gevallen een evaluatie van een incident wordt uitgevoerd en wie dit bepaalt.

2.5.3 *Rapportages gericht op het naleven integriteitsmaatregelen niet aanwezig*

DUO heeft geen rapportages gericht op het naleven van integriteitsmaatregelen en -controles (bijvoorbeeld) gericht op de BIO of AVG, zowel niet intern binnen DUO als richting andere partijen.

2.6 Audit of verbijzonderde interne controle op naleving processen niet aangetroffen

In de SLA is bij "Audit" aangegeven dat met DUO overlegt over het uitvoeren van een audit en dat DUO rapporteert over de follow-up van de bevindingen uit de audit en over de concrete vervolgstappen. Wij hebben geen auditrapport of documenten over een concrete auditplanning aangetroffen.
Naast het uitvoeren van audits kan door middel van verbijzonderde interne controle meer zekerheid worden verkregen over het daadwerkelijk, op een goede wijze naleven van processen en maatregelen en over bijvoorbeeld de juistheid en volledigheid van rapportages. Er is geen beleid, opzet en/of planning van de verbijzonderde interne controlewerkzaamheden gericht op de processen rond het printen en couverteren of bijvoorbeeld gericht op changemanagement of het proces van logische toegangsbeveiliging aanwezig. Er zijn tevens zijn geen rapportages van interne controle aangetroffen.

2.7 Een document managementsysteem ontbreekt

In de inleiding en in hoofdstuk 3 is aangegeven dat het veel moeite kost om documenten, vastleggingen, rapportages en dergelijke te ontvangen. Een voor medewerkers inzichtelijk systeem voor het vastleggen en beheren van documenten ontbreekt. Dit ondanks dat DUO gebruik maakt van WIKI-pagina's. Overzicht en inzicht in bijvoorbeeld de aanwezige documenten en rapportages is een belangrijk hulpmiddel voor interne medewerkers (en auditor) om een goed inzicht te geven en hebben in het beleid, risico-inschattingen, de uitwerking in maatregelen, de uitvoeringspraktijk, beheersingsmaatregelen en de wijze waarop bijvoorbeeld activiteiten in de organisatie zijn geregeld en geborgd.

3 Verantwoording onderzoek

3.1 Werkzaamheden en afbakening

Uitgangspunt voor het onderzoek is de met de opdrachtgever overeengekomen opdrachtbevestiging (2022-0000055872) met onderzoeksvragen, en het daarin opgenomen onderzoekskader. Voor een weergave van de onderzoeksvragen wordt verwezen naar paragraaf 1.2. Om de onderwerpen uit het onderzoekskader te onderzoeken hebben we de volgende werkzaamheden uitgevoerd:

- Interviews met betrokkenen bij de uitvoering van werkzaamheden binnen de Print- en couverteerstraat;
- Documentenstudie;
- Waarneming ter plaatse bij de Print- en couverteerstraat.

Uitgevoerde werkzaamheden
De uitvoering van het onderzoek is gestart in februari 2022. De uitvoering van het onderzoek is in april "on hold" gezet omdat de voor het onderzoek gevraagde documenten niet tijdig waren aangeleverd en reactie uitbleef op door ons opgestelde verslagen van een interview en een bezoek ter plaatse. De ADR heeft met DUO afgesproken om meer tijd te geven voor het aanleveren van documenten. In september heeft de doorstart van het onderzoek plaatsgevonden met de op dat moment ontvangen documenten. Uitgangspunt was daarbij dat als we documenten niet hebben ontvangen, deze er niet zijn.

Hoor- en wederhoor
Bij de doorstart van het onderzoek is gebruik gemaakt van de verslagen van de reeds eerder in het jaar gehouden interview en bezoek ter plaatse. Aangezien daarop geen reactie is ontvangen is besloten tot een tussenstap in het onderzoek door de door de ADR ingevulde concept-bevindingenmatrix af te stemmen met de belangrijkste bij het onderzoek betrokken functionarissen bij DUO om na te gaan of bevindingen juist zijn weergegeven. Indien dit niet zo was is gevraagd om aan te geven wat juist is en ter ondersteuning daarvan onderliggende documentatie aan te leveren. Nadat we de reactie hadden ontvangen is het conceptrapport opgesteld.

De inhoudelijk afstemming van dit rapport heeft plaatsgevonden met de opdrachtgever. In bijgevoegde managementreactie (bijlage 3) heeft de opdrachtgever zijn visie op de onderzoeksresultaten verwoord.

3.2 Gehanteerde standaard en kwaliteitsborging

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.

3.3 Detailbevindingen

Er is een tabel met alle detailbevindingen. Dit is een intern dossierstuk van de ADR en wordt aan de opdrachtgever beschikbaar gesteld.

3.4 Verspreiding 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. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

4 Ondertekening

Den Haag, 16 maart 2023

Auditor

Auditdienst Rijk

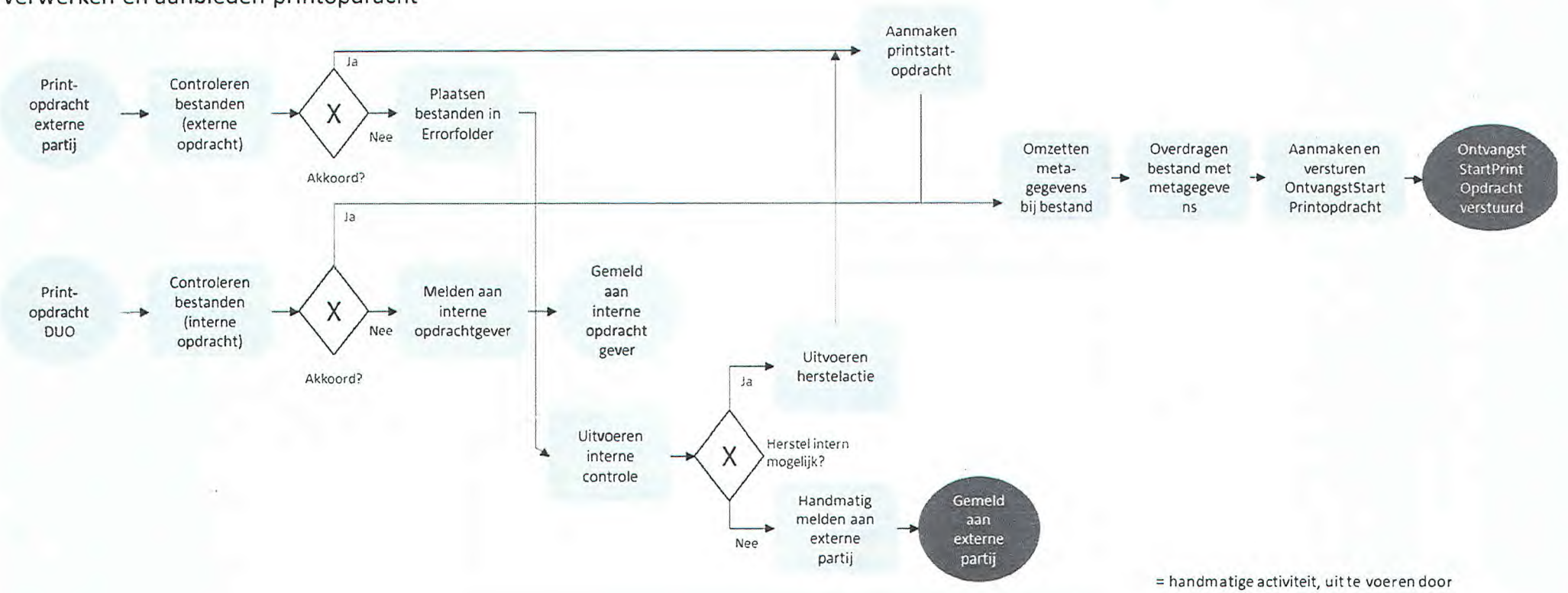
Bijlage 1 Procesbeschrijving Print- en couverteerstraat

In de Print- en couverteerstraat van DUO worden brieven geprint en gecouverteerd voor verschillende interne en externe partijen. Het proces bestaat uit drie deelprocessen, te weten: verwerken en aanbieden van een printopdracht, printen van het bestand en tenslotte het couverteren van documenten. Printopdrachten van zowel DUO als de externe klant worden ontvangen, gecontroleerd en indien akkoord, in een geautomatiseerd proces aangevuld met metagegevens en daarna aangeboden aan de printsoftware. Vervolgens worden de bestanden geprint. Hierna vinden controles hierop plaats. Indien akkoord, worden de geprinte documenten gecouverteerd. De gecouverteerde documenten worden uiteindelijk gebundeld en aangeboden voor verzending. Het proces vindt geautomatiseerd plaats. Dit betekent dat er bij verplaatsingen van en handelingen op data gebruik wordt gemaakt van verschillende technische componenten en applicaties. Het proces kan dan ook gezien worden als een aaneenschakeling van technische componenten. Tussen deze componenten bevinden zich koppelvlakken; dit zijn technische koppelingen gericht op het verzenden/ontvangen van data. Naast koppelvlakken wordt ook gebruik gemaakt van allerlei generieke componenten en software voor onder andere de bewaring van data en het samenstellen van batches.
Om meer inzicht te krijgen in de status van bestanden, is in 2020 een nieuwe Print- en couverteerstraat gerealiseerd incl. integriteitssysteem. Dit integriteitssysteem stelt DUO en haar opdrachtgevers in staat om de status van bestanden te volgen in het proces.

Bijlage 2 Schematische weergave Print- en couverteerstraat

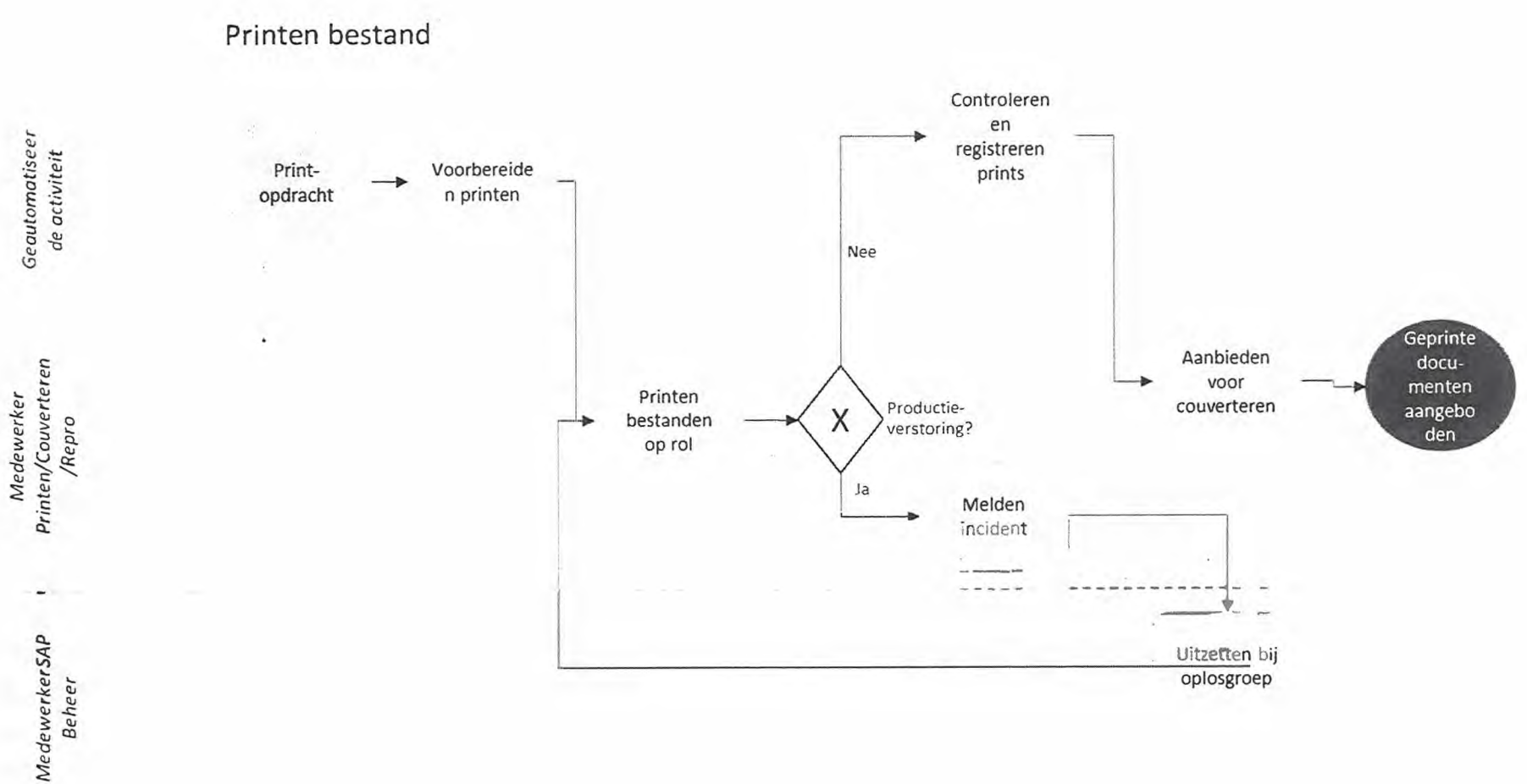
In deze bijlage zijn de drie deelprocessen van de Print- en couverteerstraat schematisch weergeven. Daarbij zijn de integriteitsmaatregelen tevens opgenomen. Dit is opgesteld op basis van het brondocument "printen en couverteren (PDF-to-print)" (versie 1.1, concept, niet gedateerd).

Verwerken en aanbieden printopdracht

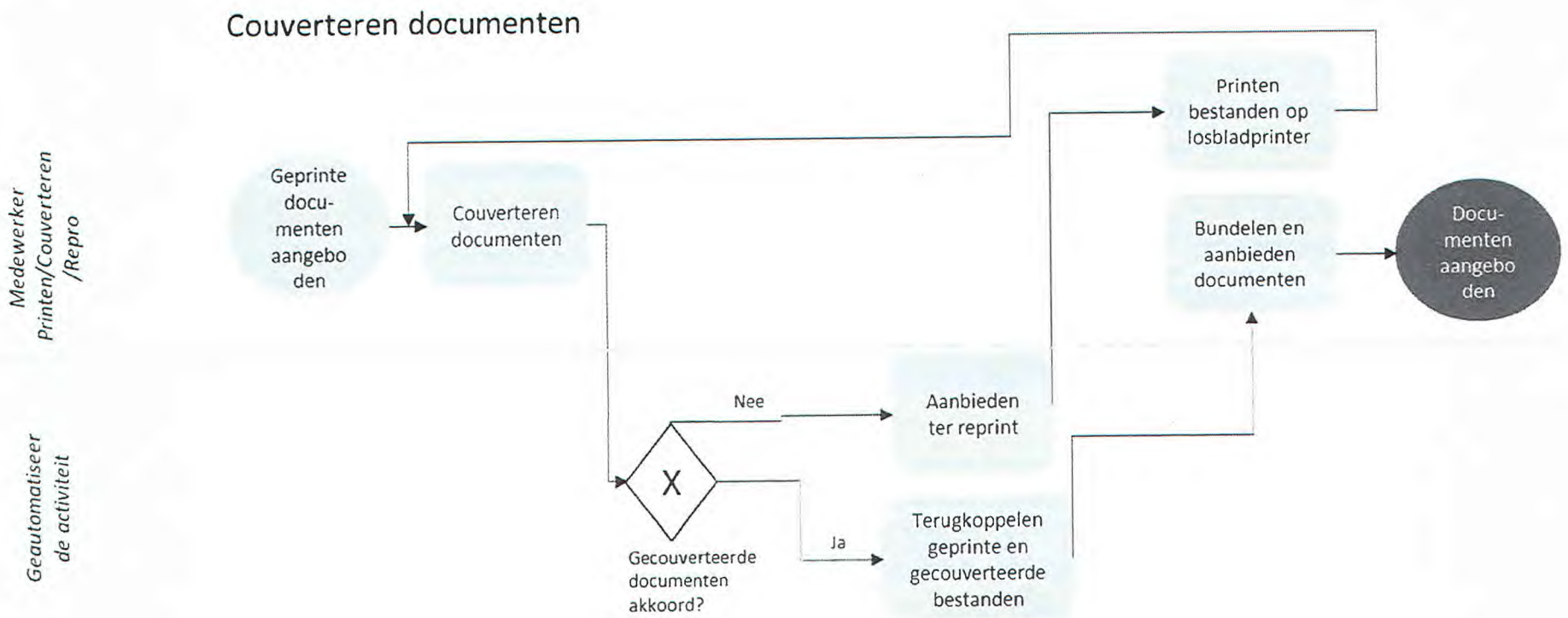


Figuur 1. Procesplaat deelproces 'Verwerken en aanbieden printopdracht'

In bovenstaande procesplaat betreffen alle processtappen een geautomatiseerde activiteit, met uitzondering van de stappen die omlijnd zijn middels een doorbroken streep.



Figuur 2. Procesplaat deelproces 'Printen bestand'



Figuur 3. Procesplaat deelproces 'Couverteren documenten'

Bijlage 3 Managementreactie

Deze bijlage bevat de managementreactie van DUO op het conceptrapport. De reactie is op 21 februari 2023 ontvangen. De reactie is geen onderdeel van het uitgevoerde onderzoek en de inhoud valt buiten onze verantwoordelijkheid.

De ADR heeft drie onderzoeksvragen gesteld. Deze vragen hebben betrekking op het ontwerp en daadwerkelijk aanwezig zijn van een risicomanagementsysteem binnen de Print- en couverteerstraat van DUO.

De 3 vragen:

1. het onderkennen van risico's
2. het treffen van passende maatregelen
3. governancemaatregelen gericht op de borging van de integriteit en vertrouwelijkheid van de gegevens en tenslotte het onderkennen van restrisico's

De ADR komt tot de onderstaande aanbeveling:
Het risico doet zich voor dat er niet voldoende maatregelen zijn getroffen om de integriteitsrisico's in voldoende mate te mitigeren of dat niet (tijdig) inzicht is in de daadwerkelijke beheersing van risico's en als gevolg daarvan, indien nodig, compenserende maatregelen niet (tijdig) worden getroffen. Het ontbreken van een gestructureerd risicomanagementproces heeft ook gevolgen voor de continuïteit van de processen. Bij vertrek van een medewerker wordt het risico gelopen dat tevens veel kennis over risico's en de beheersing ervan verdwijnt.

Wij bevelen DUO aan om een gestructureerd risico-managementproces gericht op de integriteit van de Print- en couverteerstraat (in brede zin) in te richten. Door dit in te richten wordt inzicht verkregen in de daadwerkelijke risico's, borging van de implementatie en naleving van de gewenste integriteitsmaatregelen. Dit biedt tevens een goede basis om hierover verantwoording af te leggen.

Reactie DUO

Graag willen we de ADR bedanken voor het onderzoek, de opzet is helder en we zien dat er uitgebreid is gekeken naar de beschikbare documentatie. Op grond daarvan herkennen we de opmerkingen van de ADR en geven hierna aan welke aanbevelingen we overnemen.

De focus ligt hierbij op het beter inrichten van een gestructureerd en compleet risicomanagementproces op basis van wat er nu al ligt. Veel is er al wel, maar dit zullen we beter uit moeten werken en explicieter moeten benoemen. Daarbij horen ook de al eerder ingerichte processen waarbij in het systeem waarborgen zijn ingebouwd voor bijvoorbeeld automatisch opnieuw printen en couverteren. Het verbeterde risicomanagement proces moet voor de bestaande processen/producten overzicht geven van risico's, maatregelen, interne controles en (bronnen van) rapportages bevatten. Daarnaast moet een gestructureerd changeproces om bij wijzingen/nieuwe opdrachten de impact en risico's te kunnen vaststellen worden ingericht, inclusief eventuele impact op het gesloten print- en integriteitsproces.

Ten aanzien van de gedane aanbevelingen betekent dit het volgende:

1. Een gestructureerd en compleet risicomanagementproces ontbreekt.
   Maatregel: Samen met de afdelingen Procescontrol en Compliance een risicoanalyse uitvoeren en aan de hand hiervan bepalen welke concrete maatregelen er nog ingericht moeten worden. N.B. Deze actie is reeds gestart.
   Wanneer: Q3 2023.

2. Inzicht in de mogelijkheden het gesloten systeem te beïnvloeden en de beheersing daarvan ontbreekt deels.
   Maatregel: De operators hebben nu de mogelijkheid om handmatig te kunnen ingrijpen. Om dit te beheersen wordt een autorisatieproces ingericht voor de kritische handelingen door bepaalde functionarissen inclusief de controle hierop.
   Wanneer: start Q2 2023, oplevering uiterlijk Q4 2023.
3. Gestructureerd overzicht van AVG-maatregelen binnen DUO en inbedding in risicomanagementproces ontbreekt.
   Maatregel: De genoemde onderwerpen meenemen in de uit te voeren risico analyse, waarbij dit wordt ingebed in het controleproces.
   Wanneer: Q3 2023
4. Toegangsrechten lijken soms heel ruim en zijn niet altijd te herleiden naar een persoon.
   Maatregel: Onderzocht gaat worden of binnen de huidige tooling verbijzonderingen kunnen worden aangebracht qua gebruiker. Hierop volgend zullen de procesbeschrijvingen worden aangescherpt op genoemde punten.
   Wanneer: Q2 2023
5. Rapportages over het naleven van integriteitsmaatregelen zijn in ontwikkeling.
   Maatregel: De procesbeschrijvingen aanscherpen op genoemde punten en deze conform uitvoeren.
   Wanneer: Q2 2023
6. Audit of verbijzonderde interne controle op naleving processen niet aangetroffen.
   Maatregel: het huidige rapport is een eerste aanzet. Dit helpt om de verdere controles op te zetten.
   Wanneer: Q3 2023
7. Een document managementsysteem ontbreekt.
   De aanbeveling om een DMS op te zetten nemen we niet over. Wel zullen we zorgen voor een centrale plek waar relevante documentatie vindbaar is.
   Wanneer: Q2 2023

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