NVRR-Metadossier
Informatiebeveiliging en privacybescherming

Analyse - Do's & Don'ts - Lijst Rekenkamerrapporten

Project uitgevoerd door Ton Hoenderdos

in opdracht van de VNG en de NVRR

25 januari 2023

Inhoud

1 Informatiebeveiliging en Privacybescherming

1.1 Inleiding

Wie 30 jaar terug voor het laatst werkte op een afdeling Burgerzaken bij een gemeente en daar nu weer aan de gang gaat, zal zich welhaast Catweazle wanen, de aandoenlijke tovenaar die onbedoeld een tijdreis maakt van de 11e naar de 20e eeuw en zo terechtkomt in een voor hem bizarre, vreemde wereld. In die 30 jaar is het bevolkingsregister in 1994 vervangen door de GBA (Gemeentelijke basisadministratie persoonsgegevens), dat vervolgens in 2014 is ingeruild voor de BRP (Basisregistratie Personen).

Bij de term informatiebeveiliging zou de medewerker van 30 jaar terug wellicht denken aan het postelastiek om een stapel ponskaarten, die moest voorkomen dat ze door de war raken als hij/zij die per ongeluk liet vallen, waardoor het - toen nog maar net - geautomatiseerde systeem vast zou kunnen lopen.

Vallende ponskaarten kennen we niet meer, de risico's zijn nu van een heel andere orde en worden aangeduid met termen als phishing mail[1], malware[2] , spyware[3], ransomware[4], datalek[5] en hack[6].
En onze medewerker van 30 jaar terug heeft nu ook collega's met functies die in haar/zijn tijd niet bestonden. Zo is er nu een CISO (Chief Information Security Officer), SO (Security Officer), PO (Privacy Officer) en een FG (Functionaris Gegevensbescherming).

Dit alles als gevolg van de voortgaande ontwikkeling van de functie informatievoorziening, gecombineerd met de volledige digitalisering van de basisadministratie van de (lokale) overheden. Dit brengt niet alleen onmiskenbaar grote voordelen, maar ook risico's met zich. Gemeenten als Lochem, Hof van Twente, Smallingerland, Ede en Buren kunnen erover meepraten.

Zo is het beveiligen van informatie een belangrijk thema geworden voor overheidsorganisaties en partijen waarmee zij samenwerken op het gebied van informatievoorziening. Gelukkig hoeft niet elke gemeente apart hiervoor het wiel uit te vinden, want er wordt stevig samengewerkt op dit terrein, uitmondend in de Baseline Informatiebeveiliging Overheid (BIO).

---

[1] **phishing mail**:
een vals e-mail bericht waarin malware kan zijn verstopt, waarmee wordt 'gehengeld' naar inlog- of andere persoonsgegevens.

[2] **malware**:
staat voor "malicious software", kwaadaardige software dus, bedoeld om een digitaal systeem binnen te dringen om gegevens te stelen en/of het systeem te beschadigen.

[3] **spyware**:
kwaadaardige spionage software die een systeem infecteert en gegevens over dat systeem en de gebruiker(s) ervan doorstuurt.

[4] **ransomware**:
vorm van malware die databestanden versleutelt en ontoegankelijk maakt (gijzelt), om vervolgens losgeld - "ransom" - te kunnen eisen om ze weer bruikbaar te maken.

[5] **datalek**:
als er sprake is van toegang tot - of vernietiging, wijziging of vrijkomen van - persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie.

[6] **hack**:
illegale inbraak in een computersysteem.

1.2 Baseline Informatiebeveiliging Overheid (BIO)

De BIO geeft het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. Het is dan ook een gezamenlijke ontwikkeling van Rijk, provincies, gemeenten en waterschappen, die elk zijn vertegenwoordigd in de interbestuurlijke werkgroep die zorgdraagt voor het onderhoud van de BIO.

Eerder hadden de overheidslagen ieder hun eigen baseline. Bij gemeenten was dit de BIG, waarbij de G staat voor gemeenten. Na een voorbereidingstraject zijn deze baselines per 1-1-2019 vervangen door de gezamenlijke BIO.

De BIO ondersteunt overheidsorganisaties in de wijze waarop zij hun informatiebeveiliging organiseren en uitvoeren. Zo worden de aandachtsgebieden voor de beveiliging benoemd en de rollen en verantwoordelijkheden van degenen die hierbij betrokken zijn. Vervolgens worden er beheersmaatregelen omschreven (waarbij voor de BIO is afgesproken om de Engelse term 'controls' te gebruiken) en er worden richtlijnen gegeven voor het implementeren van deze controls.

Heel in het kort ziet de toepassing van de BIO er als volgt uit. Aan de basis staat de baseline-toets met een GAP-analyse voor alle controls. Hierbij wordt getoetst in hoeverre voldaan wordt aan een bepaalde set van eisen. Het verschil tussen de huidige en gewenste situatie is de 'gap'. Bedrijfsprocessen en verantwoordelijken hiervoor worden geïnventariseerd. Waar nodig worden diepgaande risicoanalyses gemaakt en een DPIA onderzoek (Data Protection Impact Assessment; zie hieronder bij AVG). Dit is een gegevensbeschermingseffectbeoordeling dat de privacyrisico's van een gegevensverwerking in kaart brengt. Benodigde controls en maatregelen worden organisatorisch goed belegd en vastgelegd in het ISMS (Information securitymanagement system). Zo wordt de informatiebeveiliging opgezet en ingericht. Met periodieke monitoring tenslotte wordt bewaakt dat de beveiliging op niveau blijft. Hierbij duikt de term PDCA-cyclus op, dat staat voor Plan-Do-Check-Act, waarmee de lerende organisatie monitort of de controls effectief zijn in het beheersen van - ook nieuwe - risico's.

In relatie tot de BIO moet ook de nieuwe verantwoordingssystematiek ENSIA (Eenduidige Normatiek Single Information Audit) worden genoemd. Dit is een initiatief van gemeenten en de ministeries van BZK en SZW en heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hierop ook beter sturen.

Als onderdeel van de VNG draagt de IBD (informatiebeveiligingsdienst) namens gemeenten bij aan de ontwikkeling van de BIO en brengt het kennisproducten hierover uit. Alle Nederlandse gemeenten kunnen hiervan gebruik maken. Bovendien kan de IBD voor hen de functie vervullen van CERT/CSIRT (Computer Emergency Response Team / Computer Security Incident Response Team), die wordt ingeschakeld bij incidenten.

Een belangrijk doel van de BIO is de privacybescherming, zoals die is geregeld in de AVG.

1.3 Algemene Verordening Gegevensbescherming (AVG)

Vanaf 25 mei 2018 geldt de AVG voor het beheer en gebruik van persoonsgegevens (er ging een transitieperiode van twee jaar aan vooraf). Het is een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. De AVG is ook bekend onder de Engelse naam General Data Protection Regulation (GDRP).

In Nederland vervangt de AVG de Wet bescherming persoonsgegevens (Wbp). Ten opzichte van die Wbp zijn de privacyrechten van mensen versterkt en uitgebreid. Voor organisaties gelden er meer verplichtingen bij het verwerken van persoonsgegevens. En er is een verantwoordingsplicht, die inhoudt dat met documenten moet kunnen worden aangetoond dat de juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen. Zo kan er een verplichting zijn om een Data Protection Impact Assessment (DPIA) uit te voeren voor die processen waarbij de gegevensverwerking een hoog privacyrisico kan opleveren.

Ook kunnen organisaties verplicht zijn om een functionaris gegevensbescherming (FG) aan te stellen. Dit geldt in elk geval voor alle overheidsinstanties en publieke organisaties, ongeacht de gegevens die ze verwerken. Verder kan de verplichting gelden voor een organisatie die op grote schaal individuen en hun activiteiten volgen (bijv. cameratoezicht), of bijzondere persoonsgegevens (bijv. over gezondheid of geloofsovertuiging), of strafrechtelijke persoonsgegevens verwerkt.

Met de AVG is ook de Meldplicht Datalekken ingevoerd, die organisaties verplicht om alle datalekken te documenteren en in bepaalde situaties (met name bij het lekken van persoonsgegevens) ook te melden bij het Meldpunt Datalekken van de Autoriteit Persoonsgegevens.
En als er ongunstige gevolgen voor de betrokkene(n) dreigen, moeten ook zij worden geïnformeerd.

1.4 Informatiebeveiliging en Privacybescherming als onderzoeksthema

Dit is bij uitstek een onderwerp voor rekenkameronderzoek. Voor je ’t weet sluipt er in een organisatie het gevoel dat het allemaal wel meevalt, dat het allemaal zo’n vaart niet loopt. Het moge duidelijk zijn dat dit volstrekt misplaatst is, want als het wél mis gaat kunnen de gevolgen enorm zijn. De organisatie wordt dan letterlijk in het hart getroffen.

De rekenkamer kan helpen de organisatie wakker te houden, door eens in de zoveel tijd dit thema te agenderen. Al is ’t maar in een beknopte quick scan waarin wordt bezien of eerdere aanbevelingen secuur zijn opgevolgd.

2 Metadossier hoofd- en subthema's

Het metadossier Informatiebeveiliging en Privacybescherming is gemaakt op basis van een inventarisatie van Rekenkamer-onderzoeken op dit beleidsterrein. Deze zijn gevonden in de database van de NVRR én via gerichte zoekacties op internet naar rekenkameronderzoek op dit thema. Zo zijn er nu 36 publicaties in het metadossier opgenomen. De informatie is geordend op basis van een aantal hoofd- en subthema's.

Tabel 1 Hoofd- en subthema's inventarisatie Informatiebeveiliging en Privacybescherming

Hoofdthema's	Subthema's
Beleidskaders	Beleid informatiebeveiliging en privacybescherming
	is het beleid conform BIO (BIG)
	wordt voldaan aan de AVG
Financiën	budget en personele inzet
Sturing	Sturende rol college / GS
	betrokkenheid samenwerkende gemeenten
Kaderstelling	Kaderstellende rol gemeenteraad / PS
Controle	Controlerende rol gemeenteraad / PS
Toezicht	werkprocessen monitoren, bewaken en verbeteren
	Checks - Audits - Evaluatie - Risicoanalyse
Informatievoorziening	informatie voor college / GS
	informatie voor de raad / PS
Organisatie	organisatie, werkprocessen en uitvoering
	calamiteiten en risicobeheersing
	bewustwording, kennis en kunde in de organisatie
	beveiliging en autorisatie
	kwetsbaarheid ICT en Informatiesystemen
Externe hulp en partners	aansluiting op Informatiebeveiligingsdienst (IBD)
	inschakeling externen, (keten)partners én controle
	communicatie en betrokkenheid burgers
Kwaliteit	Balans tussen kwaliteit van de dienstverlening en privacy bescherming
	extern leren

3 Analyse inhoud Rekenkamerrapporten

3.1 Inleiding

De hoofdthema's die in tabel 1 zijn opgenomen, zijn gebruikt voor het inventariseren van de *centrale vragen* en de *normen* die zijn beschreven in de Rekenkamerrapporten. De subthema's uit tabel 1 zijn gebruikt voor het inventariseren van de *onderzoeksvragen*, de *conclusies* en de *aanbevelingen* die zijn beschreven in de Rekenkamerrapporten.

Om iets meer te kunnen zeggen over de inhoud van de Rekenkamerrapporten die over Informatiebeveiliging en Privacybescherming zijn geschreven, is nagegaan hoe vaak de hoofdthema's in de centrale vragen (§3.2) en de normen (§3.3) terugkomen én hoe vaak de subthema's in de conclusies en aanbevelingen (§3.4) terugkomen.

3.2 Centrale vragen

Tabel 2 geeft een overzicht van de verschillende hoofdthema's die in de centrale vragen van de Rekenkameronderzoeken voorkomen.[7]

Tabel 2 Centrale vragen Rekenkameronderzoek Informatiebeveiliging en Privacybescherming (n=36)

Hoofdthema centrale vraag	Aantal RK(cie)s	%
Beleidskaders	34	94
Financiën	0	0
Sturing	4	11
Kaderstelling	6	17
Controle	6	17
Toezicht	5	14
Informatievoorziening	3	8
Organisatie	16	44
Externe hulp en partners	1	3
Kwaliteit	0	0

In tabel 2 valt op dat de beleidskaders ten aanzien van informatiebeveiliging en privacybescherming altijd bij het onderzoek worden betrokken. En ook de organisatie hiervan is vaak onderwerp van onderzoek.

[7] Een centrale vraag kan betrekking hebben op meerdere hoofdthema's.

3.3 Normen

De normen die de Rekenkamer(cie)s hebben geformuleerd, geven ook een indicatie van de onderwerpen die door de Rekenkamer(cie)s zijn onderzocht op het gebied van Informatiebeveiliging en Privacybescherming.[8] Tabel 3 geeft een overzicht.

Tabel 3 Normen Rekenkameronderzoek Informatiebeveiliging en Privacybescherming (n=36)

Normen	Aantal RK(cie)s	%
Beleid informatiebeveiliging en privacybescherming	18	50
is het beleid conform BIO (BIG)	18	50
wordt voldaan aan de AVG	16	44
budget en personele inzet	5	14
Sturende rol college / GS	11	31
betrokkenheid samenwerkende gemeenten	3	8
Kaderstellende rol gemeenteraad / PS	7	19
Controlerende rol gemeenteraad / PS	2	6
werkprocessen monitoren, bewaken en verbeteren	20	56
Checks - Audits - Evaluatie - Risicoanalyse	17	47
informatie voor college / GS	4	11
informatie voor de raad / PS	8	22
organisatie, werkprocessen en uitvoering	21	58
calamiteiten en risicobeheersing	13	36
bewustwording, kennis en kunde in de organisatie	17	47
beveiliging en autorisatie	14	39
kwetsbaarheid ICT en Informatiesystemen	9	25
aansluiting op Informatiebeveiligingsdienst (IBD)	1	3
inschakeling externen, (keten)partners én controle	13	36
communicatie en betrokkenheid burgers	5	14
Balans tussen kwaliteit van de dienstverlening en privacy bescherming	5	14
extern leren	0	0

Uit tabel 3 blijkt dat normen vaak betrekking hebben op het beleid ten aanzien van informatie-beveiliging en privacybescherming, of dat op orde is. En hoe dit vervolgens in de organisatie zijn doorwerking vindt. Niet alleen op papier, maar ook in de praktijk en in de hoofden van de mensen. Vaak hebben normen ook betrekking op monitoring en risicoanalyse.

[8] Een norm kan betrekking hebben op meerdere hoofdthema's.

3.4 Conclusies en aanbevelingen

De conclusies en aanbevelingen zijn geïnventariseerd op basis van 22 subthema's die onder 10 hoofdthema's vallen (zie ook tabel 1).

Hoofdthema's met één subthema

Drie hoofdthema's bestaan uit één subthema. Dit zijn de hoofdthema's: financiën, kaderstelling en controle. Omdat deze hoofdthema's slechts één subthema hebben, zijn de aantallen (die in de tabellen staan) onderling vergelijkbaar. De aantallen geven namelijk het aantal Rekenkamer(cie)s weer dat het betreffende subthema in hun conclusies dan wel aanbevelingen heeft opgenomen .

Hoofdthema's met meerdere subthema's

De overige zeven hoofdthema's bestaan uit meerdere subthema's. Dit zijn de hoofdthema's: Beleidskaders, Sturing, Toezicht, Informatievoorziening, Organisatie, Externe hulp en partners en Kwaliteit. Omdat het aantal subthema's per hoofdthema verschilt, zijn de aantallen (zoals opgenomen in de tabellen) niet onderling vergelijkbaar. De tabellen geven wel een indicatie welke hoofdthema's veel voorkomen in de conclusies en aanbevelingen.

3.4.1 Conclusies

Conclusies hoofdthema's met één subthema

In tabel 4 staat per hoofdthema (met één subthema) het aantal Rekenkamer(ie)s dat conclusies heeft getrokken waarin het betreffende thema aan bod komt.

Tabel 4 Conclusies: hoofdthema's met één subthema (n=36)

Hoofdthema	Subthema	Aantal RK(cie)s	%
Financiën	budget en personele inzet	8	22
Kaderstelling	Kaderstellende rol gemeenteraad / PS	15	42
Controle	Controlerende rol gemeenteraad / PS	16	44

Conclusies hoofdthema's met meerdere subthema's

In tabel 5 staat per hoofdthema (met meerdere subthema's) het aantal conclusies dat betrekking heeft op het betreffende hoofdthema. In de 3e kolom staat aangegeven hoeveel subthema's elk hoofdthema heeft.

Tabel 5 Conclusies: hoofdthema's met >1 subthema's (n=36)

Hoofdthema	Aantal	Aantal subthema's
Beleidskaders	71	3
Sturing	27	2
Toezicht	35	2
Informatievoorziening	23	2
Organisatie	127	5
Externe hulp en partners	24	3
Kwaliteit	2	2

In tabel 5 is te zien dat de meeste conclusies (127) zijn geformuleerd op het hoofdthema Organisatie.

Tabel 5a tot en met 5g geeft de aantallen per subthema, onbecommentarieerd, want de tabellen spreken voor zich.

Conclusies Beleidskaders

Tabel 5a Conclusies: subthema's Beleidskaders (n=36)

Subthema Beleidskaders	Aantal RK(cie)s	%
Beleid informatiebeveiliging en privacybescherming	32	89
is het beleid conform BIO (BIG)	21	58
wordt voldaan aan de AVG	18	50

Conclusies Sturing

Tabel 5b Conclusies: subthema's Sturing (n=36)

Subthema Sturing	Aantal RK(cie)s	%
Sturende rol college / GS	16	44
betrokkenheid samenwerkende gemeenten	11	31

Conclusies Toezicht

Tabel 5c Conclusies: subthema's Toezicht (n=36)

Subthema Toezicht	Aantal RK(cie)s	%
werkprocessen monitoren, bewaken en verbeteren	19	53
Checks - Audits - Evaluatie - Risicoanalyse	16	44

Conclusies Informatievoorziening

Tabel 5d Conclusies: subthema's Informatievoorziening (n=36)

Subthema Informatievoorziening	Aantal RK(cie)s	%
informatie voor college / GS	4	11
informatie voor de raad / PS	19	53

Conclusies Organisatie

Tabel 5e Conclusies: subthema's Organisatie (n=36)

Subthema Organisatie	Aantal RK(cie)s	%
organisatie, werkprocessen en uitvoering	33	92
calamiteiten en risicobeheersing	24	67
bewustwording, kennis en kunde in de organisatie	31	86
beveiliging en autorisatie	14	39
kwetsbaarheid ICT en Informatiesystemen	25	69

Conclusies Externe hulp en partners

Tabel 5f Conclusies: subthema's Externe hulp en partners (n=36)

Subthema Externe hulp en partners	Aantal RK(cie)s	%
aansluiting op Informatiebeveiligingsdienst (IBD)	3	8
inschakeling externen, (keten)partners én controle	16	44
communicatie en betrokkenheid burgers	5	14

Conclusies Kwaliteit

Tabel 5g Conclusies: subthema's Kwaliteit (n=36)

Subthema Kwaliteit	Aantal RK(cie)s	%
Balans tussen kwaliteit van de dienstverlening en privacy bescherming	1	3
extern leren	1	3

3.4.2 Aanbevelingen

Aanbevelingen hoofdthema's met één subthema

In tabel 6 staat per hoofdthema (met één subthema) het aantal Rekenkamer(ie)s dat aanbevelingen heeft geformuleerd waarin het betreffende thema aan bod komt. In de 4e kolom staan de percentages.

Tabel 6 Aanbevelingen: hoofdthema's met één subthema (n=36)

Hoofdthema	Subthema	Aantal RK(cie)s	%
Financiën	budget en personele inzet	20	56
Kaderstelling	Kaderstellende rol gemeenteraad / PS	20	56
Controle	Controlerende rol gemeenteraad / PS	13	36

Veel aanbevelingen zijn gericht aan de gemeenteraad, met name wat betreft hun kaderstellende rol. En even vaak worden er aanbevelingen gedaan ten aanzien van budget en personele inzet.

Aanbevelingen hoofdthema's met meerdere subthema's

In tabel 7 staat per hoofdthema (met meerdere subthema's) het aantal aanbevelingen dat betrekking heeft op het betreffende hoofdthema. In de 3e kolom staat weer aangegeven hoeveel subthema's elk hoofdthema heeft.

Tabel 7 Aanbevelingen: hoofdthema's met >1 subthema's (n=36)

Hoofdthema	Aantal	Aantal subthema's
Beleidskaders	31	3
Sturing	22	2
Toezicht	36	2
Informatievoorziening	41	2
Organisatie	103	5
Externe hulp en partners	21	3
Kwaliteit	0	2

De aanbevelingen zijn vooral gericht op de organisatie rond informatiebeveiliging en privacybescherming.

Aanbevelingen Beleidskaders

Tabel 7a Aanbevelingen: subthema's Beleidskaders (n=36)

Subthema Beleidskaders	Aantal RK(cie)s	%
Beleid informatiebeveiliging en privacybescherming	19	53
is het beleid conform BIO (BIG)	8	22
wordt voldaan aan de AVG	4	11

Aanbevelingen richten zich weinig rechtstreeks tot BIO en AVG. Indirect gebeurt dit natuurlijk wel, omdat de onderwerpen waarop vaker aanbevelingen worden geformuleerd, ook onderdeel uitmaken van het beleid met betrekking tot BIO en AVG.

Aanbevelingen Sturing

Tabel 7b Aanbevelingen: subthema's Sturing (n=36)

Subthema Sturing	Aantal RK(cie)s	%
Sturende rol college / GS	17	47
betrokkenheid samenwerkende gemeenten	5	14

Aanbevelingen Toezicht

Tabel 7c Aanbevelingen: subthema's Toezicht (n=36)

Subthema Toezicht	Aantal RK(cie)s	%
werkprocessen monitoren, bewaken en verbeteren	12	33
Checks - Audits - Evaluatie - Risicoanalyse	24	67

Aanbevelingen Informatievoorziening

Tabel 7d Aanbevelingen: subthema's Informatievoorziening (n=36)

Subthema Informatievoorziening	Aantal RK(cie)s	%
informatie voor college / GS	12	33
informatie voor de raad / PS	29	81

Hier valt op hoe vaak aanbevelingen er op gericht zijn om de raad te voorzien van adequate informatie om haar kaderstellende en controlerende taken te kunnen uitoefenen.

Aanbevelingen Organisatie

Tabel 7e Aanbevelingen: subthema's Organisatie (n=36)

Subthema Organisatie	Aantal RK(cie)s	%
organisatie, werkprocessen en uitvoering	31	86
risicobeheersing in de praktijk	20	56
bewustwording, kennis en kunde in de organisatie	26	72
beveiliging en autorisatie	14	39
kwetsbaarheid ICT en Informatiesystemen	12	33

Bijna altijd zijn er aanbevelingen gedaan gericht op de organisatie én of er binnen de organisatie voldoende bewustwording, kennis en kunde is op het thema Informatiebeveiliging en Privacybescherming.

Aanbevelingen Externe hulp en partners

Tabel 7f Aanbevelingen: subthema's Externe hulp en partners (n=36)

Subthema Externe hulp en partners	Aantal RK(cie)s	%
aansluiting op Informatiebeveiligingsdienst (IBD)	3	8
inschakeling externen, (keten)partners én controle	15	42
communicatie en betrokkenheid burgers	3	8

Aanbevelingen Kwaliteit

Tabel 7g Aanbevelingen: subthema's Kwaliteit (n=36)

Subthema Kwaliteit	Aantal RK(cie)s	%
Balans tussen kwaliteit van de dienstverlening en privacy bescherming	0	0
extern leren	0	0

Hoewel de onderwerpen van tabel 7g wel aan de orde zijn in de onderzoeken, worden er nergens concrete aanbevelingen gedaan hoe hiermee kan of zou moeten worden omgegaan.

4 Tips & Tricks en Do's & Don'ts

Op basis van de inventarisatie van de rekenkamerrapporten op het gebied van Informatiebeveiliging en Privacybescherming en van eerdere metadossier-inventarisaties op andere thema's, geven we een aantal algemene en specifieke tips/opmerkingen voor de Rekenkamer(cie)s die onderzoek willen gaan uitvoeren naar het onderwerp Informatiebeveiliging en Privacybescherming.

Algemene tips/opmerkingen Rekenkameronderzoek:

- Zorg voor een goede leesbaarheid van het rapport. Dit kan door:
    - een duidelijke structuur van de rapportage;
    - naast het reguliere rapport een publieksversie uit te brengen;
    - het rapport in een format op te maken dat digitaal goed leesbaar is door bijvoorbeeld met tabbladen te werken of de rapportage in de vorm van een of meerdere factsheets op te maken;
- Het bevordert de leesbaarheid als conclusies en aanbevelingen worden geformuleerd in één zin met daaronder een korte toelichting.
- Neem altijd normen of een normenkader op in het rapport. Dit maakt het onderzoeksproces transparant voor de ambtelijke organisatie, het college en de raad; zij weten op basis van welke uitgangspunten de conclusies van het onderzoek getrokken zijn. Houd rekening bij het opstellen van de normen met de volgende aspecten:
    - relatie tussen de normen en de centrale -/ onderzoeksvragen en/of de conclusies;
    - voor zover mogelijk de normen operationaliseren;
    - de aanduiding "het bereiken van doelen" vraagt om een nadere precisering. Het bereiken van doelen kan namelijk betrekking hebben op doeltreffendheid, effectiviteit, resultaten, outcome, prestaties of maatschappelijke effect;
- In verschillende rapporten wordt gesproken over "de gemeente". Het is duidelijker om te spreken over het college en/of de gemeenteraad omdat beide andere functies, rollen en verantwoordelijkheden hebben.

Specifieke tips/opmerkingen voor onderzoek naar Informatiebeveiliging en Privacybescherming:

- dit onderzoeksonderwerp vraagt om een secure en punctuele onderzoekswerkwijze door de rekenkamer. Graag op het pietluttige af moet gestructureerd worden doorgenomen of echt alle aspecten op het thema informatiebeveiliging en privacybescherming goed op orde zijn. De reden hiervoor is dat één zwakke schakel, één vergeten detail kan maken dat het gemeentelijk informatiesysteem wordt binnengedrongen, ook al is de beveiliging op alle andere onderdelen wél op orde;
- het draait om de driehoek mens-organisatie-techniek. Om een afgewogen oordeel te kunnen geven over de kwaliteit van de informatiebeveiliging en privacybescherming, moeten deze alle drie in het onderzoek worden betrokken;
- het beleid en de organisatie met betrekking tot informatiebeveiliging en privacybescherming moet op papier goed op orde zijn. Maar natuurlijk moet dit ook in de praktijk goed worden uitgevoerd. Beide moeten dus een plaats krijgen in het onderzoek. Hierbij moeten ook de eventueel ingeschakelde (keten)partners worden betrokken;

- als het budget en de personele inzet dat voor informatiebeveiliging en privacybescherming ter beschikking is, wordt betrokken bij het onderzoek, biedt het een nuttig inzicht als ook een schatting wordt gevraagd of gemaakt van de (financiële) risico's die men loopt in geval van calamiteiten;
- tenslotte - the proof of the pudding is in the eating - praktijktesten kunnen heel nuttig zijn om te testen hoe het werkelijk is gesteld met informatiebeveiliging en privacybescherming. Bij de onderzoeken die in het metadossier zijn opgenomen, zijn pentesten[9] uitgevoerd en mystery guests[10] op pad gestuurd, die soms toch opmerkelijk ver het systeem en/of gebouw bleken te kunnen binnendringen.

[9] pentest staat voor penetratietest: toets van computersystemen op kwetsbaarheden in de beveiliging, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken.

[10] mystery guest: een - liefst goed toneelspelende - persoon die op bezoek gaat bij een organisatie, waar zij/hij in ruimtes en bij informatie probeert te komen, wat duidelijk niet de bedoeling is. Het kan nog een stap verder gaan, als zij/hij dan ook nog probeert in te breken op het lokale computernetwerk.

5 Rekenkamerrapporten in het NVRR-Metadossier Informatiebeveiliging en Privacybescherming

Gemeenten:

- Achtkarspelen en Tytsjerksteradiel, *It is mei sizzen net te dwaan; Rekenkameronderzoek naar Informatiebeveiliging en privacy Achtkarspelen en Tytsjerksteradiel*, 2019.
- Amersfoort, *Bescherming persoonsgegevens; Rekenkameronderzoek*, 2021.
- Berg en Dal, *Weten wat je moet weten; Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming - rapport gemeente Berg en Dal*, 2022.
- Beuningen, *Weten wat je moet weten; Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming - rapport gemeente Beuningen*, 2022.
- Blaricum, Eemnes en Laren (BEL gemeenten), *Privacy in het sociaal domein*, 2017.
- Breda, *Informatiebeveiliging bij de gemeente Breda*, 2016.
- Cranendonck, Heeze-Leende, Valkenswaard (Samenwerking A2-gemeenten), *Onderzoek Informatieveiligheid A2-gemeente*, 2020.
- Delft, *Informatiebeveiliging binnen de gemeente Delft*, 2018.
- Delfzijl, Appingedam en Loppersum (DAL); nu: Eemsdelta (per 1/1//2021), *Quick Scan-Informatiebeveiliging DAL-gemeenten*, 2018.
- Dronten, *Privacy en informatieveiligheid in het sociaal domein; werkbaarheid van wet- en regelgeving*, 2019.
- Eindhoven, *Informatieveiligheid smart & safe?*, 2021.
- Gooise Meren, *Privacy in het sociaal domein; Rapportage Rekenkamercommissie Gooise Meren*, 2017
- Haarlem, *Verantwoordelijkheid voor Veiligheid; Onderzoek naar Informatiebeveiliging*, 2019.
- Hillegom en Lisse, *Quick scan Informatiebeveiliging - Gemeente Lisse*, 2022.
- Hoeksche Waard, *Informatiebeveiliging en privacy gemeente Hoeksche Waard*, 2021.
- Hof van Twente, *De perfecte storm Informatiebeveiliging Gemeente Hof van Twente*, 2022.
- Laarbeek, *Onderzoek Rekenkamercommissie Informatiebeveiliging Gemeente Laarbeek*, 2019.
- Maasdriel, *Beveiliging van informatie; Memorandum*, 2018.
- Nijmegen, *Weten wat je moet weten; Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming - rapport gemeente Nijmegen*, 2022.
- Opmeer (RKC Koggenland), *Informatiebeveiliging Gemeente Opmeer*, 2022.
- Overbetuwe, *Volwassenheidsonderzoek Informatiebeveiliging gemeente Overbetuwe*, 2021.
- Pijnacker-Nootdorp, *Privacybeleid; Onderzoek naar privacybeleid in Pijnacker-Nootdorp*, 2018.
- Ridderkerk, *Informatie in goede handen?; Rapport over de informatiebeveiliging in Ridderkerk*, 2020.
- Rotterdam, *In onveilige handen; onderzoek informatiebeveiliging van gevoelige informatie*, 2017.
- 's Hertogenbosch, *Privacy, verantwoord datagebruik, en de rol van de raad; Een verkenning van beleid en uitvoering*, 2021.
- Son en Breugel, Rapport *rekenkamercommissie Informatiebeveiliging en privacy*, 2020.
- Utrecht, *Zo sterk als de zwakste schakel; een onderzoek naar de informatieveiligheid bij de gemeente Utrecht*, 2021.
- Wassenaar, Voorschoten, Oegstgeest, Leidschendam-Voorburg, *Rekenkameronderzoek informatiebeveiliging van gemeenten en verbonden partijen*, 2021.
- Wijchen, *Weten wat je moet weten; Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming - rapport gemeente Wijchen*, 2022.
- Zoetermeer, *Quick Scan - Informatiebeveiliging gemeente Zoetermeer*, 2017.

Provincies:

- Gelderland (RK Oost-Nederland), *In veilige handen?; informatieveiligheid Gelderland*, 2019.
- Limburg (Zuidelijke Rekenkamer), *Informatieveiligheid provincie Limburg*, 2018.
- Limburg (Zuidelijke Rekenkamer), *Vervolgonderzoek Informatieveiligheid Provincie Limburg*, 2022.
- Noord-Brabant (Zuidelijke Rekenkamer), *Informatieveiligheid provincie Noord-Brabant*, 2018.
- Noord-Brabant (Zuidelijke Rekenkamer), *Vervolgonderzoek Informatieveiligheid Provincie Noord-Brabant*, 2022.
- Overijssel (RK Oost-Nederland), *In veilige handen?; informatieveiligheid Overijssel*, 2019.