Rapport van bevindingen *Assessment informatiebeveiliging 2021* provincie Utrecht

4e meting naar het organisatiebrede informatiebeveiligingsniveau

SAMENVATTING

Definitief

Colofon

DATUM	14-03-22
VERSIE & STATUS	1.2 definitief
PORTEFEUILLEHOUDER	Anneke Knol
OPDRACHTGEVER	Johan Luiks, concern controller
AUTEUR & AUDITOR	Victor Roos, concernadviseur, CCO M.J. van Zitteren RE, Q-RESULTANCY (secundant)
ONDERWERP	Samenvatting Rapport van bevindingen *Assessment informatiebeveiliging 2021* provincie Utrecht
VERSPREIDING	beperkte kring: algemeen directeur, concerncontroller, overige CMT-leden, leden stuurgroep IV&P, GS, PS

Inhoudsopgave

1 Inleiding

Achtergrond

De afgelopen jaren is veel in gang gezet om de informatieveiligheid binnen overheidsorganisaties en -lagen te verbeteren. In 2018 heeft met de AVG de bescherming van persoonsgegevens veel aandacht gekregen. In 2019 is de Baseline Informatiebeveiliging Overheid de standaard geworden voor Nederlandse overheden. Uit grootschalige cyberincidenten en datalekken die regelmatig het nieuws halen blijkt onverminderde dreiging en de noodzaak te blijven investeren in betere informatiebeveiliging. Ervaring leert dat echte informatiebeveiliging en zorgvuldige bescherming van persoonsgegevens pas wordt bereikt als we allemaal, van hoog tot laag, doordrongen zijn van het belang én van de risico's. Daarvoor is verscherping van het bewustzijn en concrete sturing op informatiebeveiliging binnen overheidsorganisaties nodig.

De provincies hebben sinds 2013 met ondersteuning van het IPO en de Taskforce de provinciale informatieveiligheid een impuls gegeven. Dit heeft eind 2014 geleid tot de ondertekening van het convenant interprovinciale regulering informatieveiligheid, waarin de provincies zich committeren aan een afsprakenkader en de verantwoordelijkheid nemen voor zelfregulering (het zelf borgen van een adequaat niveau van) informatieveiligheid. Bij de provincie Utrecht zijn sindsdien een scala aan onderzoeks- en verbeteractiviteiten ontplooid, gericht op het bereiken van een adequaat beveiligingsniveau en het verhogen van veilig gedrag van medewerkers. Assessments op dit onderwerp in 2015, 2017 en 2019 wezen uit dat de provincie Utrecht worstelt om dit beveiligingsniveau te bereiken.

Centrale onderzoeksvraag

In lijn met het afsprakenkader van het convenant interprovinciale regulering informatieveiligheid, geeft de provincie Utrecht ook invulling aan verantwoording en toezicht op dit onderwerp. De provincie Utrecht heeft zich gecommitteerd om zelf informatieveiligheid te reguleren en draagt de verantwoordelijkheid voor de te nemen maatregelen. (Zie B-stuk Zelfregulering informatiebeveiliging definitief, december 2014.) De provincie Utrecht zet voor het inrichten van haar zelfregulering stappen om de risico's rondom informatiebeveiliging af te wegen en passende maatregelen te treffen. Een van de onderdelen hiervan betreft het 1x per 2 jaar uitvoeren van een onafhankelijke toets (assessment) op *de staat van haar informatiebeveiliging*. Deze toets werd in 2015 voor het eerst uitgevoerd, in 2017 voor de 2e maal en in de 2e helft van 2019 voor de 3e maal. Dit onderzoek betreft de vierde toets in 2021. CCO (3e line of defense) organiseert de uitvoering. "De bevindingen hiervan worden in de vorm van een control- of auditrapport aan bestuur en management gerapporteerd" (citaat uit het convenant).

De doelstellingen van het assessment op informatiebeveiliging zijn:

1. Inzicht geven in het informatiebeveiligingsniveau van de provincie Utrecht.
2. Inzicht geven in de implementatiestatus van het beleid informatiebeveiliging.
3. Voldoen aan de vereiste van onafhankelijke toets uit het convenant interprovinciale regulering informatieveiligheid, onderdeel verantwoording en toezicht.

De resultaten van 1 en 2 zijn opgenomen in het dashboard informatiebeveiliging. Bestuur en management kunnen met het dashboard de ontwikkeling van de provincie Utrecht op het vlak van informatiebeveiliging volgen en zonodig bijsturen, wanneer de bevindingen en/of externe ontwikkelingen daartoe aanleiding geven.

Het dashboard informatiebeveiliging geeft de staat van de informatiebeveiliging weer langs de volgende onderwerpen:

Beleid (normen)	Relevante wet- en regelgeving, overheidsbeleid en normen voor informatiebeveiliging volgen en adopteren
Risicoanalyses	Identificeren, analyseren en behandelen van informatiebeveiligingsrisico's
IB-beleid en plan	Onderhouden van beleid voor informatiebeveiliging, afgestemd op strategische doelen en risico's
Uitvoering	Beheersen van de veiligheid van informatie (mensen, processen, techniek) en daarover rapporteren
Continuïteit	Waarborgen van de continuïteit van provinciale taken & dienstverlening na uitval/verstoring ICT
Ketens	Samenwerken en sturen op afspraken over informatiebeveiliging met leveranciers, afnemers, partners

Aansluiten	Aansluiten op relevante diensten en samenwerkingsverbanden voor bijschakelen kennis en kunde
Incidentmanagement	Informatiebeveiligingsincidenten systematisch voorkomen, detecteren, isoleren, herstellen
Toetsing en verantwoording	Toetsen en verantwoorden over regulering informatiebeveiliging (mate van in control zijn)
Evaluatie	Evalueren ontwikkelingen, incidenten, processen en heroverwegen risico's, risicobehandeling en beleid
Leerstrategie	Strategie voor en uitvoering van organisatieleren op het gebied van informatiebeveiliging

De bovengenoemde onderwerpen en de vraagstelling zijn door CCO verder uitgewerkt in het referentiekader dat sinds de nulmeting in 2015 gehanteerd en wanneer nodig geactualiseerd wordt. (In dit referentiekader wordt verwezen naar de normen uit de Baseline Informatiebeveiliging Overheid (BIO).

In mei 2021 is het concernbrede risicobeeld informatiebeveiliging en privacy geactualiseerd. Hierin zijn de belangrijkste risico's die de provincie loopt op deze gebieden geïdentificeerd. Gezien de relatie tussen deze risico-identificatie en het object van onderzoek is verbinding gelegd tussen de bevindingen en de aangetroffen risico's. De risico's uit het risicobeeld geven relevante informatie over de mate waarin de provincie Utrecht het niveau van informatiebeveiliging reguleert.

2 Samenvatting bevindingen

In dit hoofdstuk zijn de belangrijkste resultaten van het assessment informatiebeveiliging 2021 opgenomen, dat door CCO is uitgevoerd met ondersteuning van Q-RESULTANCY. Met het assessment informatiebeveiliging wordt voldaan aan de vereiste van onafhankelijke toets uit het convenant interprovinciale regulering informatieveiligheid, onderdeel verantwoording en toezicht. Het rapport geeft inzicht in het informatiebeveiligingsniveau en de implementatiestatus van het beleid informatiebeveiliging van de provincie Utrecht.

Introductie

In de afgelopen 2 jaar heeft de organisatie de aanpak van informatiebeveiliging en privacy ondergebracht bij het programma IV&P. Het programma heeft de beschikking gekregen over de beschikbare expertise (alle specialisten) en de capaciteit daarvan is in deze periode bijna verdubbeld. (4 information security officers (ISO's), 1 technical information security officer (TISO), 3 privacy officers (PO). Het programma heeft een regisseur gekregen voor versterking van de sturing en de verbinding met de lijn, het management en het bestuur.

Uit het onderzoek is gebleken dat er veel geïnvesteerd is in verbinding, het verbeteren van kennis en bewustwording. Dit wordt door de lijn ervaren en de bekendheid met het onderwerp en de spelers van IV&P is duidelijk gegroeid. De oprichting van het leernetwerk heeft hieraan bijgedragen. In de afgelopen 2 jaar is het overkoepelende beleid voor informatiebeveiliging (IB) vernieuwd en zijn op verschillende onderwerpen specifieke beleidsuitwerkingen en richtlijnen opgesteld. Daarnaast werkt het programma de laatste maanden aan de versterking van de weerbaarheid door het opstellen van een incident respons-plan, het organiseren van een crisisteam daarvoor ("CERT") en het oefenen met fictieve cyberaanvallen. Het programma heeft de afgelopen periode ook gestaag gewerkt aan het in kaart brengen van IV&P-aspecten bij applicaties met het uitvoeren van korte scans ("BIA").

De extra inspanning van het programma wordt ervaren door de organisatie, maar de ontwikkeling in volwassenheid van de processen op het gebied van informatiebeveiliging gaat moeizaam. De bevindingen uit dit onderzoek duiden de problemen die de ontwikkeling van de volwassenheid tegenwerken. Voor een goed begrip van deze bevindingen is het van belang deze te plaatsen in de context van wat nodig is voor het vasthouden van het minimum procesvolwassenheidsniveau 2 en het bereiken van de ambitie procesvolwassenheidsniveau 3 over de volle breedte van de organisatie. De bevindingen beschrijven de belangrijkste problemen (naar de mening van de auditors de waarschijnlijke oorzaken) die –ondanks alle inspanningen- verhinderen dat de organisatie op het gebied van informatiebeveiliging kan groeien naar niveau 3.

Feitelijke bevindingen

De onderzoekswerkzaamheden hebben de bevindingen in hoofdstuk 3 opgeleverd, waarvan de belangrijkste hieronder zijn samengevat:

I. *Gebrek aan opvolging aanbevelingen uit onderzoeken en aan implementatie van beveiligings-maatregelen bij risico's*
   De opvolging van aanbevelingen uit onderzoeken (assessment, risicobeeld, digitrust meting, selfassessments, pentesten) is niet concreet terug te vinden in werkplannen en actielijsten. De organisatie beschikt over een standaard werkwijze voor het bepalen van risico's op het gebied van informatiebeveiliging en privacy bij processen, wat heeft geresulteerd in 25 korte scans om situaties in kaart te brengen. Opvolging van risico's met nadere analyses informatiebeveiliging en voorschrijving, ontwerp en implementatie van aanvullende beveiligingsmaatregelen vindt nog weinig plaats. Met VKA worden de werkwijze en vaardigheden verbeterd.

II. *De lijn is verantwoordelijk voor IV&P, maar beschikt niet over de benodigde expertise en rapporteert er niet over*
   De lijn is verantwoordelijk gesteld voor IV&P, d.w.z. het implementeren van de basismaatregelen van de baseline informatiebeveiliging overheid (BIO) en waar nodig aanvullende maatregelen. In de domeinplannen wordt IV&P als onderwerp genoemd dat structurele verbetering vraagt. Het programma faciliteert en adviseert alleen en beschikt daarvoor over de beschikbare expertise (alle specialisten). Dat wringt, te meer omdat de lijn niet over de benodigde expertise beschikt om

door te vragen, adviezen op te volgen en maatregelen te implementeren, het voor de lijn niet altijd duidelijk is wat precies verwacht wordt en de lijn verwijst naar de wasstraat. Het is de vraag hoe de lijn verantwoordelijk kan zijn voor IV&P als de processen en expertise daarvoor niet zijn overgedragen aan de lijn. Zolang dat niet gebeurt moet het programma zorgdragen voor de uitvoering van reguliere operationele activiteiten. In dat kader mag van adviseurs worden verwacht dat zij instappen om mee te helpen bij concrete processen en situaties in de lijn die om maatwerk vragen. Het programma rapporteert concernbreed aan CMT en bestuur, maar draagt die uitvoeringsverantwoordelijkheid niet, waardoor de voortgang in de lijn onderbelicht blijft.

III. *Plannen en rapportages activiteitgericht, niet resultaatgericht*
In het programmaplan zijn de programmadoelen voor IV&P duidelijk geformuleerd. In het programmaplan, de werkplannen en de voortgangrapportages is niet terug te vinden welke concrete resultaten moeten worden behaald voor het bereiken van de IV&P-doelen. Er wordt op basis van activiteiten gewerkt en gerapporteerd. De privacy-activiteiten zijn wel duidelijk beschreven. Er is geen helder beeld van welke resultaten moeten worden opgeleverd voor overdracht naar de lijn en hoever de realisatie daarvan gevorderd is.

IV. *Versterking governance IV&P langs managementcyclus nog niet in gang gezet door CMT; het programma kan slechts verleiden en faciliteren*
Naar aanleiding van het assessment informatiebeveiliging 2019 heeft de organisatie aan PS toegezegd dat de governance IV&P zal worden versterkt met een focus op eigenaarschap en verantwoording over de beheersing van risico's op het gebied van informatiebeveiliging en privacy, evenals het monitoren of acties het gewenste effect hebben door het uitvoeren van testen en inbedding in de interne managementcyclus. Er is nog geen rapportagelijn over de domeinen in ontwikkeling. Het CMT stuurt niet actief op het aanpakken van informatiebeveiliging- en privacyrisico's en heeft opname ervan in managementcontracten afgewezen. De inbedding in de managementcyclus is daarmee nog niet tot stand gekomen. De concernbrede sturing vanuit het CMT vindt reactief plaats op geagendeerde stukken die vaak hamerstuk zijn (gemaakt). Opvolging van besluiten wordt niet gevolgd. Het CMT laat de sturing daarmee vooral aan het programma IV&P. De betekenis van het voorgaande is dat de organisatie van het CMT ten aanzien van informatiebeveiliging en privacy geen bijzondere prioriteit ervaart en de versterking van het eigenaarschap en de actiegerichtheid bij de managers achterblijft. Het programma IV&P moet daardoor de organisatie verleiden, faciliteren, aanjagen en kan het niet scherp spelen.

V. *Het programma worstelt met IB-vraagstukken door ontoereikende inhoudelijke aansturing*
Het programma IV&P worstelt met een aantal inhoudelijke vraagstukken (vooral het beleidsproces, het risicogebaseerd werken en het kwaliteitsysteem) die een rem zetten op de vooruitgang van met name informatiebeveiliging. De ontwikkelstappen voor groei naar een hoger volwassenheidsniveau zijn niet duidelijk geformuleerd. Er is meer inhoudelijke aansturing nodig die tot dusver nog ontoereikend is gegeven door het programma of de CISO. Competenties op het gebied van informatiebeveiliging in relatie tot de 3 genoemde inhoudelijke vraagstukken verdienen extra aandacht. Voor risicogebaseerd werken is dit in gang gezet, met hulp van VKA.

VI. *Onvolledig zicht en grip op incidenten, geen lering en zicht op oorzaken*
De organisatie heeft onvolledig zicht en grip op incidenten met betrekking tot informatie-beveiliging en privacy. Het programma IV&P heeft een eigen excel die gebruikt wordt voor vast-legging en opvolging van vragen en incidenten komende vanuit de e-mailboxen van IV&P. Er is echter geen centrale registratie waar verschillende interne en externe bronnen samenkomen en incidenten blijven daardoor onder de radar. Incidenten worden gezien als operationele zaken (actie gericht op herstel operatie) en niet als bron om te leren. Er wordt bijvoorbeeld geen lering getrokken uit het majeure BIJ12-incident met behulp van oorzakenanalyse, evaluatie en aanbevelingen. Zonder een grondhouding om te willen leren van *alle* incidenten (niet alleen de grote) krijgt de PU geen zicht op de grondoorzaken van incidenten.

VII. *Onvoldoende leveranciersmanagement bij omvangrijke uitbesteding*
De organisatie gaat mee in de trend van toenemende uitbesteding van informatieverwerking en ICT. Daarnaast zijn er veel samenwerkingsverbanden met partners. Informatiebeveiliging en privacy wordt in toenemende mate meegenomen in overeenkomsten. Stappen vooruit op het gebied van eigenaarschap, inkoopcontracten en leveranciersmanagement zijn onderhanden bij IJS

en IEA. Bij veel oudere overeenkomsten is dit echter niet goed geregeld. Daarnaast is aansturing op en monitoring van beveiligingsafspraken met leveranciers nog zwak geregeld, mede veroorzaakt door onderontwikkeld assetbeheer en eigenaarschap.

Procesvolwassenheid

Per onderdeel van het dashboard informatiebeveiliging heeft een inschaling van procesvolwassenheids-niveau's plaatsgevonden. De resultaten worden hieronder weergegeven, afgezet tegen de resultaten van de 0-meting uit 2015, de 1-meting uit 2017 en de 2-meting uit 2019. In 2016 zijn doelen vastgesteld voor het procesvolwassenheidsniveau: minimum 2, ambitie 3.

Schaal:

- 5 Geoptimaliseerd
- 4 Gemanaged
- 3 Gedefinieerd (= ambitie)
- 2 Herhaalbaar (= minimum)
- 1 Initieel
- 0 Niet aanwezig

Dashboard informatie-veiligheid	Volwassenheids-niveau 2015	Volwassenheids-niveau 2017	Volwassenheids-niveau 2019	Volwassenheids-niveau 2021
Beleid & normen	1	1	1	1
Risicoanalyse	1	1	2	1
Uitvoering	1	1	1	1
Continuïteit	1	1	1	2
Ketens	1	1	1	1
Aansluiten	2	2	2	2
Incidentmanagement	1	1	2	1
Toetsing & verantwoording	1	1	1	1
Evaluatie	1	1	1	1
Leerstrategie	1	2	1	2

Uit de ontwikkeling van de volwassenheid van de processen komt naar voren dat de organisatie moeite heeft om niveau 2 vast te houden. In 2019 werd niveau 2 bereikt bij risicoanalyse en incidentmanagement, maar deze zijn weer teruggevallen naar niveau 1. De onderdelen continuïteit en leerstrategie hebben extra aandacht gekregen, wat heeft geleid tot groei naar niveau 2. In het algemeen is niveau 2 kwetsbaar voor terugval naar 1. Het is belangrijk vast te houden aan de ambitie om niveau 3 te bereiken voor een goede regulering van het beveiligingsniveau. In procesvolwassenheid kan echter geen niveau worden overgeslagen. Het bereiken en behouden van niveau 2 over de brede linie moet daarom het eerste doel zijn.

Het bepalen van de volwassenheid van privacy-processen is buiten de scope van dit onderzoek, maar er ligt een duidelijke relatie met informatiebeveiliging, ook in de aanpak het programma IV&P. Het is daarom van belang te vermelden dat de auditors de indruk hebben dat de volwassenheid van privacy-processen zich goed ontwikkelt.

3 Aanbevelingen

Hieronder zijn de aanbevelingen opgenomen waarbij de aansluiting wordt gemaakt met de hoofdbevindingen uit de managementsamenvatting. In de verbetering van de regulering van informatiebeveiliging zal het zwaartepunt moeten liggen op het verlagen van risico's en het opvolgen van aanbevelingen met een procesgerichte aanpak uitgevoerd door een IV&P-lijnorganisatie. Daar waar [3] is vermeld is sprake van een aanbeveling die bedoeld is voor het bereiken van procesvolwassenheidsniveau 3.

I. *Neem de aanbevelingen en hoge risico's mee naar actiemanagement en sturingsrapportage en stuur vanuit CIO-office op de opvolging en afdoening.*

- Aanbevelingen uit onderzoeken onder actiemanagement brengen.
- Opvolging hoge risico's (zoals in risicobeeld) opnemen in managementcyclus.
- Periodieke sturingsrapportage op basis van actiemanagement en risicobeeld.

II. *Zorg dat lijn haar verantwoordelijkheid voor informatiebeveiliging kan waarmaken door begrijpelijke kaders en expertise beschikbaar te stellen die helpt met implementeren van beveiligingsmaatregelen en/of de dienstverlener aan te sturen*

- Dit geldt voor zowel de basismaatregelen als voor de aanvullende maatregelen (maatwerk) in specifieke processen en ondersteunende systemen waar dat vanwege risico's nodig is.
- Zorg voor structurele monitoring en evaluatie van de werking van beveiligingsmaatregelen [3].
- Zorg daarbij voor functiescheiding tussen uitvoering en toetsing [3].
- Versterk de kennis van de IB-professionals op het gebied van techniek en informatievoorziening en ICT in de primaire processen, zodat zij kunnen helpen met implementeren of leveranciers aansturen.
- Voor begrijpelijke kaders zie V.

III. *Transformeer de aanpak naar het inrichten en op gang brengen van IB-processen op basis van de vereisten voor het procesvolwassenheidsniveau – eerst 2, later 3*

- Wijs proceseigenaren aan, werk procesdoelen uit op basis van de te bereiken volwassenheid en evalueer hoe het proces presteert ten opzichte van deze doelen (maak meetbaar [3]); gebruik het kwaliteitssysteem daarvoor en maak een afgewogen keuze voor het te hanteren volwassenheidsraamwerk.
- Werk uit hoe de IV&P-lijnorganisatie eruit ziet die deze processen gaat uitvoeren, zowel centraal als decentraal
- Breng de programmacapaciteit naar rato terug naar de lijnorganisatie bij overdracht van lopende processen.
- Werk de rol voor het decentrale IV&P-aanspreekpunt uit.

IV. *Versterk de governance IV&P in lijn met de toezegging aan PS.*

- De CIO-office neemt de regie voor inbedding van beheersing van risico's op het gebied van informatiebeveiliging en privacy in de managementcyclus (rapportagelijn over de domeinen, aanpak risico's in managementcontracten); de CMT-leden brengen dit in praktijk met ondersteuning van de CIO-office.
- De CMT-leden tonen eigenaarschap van IV&P, stellen beleidskaders afkomstig van de CIO-office hiervoor vast en dragen ter verbetering van de actiegerichtheid het belang ervan goed uit in het CMT, MT en managementgesprekken.
- De CIO-office behandelt periodiek de sturingsrapportage, stuurt bij wanneer opvolging achterblijft en informeert het CMT.
- Het CMT benadrukt het belang van actuele kennis op het gebied van informatiebeveiliging en privacy en geeft daarbij zelf het goede voorbeeld met het volgen van een training.

V. *Versterk de inhoudelijke sturing en pas die toe bij de procesgerichte aanpak.*

- Werk in de CIO-office concreet met beleidskaders uit waar de inhoudelijke SOLL-situatie uit bestaat, waar de domeinen zich aan moeten houden en welke resultaten wanneer door wie moeten worden bereikt (nog ontbrekende beleidskaders en richtlijnen, beheersing van risico's door het treffen van maatregelen, concretisering van basisbeveiligingsmaatregelen, inrichting en gebruik kwaliteitssysteem, monitoring en aansturing leveranciers).

- Naast de voorgaande inhoudelijke SOLL-agenda ontwikkelt de CIO-office ook een SOLL-agenda voor professionalisering en het bereiken van het procesvolwassenheidsniveau (eerst 2, later 3), zie aanbeveling III.
- Breng de CISO in positie voor inhoudelijke kaderstelling en sturing vanuit de CIO-office, onafhankelijk van het programma. Dit impliceert een meer kaderstellende en minder toezichthoudende invulling van deze rol.
- Voeg een functionele aansturingslijn toe van de CISO naar de ISO's.
- Stuur op volledige rolinvulling in lijn met de functieprofielen voor de IB-professionals.
- Versterk kennis en vaardigheden van de IB-professionals met betrekking tot het opstellen van (specifiek) beleid en richtlijnen, het specifiek concretiseren van BIO-maatregelen naar de organisatie, het risicogebaseerd werken en het inrichten van en werken met een kwaliteitssysteem (ISMS).

VI. Volg incidenten op met een centrale registratie en gebruik incidenten als bron om te leren

- Zet een centrale registratie op voor beveiligingsincidenten en breng daar informatie over beveiligingsincidenten uit verschillende bronnen (e-mailboxen IV&P, FAC, IEA, bedrijfskritieke leveranciers) samen voor opvolging, afdoening en evaluatie.
- Evalueer periodiek het incidentenbeeld vanuit het perspectief van dreigingen, risicobeheersing, verbetering van processen, bijvoorbeeld aansturing van leveranciers en leerstrategie [3].
- Evalueer grote incidenten, leg de lessen vast in een evaluatierapport met grondoorzakenanalyse en neem deze mee naar actiemanagement.

VII. Breng en houd IB-afspraken in contracten met leveranciers in beeld en stuur risicogebaseerd op naleving

- Zorg voor inzicht in alle contracten met relevant aandeel IT en de mate waarin afspraken zijn gemaakt over informatiebeveiliging en privacy. Begin met bedrijfskritieke leveranciers. Overige leveranciers [3].
- Versterk het assetbeheer om te komen tot een sluitend en actueel overzicht van assets.
- Ontwikkel verschillende regimes voor leveranciersmanagement gericht op de naleving van IB-contractafspraken op basis van de risico's die worden gelopen in de processen die afhankelijk zijn van deze contracten [3].
- Beoordeel welke risico's worden gelopen bij (oudere) contracten zonder goede IB-afspraken.
- Breng het risicogebaseerd leveranciersmanagement in praktijk, door contracteigenaren (teamleider of domeinmanager) te ondersteunen met instrumentatie (checklists, voorbeeldbrieven) en advies, zie ook aanbeveling II.