Auditdienst Rijk
Ministerie van Financiën

Auditdienst Rijk
Inlichtingen

Aan
Voorzitter en leden SG-overleg

Datum
7 september 2015

Notitienummer
ADR/

notitie

Tussentijds rijksbreed beeld 2015

1. Inleiding

In maart 2015 zijn in het SGO de hoofdlijnen van de samenvattende auditrapporten 2014 besproken. Net als vorig jaar presenteert de ADR nu het rijksbrede tussentijdse beeld over 2015. Hierin geven wij signalen (early warnings, geen early judgements) die de ministeries in staat stellen om tijdig actie te ondernemen.

Deze notitie geeft een rijksbreed beeld. Onze departementale teams zullen daar waar relevant de departementspecifieke aanbevelingen onder de aandacht brengen via een interim-rapportage of in het auditcommittee.
Vanuit het rijksbrede beeld zien wij in het algemeen dat ministeries de aandachtspunten uit de samenvattende auditrapporten 2014 oppakken. Voor het financieel beheer hebben wij twee rijksbrede early warnings met betrekking tot de correcte toepassing van de aanbestedingsregels en de WNT. Daarnaast hebben wij, vanwege het belang daarvan, het IT-beheer een prominente plaats gegeven in het tussentijds beeld.

In het tussentijds beeld zijn onze aandachtspunten opgenomen volgens onderstaande lijnen:

- Aandacht voor IT-beheer nodig
  Ontwikkelingen in de ICT en aangepaste wetgeving, met name op het gebied van privacy, vragen om continue aandacht voor het IT-beheer.
- Bedrijfsvoering verdient aandacht bij veranderingen
  De veranderingen in inrichting van de rijksdienst en de wijzigingen in wet- en regelgeving vragen om een tijdige aanpassing van de bedrijfsvoering (waaronder het beheer), om uitvoerings- en rechtmatigheidsproblemen te voorkomen.

2. Aandacht voor IT-beheer nodig

Ontwikkelingen in de ICT en aangepaste wetgeving, met name op het gebied van privacy, vragen om continue aandacht voor het IT-beheer.

2.1. Gevoel van urgentie ontbreekt, beperkte stappen gezet in bewustwording van informatiebeveiliging

Informatiebeveiliging wordt een steeds belangrijker onderwerp, mede door de ontwikkelingen op het gebied van privacywetgeving.
Het informatievoorzienings- en beveiligingsbeleid zal moeten aansluiten op de huidige mate van digitalisering en uitbesteding van IT-voorzieningen. Een aantal departementen richt hiertoe opnieuw de informatiebeveiligingsfunctie in. Ook wordt op meerdere departementen gewerkt aan (het opzetten van) een bewustwordingscampagne informatiebeveiliging voor management en medewerkers.

Van belang is dat de aandacht voor informatiebeveiliging wordt vastgehouden en getroffen maatregelen ook daadwerkelijk aantoonbaar worden gemaakt in de dagelijkse processen. Hierbij zal zorg moeten worden besteed aan het structureel inbedden van informatiebeveiliging. De 'tone at the top' is essentieel in het bewustwordingsproces.

2.1.1. Nieuwe privacywetgeving vraagt om het treffen van beheersingsmaatregelen voor 1 januari 2016

Wij zien binnen het Rijk dat nog te weinig stappen worden ondernomen om te voldoen aan de nieuwe wetgeving op het gebied van privacy die vanaf januari 2016 van kracht zal zijn.
Op korte termijn vindt er een groot aantal wijzigingen plaats op het gebied van privacy wet- en regelgeving. Als gevolg van de nieuwe Wet Meldplicht Datalekken zijn zowel private als publieke organisaties die persoonsgegevens verwerken met ingang van 1 januari 2016 verplicht om een datalek te melden. Ook bij het niet (goed) naleven van een beveiligingsmaatregel kan al sprake zijn van een datalek. Daarnaast zal de nieuwe Europese Algemene Verordening Gegevensbescherming naar verwachting begin 2016 in werking treden. In deze verordening is een algemene zorgplicht opgenomen. Op basis daarvan moet een organisatie intern privacybeleid ontwikkelen en adequate beveiligings-maatregelen treffen, zodat aantoonbaar aan deze zorgplicht wordt voldaan. Het niet voldoen aan de in deze wetgeving opgenomen zorgplicht kan leiden tot hoge boetes voor organisaties of bestuurders en imagoverlies.

Binnen de rijksdienst vinden verwerkingen van persoonsgegevens veelal in ketens plaats en bevinden de gegevens zich in informatiesystemen waarvan het beheer kan zijn uitbesteed aan interne of externe dienstverleners. Als gevolg van de gewijzigde regelgeving ontstaat tevens een ketenaansprakelijkheid. Dit betekent dat er ketenbreed afspraken dienen te worden gemaakt op welke wijze ketenpartijen omgaan met mogelijke inbreuken op de beveiliging en datalekken.

Wij adviseren het SGO om betrokken partijen CBP, DGOBR/CIO Rijk, Nationaal Cyber Security Centrum(NCSC) en ADR samen hierin te laten optrekken.

2.1.2. Maatregelen BIR worden nog onvoldoende aantoonbaar gemaakt

Begin dit jaar zijn met de in-controlverklaring naleving Baseline Informatiebeveiliging Rijksdienst (BIR) de afwijkingen in beeld gebracht, risico's benoemd en verbeterplannen opgesteld. Wij zien dat ministeries nu de stap moeten maken van verbeterplan naar daadwerkelijke implementatie van te nemen maatregelen. De maatregelen worden nu nog onvoldoende aantoonbaar gemaakt. Het opzetten van een zogenoemde Information Security Management

System (set van beleid, procedures, maatregelen en instrumenten die passen in een PDCA-cyclus) kan helpen om de effectiviteit van de beheersmaatregelen van de BIR te gaan monitoren. De regierol van DGOBR is in deze belangrijk. DGOBR is voornemens om haar monitoring rol in te vullen door onder meer halfjaarsgesprekken met de CIO's van de departementen.

2.2. Beheer bij legacysystemen blijft onder druk staan

De ICT bij grote uitvoerende diensten (zoals DUO, Belastingdienst) kent een aantal legacysystemen waar het beheer, onder meer door verouderde functionaliteit, onder druk staat. Dit levert een verhoogd risico op voor productieverstoringen. Vernieuwingen en aanpassingen als gevolg van bijvoorbeeld wijzigingen in wet- en regelgeving kunnen moeilijk worden doorgevoerd. De Belastingdienst neemt de problematiek rond legacysystemen mee in het traject van de investeringsagenda.

2.3. Toepassing IT-tooling nodig om in control te blijven

Het Rijk heeft te maken met een toenemende digitalisering van werkprocessen. Monitoringtools kunnen helpen om in control te blijven, mits deze zijn aangepast aan de nieuwe ontwikkelingen en de randvoorwaarden zijn vervuld.

2.3.1. Toepassing monitoringtools bij ministeries stap voor stap

De ADR heeft de afgelopen jaren bij een groot aantal ministeries geïnvesteerd in de inzet van IT-tooling op de bedrijfsvoeringsystemen en de daaraan gekoppelde relevante primaire systemen vooral vanuit de wettelijke controletaak. Deze investering is vooral ingegeven door de verdere digitalisering die door de ministeries voor de uitvoering van hun taken wordt ingezet.

Wij signaleren een positieve ontwikkeling dat zowel bij de eerste als tweede 'line of defence' binnen ministeries meer initiatieven ontstaan om IT-tooling te gaan gebruiken. Het daarbij voortvarend inbedden van IT-tooling in de planning en controlcyclus, gaat stap voor stap en verdient van de ministeries de volle aandacht om tot een optimale interne beheersing te komen. Zodra deze inbedding is gerealiseerd, is het voor de ADR bovendien mogelijk om meer te kunnen steunen op de monitoring van de ministeries zelf. Dit past bij de rol van de ADR als de derde 'line of defence'.

Wij hebben het SGO toegezegd om voor het einde van het jaar samen met elk ministerie een departementaal stappenplan te maken hoe te komen tot een volwaardige inzet van monitoringssystemen door de tweede 'line of defense'. Wij zullen u aan het einde van het jaar de voortgang terzake melden.

2.3.2. Randvoorwaarden voor de inzet van tooling verdient aandacht

Voor het effectieve gebruik van IT-tooling door ministeries en ADR moet een aantal noodzakelijke randvoorwaarden vooraf ingevuld zijn. Zo zal bijvoorbeeld de datakwaliteit in de systemen op orde moeten zijn. Ook dienen juiste systeeminstellingen aanwezig te zijn, zodat een betrouwbare logging beschikbaar is. Daarbij is diepgaande kennis van de systemen en processen noodzakelijk om de juiste analyses voor de IT-tools te definiëren. Op basis van onze ervaringen constateren wij regelmatig dat bij ministeries deze randvoorwaarden nog niet goed ingevuld zijn. Daardoor is de bruikbaarheid van de uitkomsten van analyses uit IT-tooling vaak nu nog beperkt.

Wij zien dat de aandacht bij de implementatie van nieuwe systemen vooral uitgaat naar de techniek. De impact van vernieuwingen in systemen op werkprocessen en medewerkers moet niet worden onderschat. Er is aandacht nodig voor de medewerkers om hen te ondersteunen in het veranderingsproces naar meer IT-gedreven werken en de benodigde (ICT) vaardigheden die dat vraagt.

3. Bedrijfsvoering verdient aandacht bij verandering

De veranderingen in inrichting van de rijksdienst en de wijzigingen in wet- en regelgeving vragen om een tijdige aanpassing van de bedrijfsvoering, om uitvoerings- en rechtmatigheidsproblemen te voorkomen.

3.1. Aandacht voor governance nodig bij (her-)inrichting Rijk

3.1.1. Kansen SSO's door samenwerking en meer transparantie

Het Rijk is in beweging. Steeds meer bedrijfsvoeringstaken worden ondergebracht bij rijksbrede Shared Service-Organisaties (SSO's), grote geldstromen worden overgeheveld naar gemeenten en vinden reorganisaties plaats. Doel is om de rijksdienst efficiënter en effectiever te maken.

SSO's zijn volop in beweging om de kwaliteit van hun dienstverlening te verbeteren en tegelijkertijd te voldoen aan de opdracht van doelmatigheid. Wij zien dat deze beide doelstellingen soms op gespannen voet met elkaar staan, omdat een hoge kwaliteit wordt verlangd tegen zo laag mogelijke kosten. Wij zien dat op sommige plekken het beheer binnen een SSO hierdoor nadelig wordt beïnvloed.
De verschuiving van verantwoordelijkheden van ministeries naar SSO's leidt tot een herziene verantwoordelijkheidsverdeling waarbij regie op de keteninrichting essentieel is, dat van invloed is op het in control zijn.
Een verdere stapeling van regie en verantwoording is niet de enige oplossing. De kansen liggen in samenwerking en transparantie, waarmee het vertrouwen tussen SSO's en ministeries wordt vergroot.

Samen met DGOBR wordt momenteel gewerkt aan een vergelijkende rapportage over SSO's. Deze zal in oktober in de begeleidingscommissie komen en daarna beschikbaar zijn voor het SGO.

3.1.2. Toezicht op uitvoering gedecentraliseerde taken in ontwikkeling

Sinds 1 januari 2015 heeft decentralisatie van taken van het Rijk naar gemeenten plaatsgevonden. Na de feitelijke transitie is nu aandacht nodig voor de correcte uitvoering van taken waarbij wordt voldaan aan de in de wet- en regelgeving opgenomen rechtmatigheidscriteria. Het toezicht op deze uitvoering en de wijze waarop informatie moet worden verkregen ten behoeve van het systeemtoezicht door het Rijk is nog in ontwikkeling.

3.2. Uitvoering regelgeving blijft punt van zorg

Wij zien dat in de komende periode nog verscherpte aandacht nodig is voor correcte toepassing van aanbestedingsregels, WNT en afrekening van voorschotten om rechtmatigheidsproblemen aan het einde van het jaar te voorkomen. In 2016 zal de invoering van de Vpb-plicht voor overheidsonderneming mogelijk leiden tot een toename van administratieve lasten. De ministeries dienen hierop qua kennis en kunde goed te zijn voorbereid.

3.2.1. Verscherpte aandacht nodig invoering nieuwe circulaire inkopen

Per 1 september 2015 is de nieuwe inkoopcirculaire in werking getreden voor de Rijksoverheid. De nieuwe grensbedragen vragen om aanpassing van bestaande procedures en processen. Bij een precieze uitvoering van de circulaire door de departementen is de verwachting dat de onvolkomenheid die de Algemene Rekenkamer vorig jaar op de Rijksbrede inkoopcirculaire had, wordt opgeheven.

Een aantal departementen zijn activiteiten gestart om de bewustwording van de wijziging te vergroten. De korte voorbereidingstijd tot de implementatie vraagt om verscherpte aandacht.

3.2.2. Verlaging norm in WNT II kan onvoorziene gevolgen hebben
Met ingang van 1 januari 2015 is het algemene bezoldigingsmaximum in de Wet Normering bezoldiging Topfunctionarissen publieke en semipublieke sector (WNT) verlaagd naar het niveau van een ministersalaris (EUR 178.000). De verlaging van de norm, ten opzichte van 2014, met 30% heeft mogelijk tot gevolg dat in 2015 meer (top)functionarissen de norm overschrijden en gepubliceerd moeten worden in het jaarverslag van de diverse departementen. Ook de handhaving van de normering van ontslagvergoedingen (EUR 75.000) vraagt in een tijd met vele reorganisaties extra aandacht van de departementen.

Alle departementen dienen over een adequaat proces te beschikken om de benodigde informatie op basis van de WNT op te kunnen leveren. In de WNT is opgenomen dat departementen ook moeten rapporteren over de onder hen ressorterende onderdelen (ZBO's zonder rechtspersoonlijkheid). Met name bij deze categorie vergt het verzamelen van de benodigde gegevens voor het WNT-overzicht veel tijd. Bij de departementen is structurele aandacht nodig voor de naleving van de WNT om een ongewenste piek aan werkzaamheden in de verantwoordingsperiode te voorkomen.

3.2.3. Evaluatie, uitvoering en wetswijziging WNT III vormt uitdaging
De ontwikkelingen met betrekking tot de WNT staan niet stil. De afgelopen maanden heeft BZK hard gewerkt aan de uitvoering en naleving van de WNT-1 en WNT-2, hun taken op het gebied van toezicht en handhaving, de uitvoering van de wetsevaluatie en de voorbereidingen van de WNT-3. Minister Plasterk heeft de Kamer de toezegging gedaan dat het wetsvoorstel voor de WNT-3 nog voor jaareinde wordt aangeboden.
Voor BZK ligt er een grote uitdaging om alle punten uit de wetsevaluatie zorgvuldig te verwerken in de WNT-3 en uitvoeringsproblemen, zoals bij de invoering van de voorgaande WNT-wetten, te voorkomen. Een zorgvuldige afstemming van de WNT-3 en de reeds voorgestelde wijzigingen met betrokken partijen is hiervoor noodzakelijk.

3.2.4. Beheer voorschotten onder vergrootglas
In de concept Rijksbegrotingsvoorschriften 2016, die gelden voor de verantwoording 2015, is een afzonderlijke rapporteringstolerantie opgenomen voor de stroom afgerekende voorschotten. Dit betekent dat het nodig kan zijn om met een grotere nauwkeurigheid naar deze stroom te kijken, met mogelijk meer rechtmatigheidsfouten tot gevolg. Risico's kunnen worden vermeden door bij de voorschottenadministratie strikt toe te zien op een goede dossiervoering en het periodiek monitoren van de voorschotten.

3.2.5. VPB-plicht leidt tot verhoging beheerslasten
Met ingang van 1 januari 2016 moeten alle ministeries aangifte vennootschapbelasting gaan doen voor de wet modernisering Vpb-plicht overheidsactiviteiten. Het is een veelomvattende administratieve operatie (o.a. het opstellen van een fiscale openingsbalans), waarvan het zeer wel denkbaar is dat administratieve/bestuurlijke lasten worden verhoogd. Het is belangrijk dat de rijksbrede werkgroep Vpb, waarin alle ministeries zijn vertegenwoordigd, de inventarisatie van de activiteiten die vrijgesteld zijn van Vpb bij de ministeries nauwgezet volgt. Daarnaast dient oog te zijn voor de op te bouwen (fiscale) kennis bij de betrokken ministeries.

BIJLAGE 1

Best Practices

Op het gebied van….ontwikkelingen IT

- Om makkelijker aan te kunnen tonen in welke mate aan de Baseline Informatiebeveiliging Rijk wordt voldaan is bij **Infrastructuur en Milieu/Rijkswaterstaat** een Information Security Management System-tool beschikbaar gesteld. Daarbij wordt een learning community opgericht, waarbij ook andere organisaties binnen de rijksoverheid kunnen aansluiten.

- **VenJ** bewaakt de beveiliging van de kritieke systemen (circa 80) met de zogenaamde Risicokaart. Hiermee wordt informatiebeveiliging risicogericht gestuurd.

- **Defensie** is actief bezig om in een pilot met de ADR de toegevoegde waarde van de inzet van tooling binnen het financieel domein te onderzoeken. Deze pilot wordt in het 3e kwartaal 2015 afgerond.

- De **Belastingdienst** streeft naar optimale dienstverlening voor burgers en bedrijven. Soms gaat daarbij iets mis of is onderhoud nodig. Om burgers hierover te informeren wordt op de website aangegeven welke verstoringen en onderhoudswerkzaamheden er zijn en welke mogelijke oplossingen er zijn. Ook wordt aangegeven welke problemen opgelost zijn.

Op het gebied van….nieuwe vormen van governance

- **VWS** heeft in samenwerking met betrokken partijen acties in gang gezet om de rechtmatigheid van de gedecentraliseerde geldstromen Jeugdzorg en Wmo voor het overgangsjaar 2015 te borgen. Zo zijn in nauwe samenwerking met de ADR de rechtmatigheidscriteria in de Jeugd- en Wmo wet-en regelgeving geïnventariseerd en is door de VNG, het project IZA, VWS en met advies van de NBA de "Modeloplegger rechtmatigheidvereisten Wmo 2015 en Jeugdwet" opgesteld en gepubliceerd.

- Bij P-Direkt **(BZK)** wordt periodiek een kosten-batenanalyse opgesteld. Binnen het project Optimaal Verbinden stuurt P-Direkt op de nog te realiseren baten zoals die blijken uit deze kosten-batenanalyse. Hiermee geven de departementen en P-Direkt invulling aan hun streven naar een optimale doelmatigheid.

Op het gebied van….kwaliteitsverbetering beheer

- De SG van **BZK** heeft een zogeheten risicobeheersmatrix, die hij hanteert voor het monitoren en sturen van de risico's (financieel, politiek, organisatorisch, imago). Iedere week overlegt hij met de departementale stafdirecteuren daarover en worden directeuren waar kwesties spelen uitgenodigd om een toelichting te geven.

- **Defensie** past kwaliteitssystemen toe die bijdragen aan de monitoring en verbetering van het beheer. Inmiddels zijn deze systemen operationeel (voor het materieel beheer MKM) of nog in ontwikkeling voor het personeelsbeheer (Kwaliteitssysteem personeelsbeheer Defensie) en de IT-systemen (Kwaliteitsplan IT). Deze kwaliteitssystemen kunnen een goede bijdrage leveren aan de monitoring en control van de processen.

- Een best practice bij **V&J** is de systematiek van de kwartaalafsluitingen. Dit leidt ertoe dat administraties in toenemende mate up to date zijn bijgewerkt. Het effect daarvan is voorts dat de jaarafsluiting een meer gestroomlijnd proces wordt. Daaraan gekoppeld is de afspraak gemaakt dat de ADR de kwartaalrapportages beoordeelt, zowel gericht op de kwaliteit van het primaire proces als op de rol die de concerncontroller (DFEZ) heeft bij de kwartaalafsluitingen.