

DR RAPPORTAGE CONCERNCONTROL

DEFINITIEF

**CONCERNCONTROL
MEI 2021**

Inhoud

1. Inleiding	3
2. Aandachtsgebieden bij onze audit.....	4
3. Wat rapporteren we per aandachtsgebied?.....	5
3.1 Beslispunten	6
4. Gemeentebreed beeld	7
5. Ontwikkelingen	8
5.1 Gemeentebreed	8
5.1.1 Follow-up aanbevelingen CC en (IT)ML	8
5.1.2 Rechtmatigheidsverantwoording (RV)	9
5.1.3 Datagedreven werken Concerncontrol	11
5.1.4 Risicomanagement	12
5.1.5 In Control Statement (ICS)	13
6. Uitkomsten onderzoeken	14
6.1 Bedrijfsvoering	14
6.1.1 IT Governance.....	14
6.1.2 Informatiebeveiliging	15
6.1.2 VIC Bedrijfsvoering	16
6.2 Sociaal Domein.....	20
6.2.1 TOZO/TONK.....	20
6.2.2 Onderzoek procesreconstructie Summa/Ster College.....	21
6.2.3 VIC SD.....	22
6.3 Ruimtelijk Domein	24
6.3.1 VIC RD	24
6.4 Bureau FG.....	27
6.5 Overige onderwerpen	29



1. Inleiding

Inleiding

Concerncontrol (CC) streeft er naar minimaal twee keer per jaar een DR-rapportage uit te brengen. In september 2020 hebben wij de laatste DR-rapportage uitgebracht, die ook ter kennisname is gedeeld met het College.

Deze rapportage bevat de uitkomsten van de onderzoeken die tot en met april 2021 zijn afgerond. We onderscheiden beslispunten en punten ter kennisgeving voor de DR.

Tevens zijn in deze rapportage naast de 'harde' bevindingen een aantal 'zachte' elementen (zoals cultuur) opgenomen, die wij graag onder de aandacht brengen. Daarnaast is ook info van bureau FG opgenomen dat dit jaar bij Concerncontrol is gekomen.

Veel inzet van CC was vorig jaar en ook dit jaar nog gericht op voorbereiding/opzet van de verplichte rechtmatigheidstoets in de vorm van opzetten en uitvoeren van werkprogramma's. Het effect daarvan – het resultaat van de daadwerkelijke toetsing – is nu zichtbaar.

De uitkomsten van onze VIC-onderzoeken worden niet meer vastgelegd in afzonderlijke rapportages om hiermee het rapporteren efficiënter en eenduidig te maken. De teksten uit deze DR-rapportage hebben wij in het kader van hoor- wederhoor afgestemd met de betreffende sector respectievelijk proceseigenaar. We hebben ons hierbij zo veel mogelijk beperkt tot de meest zwaarwegende bevindingen uit onze onderzoeken waarop spoedig acties benodigd zijn om rechtmatigheids- en beheersingsrisico's te reduceren. Echter is er op sommige punten meer detail zichtbaar dan in onze eerdere rapportages.

Leeswijzer

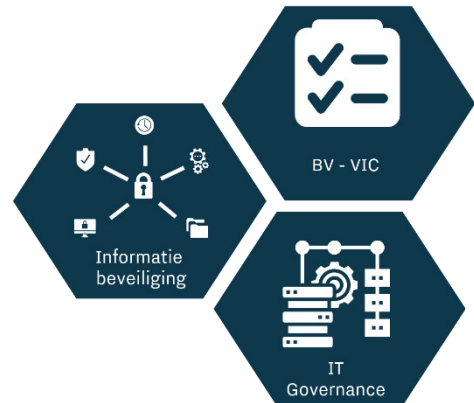
In hoofdstuk 2 zijn de aandachtsgebieden genoemd van de uitgevoerde onderzoeken. In hoofdstuk 3 zijn de beslispunten opgenomen. Vervolgens geven wij in hoofdstuk 4 het gemeentebrede beeld weer, en in hoofdstuk 5 en 6 per aandachtsgebied de meest noemenswaardige bevindingen /informatie.

2. Aandachtsgebieden bij onze audit

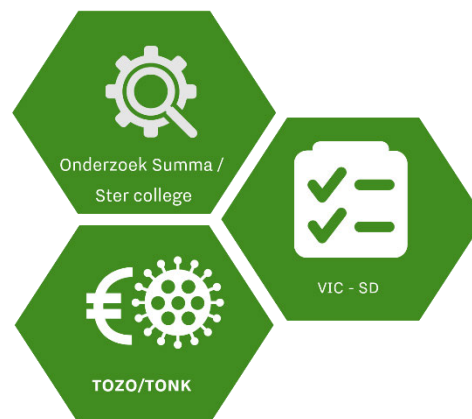
Gemeentebrede ontwikkelingen (5.1)



Bedrijfsvoering (6.1)



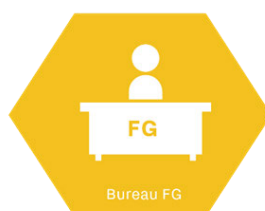
Sociaal Domein (6.2)



Ruimtelijk Domein (6.3)



Bureau FG (6.4)



Overige onderwerpen (6.5)



3. Wat rapporteren we per aandachtsgebied?

Bevinding De bevindingen die we hebben voor een bepaald aandachtsgebied	Onderwerp Het onderwerp dat extra aandacht vereist binnen het aandachtsgebied
Sterk Punt Volgens ons is dit een werkwijze die als voorbeeld kan dienen voor de organisatie/ het proces/het project. Alleen vermeld indien relevant.	Verbeterpunten Volgens ons is dit een punt waarop het proces kan verbeteren en/of kan leren van andere sectoren
Beslispunt/Ter Kennisgeving Beleggen van de verantwoordelijkheid tot uitvoering van verbeterpunten in de organisatie met daar aan gekoppeld een termijn. Sommige punten ter kennisgeving hier is geen actie nodig. Datum afhandeling is gebaseerd op een inschatting van CC voor wat betreft de haalbaarheid in relatie tot complexiteit en/of urgentie	Uitzonderingsrapportage Dit rapport bevat de meest zwaarwegende bevindingen die uit onze onderzoeken naar voren zijn gekomen.



3.1 Besispunten

*

Nr.	Aandachtsgebied	Besispunt
1	[REDACTED]	[REDACTED]
2	BV-IT Governance	Opdracht geven aan sectorhoofd I&B en CIO om zorg te dragen voor tijdige en goede overdracht aan de opvolgers van externe medewerkers op sleutelposities. In het verlengde hiervan zorgdragen voor vastlegging van gemaakte keuzes en genomen besluiten.
3	BV-Informatiebeveiliging	Geef CIO/CISO opdracht zo spoedig mogelijk daadkrachtig aan de slag te gaan met de implementatie van de BIO (waar ook het wachtwoord/toegangsbeleid en de bedrijfscontinuïteit deel van uit maken).
4	[REDACTED]	[REDACTED]
5	[REDACTED]	[REDACTED]
6	[REDACTED]	[REDACTED]
7	[REDACTED]	[REDACTED]
8	[REDACTED]	[REDACTED]
9	[REDACTED]	[REDACTED]
10	[REDACTED]	[REDACTED]
11	[REDACTED]	[REDACTED]

6.1.2 Informatiebeveiliging



Overzicht bevindingen informatiebeveiliging

CC heeft interne reviews uitgevoerd op de DIGID audits en Suwinet in het kader van de ENSIA verantwoording, het wachtwoordbeleid en een aantal andere beleidsstukken in het kader van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). CC heeft vastgesteld dat het proces rondom de DIGID audits en de Suwinet audit nu goed is verankerd in de organisatie, voor het 2^e jaar op rij zijn deze op een eenduidige en gestructureerde manier uitgevoerd en vastgelegd. Verbeterpunt dat uit de reviews naar voren komt is een al eerder geconstateerde bevinding door CC en Deloitte dat de verstrekte Third Party Mededelingen (TPM) die Eindhoven ontvangt van leveranciers beoordeeld moeten worden en dat indien er sprake is van beperkingen in de verklaring de risico's hieraan verbonden voor de interne bedrijfsvoering (zichtbaar) moeten worden afgewogen.

CC benadrukt wel dat de externe auditor (en ook CC) alleen audits hebben uitgevoerd op de DIGID koppelingen Suwinet. De overige onderdelen van de ENSIA verantwoording zijn een zelfevaluatie die niet worden gecontroleerd door de externe auditor. CC heeft hier in het verleden wel reviews op uitgevoerd en hier aanbevelingen voor gedaan (zie ook hieronder opmerking over implementatie BIO).

De voortgang van de implementatie van de BIO is nog steeds een zorgpunt. Weliswaar zijn recentelijk een aantal beleidsdocumenten (waaronder het wachtwoord/toegangsbeleid) opgeleverd maar deze voldoen naar de mening van CC nog niet aan de daar aan te stellen eisen. Recente beveiligingsincidenten bij onder andere gemeente Hof van Twente en gemeente Lochem en de universiteit van Maastricht laten zien dat hier meer urgentie en daadkracht geboden zijn.

Indien onze organisatie onverhoopt te maken krijgt met een ernstig (cyber)security incident dan zijn we hierop onvoldoende voorbereid. Aanbevelingen over business impact analyses en continuïteitsplannen zijn nog niet of deels (documenten die al langere tijd de status concept hebben) opgevolgd. Een samenhangend beeld van hoe dan te handelen is onvoldoende gewaarborgd en nog nooit geoefend. De plannen om deze aanbevelingen op te lossen hebben een erg lange (te lange) doorlooptijd. Risico is dat we als zich een incident voordoet niet weten hoe te handelen, waarde prioriteiten liggen en het meer capaciteit, tijd en kosten met zich meebrengt dan wanneer we ons goed voorbereiden.

Sterke punten

Verankering en vastlegging van de informatie voor de externe audits op DIGID en Suwinet in het kader van de ENSIA verantwoording binnen de organisatie.

Onderwerp	Advies
Beoordeling Third Party Mededelingen (TPM)	Voer conform eerdere aanbevelingen beoordelingen uit van de ontvangen TPM-verklaringen en weeg indien er sprake is van beperkingen de risico's voor de interne bedrijfsvoering.
Urgentie en daadkracht informatiebeveiliging noodzakelijk	Geef prioriteit aan de implementatie van de BIO. Stel hiertoe een implementatieplan op waarin duidelijke mijlpalen en planningsmomenten zijn beschreven. Rapporteer conform eerder DR besluit ieder kwartaal aan de DR over de voortgang.
	Geef prioriteit aan het opstellen en vaststellen van het gemeentebrede wachtwoord/toegangsbeveiligingsbeleid.
	Zorg voor een samenhangend beleid omtrent hoe te handelen in geval van een ernstig (cyber)security incident.

Beslispunt 3

Geef CIO/CISO opdracht zo spoedig mogelijk daadkrachtig aan de slag te gaan met de implementatie van de BIO (waar ook het wachtwoord/toegangsbeleid en de bedrijfscontinuïteit deel van uit maken).

6.4 Bureau FG



Ter kennisgeving Bureau FG

Hieronder zijn bevindingen opgenomen over de status van de basis AVG-verplichtingen per eerste kwartaal 2021.

Datalekken: in het eerste kwartaal van 2021 zijn in totaal 49 meldingen van datalekken opgenomen in het datalekkenregister van de gemeente. Bij 2 meldingen is sprake van een onvolledige registratie omdat de noodzakelijke informatie niet is verstrekt door de sectoren.

Van de 49 datalekken zijn er 5 van zodanige ernstige aard dat een melding is gedaan bij de Autoriteit Persoonsgegevens (AP). Bij 2 van deze 5 meldingen is de melding te laat gedaan (na de verplichte wettelijke termijn van 72 uur). Als reden werd gegeven dat onvoldoende tijd en capaciteit beschikbaar was om de benodigde informatie op tijd te verstrekken. Deze reden geldt niet als legitieme reden. Hiermee is de gemeente in overtreding van de AVG.

Bij 12 van deze 50 meldingen van datalekken heeft de verantwoordelijke sector betrokkenen (degenen die zijn getroffen door het datalek) geïnformeerd over het datalek. In 2 gevallen is het advies gegeven om betrokkenen te informeren vanwege de mogelijke impact op betrokkene, maar is dit advies niet gevolgd.

Uitgelicht: in het eerste kwartaal van 2021 is een melding datalek gedaan als gevolg van een hack bij een door de gemeente ingeschakelde externe verwerker. Dit is de eerste keer dat deze situatie zich heeft voorgedaan. De verwerker heeft een datalek-onderzoek uitgevoerd en de desbetreffende sector geïnformeerd over de resultaten. Hieruit kwam naar voren dat de kans als zeer klein (0,1%) werd ingeschat dat persoonsgegevens onderdeel zijn geweest van de hack. Ook zijn preventieve maatregelen getroffen door de verwerker (opbouw nieuwe beveiligde omgeving, uitvoeren van software updates). Van het incident is tijdig melding gedaan bij de AP. De situatie is aanleiding geweest om de betrokken sector te adviseren de verwerking alsnog op te nemen in het verwerkingsregister. Ook bleek dat er geen verwerkersovereenkomst was gesloten met de verwerker, waardoor de wettelijk verplichte afspraken tussen de gemeente, als verwerkingsverantwoordelijke, en de verwerker niet zijn vastgelegd. Geadviseerd is dit alsnog te doen

Verwerkingsregister: het completeren van het verwerkingsregister blijft achter. Na het eerste kwartaal van 2021 is nog altijd ongeveer 15% van het aantal verwerkingen niet compleet opgenomen in het register. Met niet compleet wordt bedoeld dat niet alle verplichte velden zijn gevuld.

DPIA's. In het eerste kwartaal van 2021 zijn 5 DPIA trajecten door de organisatie afgerond.

Het gaat om:

- Control: inwonersenquête;
- P&O: verzuimregistratie
- RU: verzorgen van zwemlessen
- SD: vroeg signalering
- PuCo: opname telefoongesprekken KCC

Bij de DPIA opname telefoongesprekken KCC is afgeweken van het FG advies bij deze DPIA.

In het eerste kwartaal van 2021 zijn 11 nieuwe DPIA trajecten gestart. Er lopen op dit moment nog 57 DPIA trajecten en er zouden nog 32 DPIA trajecten moeten starten.

In het eerste kwartaal van 2021 is de eerste voorafgaande raadpleging bij de AP in gang gezet. Dit betrof een uitgevoerde DPIA waar de risico's niet konden worden weggenomen door maatregelen.



Ter kennisgeving Bureau FG

In het eerste kwartaal van 2021 is een onderzoek naar het gebruik van data van de Belastingdienst afgerond. Het is aanleiding geweest voor een aantal aanbevelingen die betrekking hebben op nakoming van de AVG basisverplichtingen zoals het completeren van het verwerkingsregister en het tijdig starten en afronden van DPIA-trajecten.

Tenslotte: in 2019 werd door de AP een onderzoek gestart naar smart city toepassingen. De gemeente Eindhoven is door de AP in dit onderzoek betrokken. De onderzoekresultaten zijn nog altijd niet bekend, maar worden voor de zomer van 2021 verwacht.