Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Op weg naar digitaal veilige DOWR-gemeenten

Informatiebeveiligingsplan 2021



Uitgave : Versie 1.5
Opsteller : H.A. Bremer, Chief Information Security Officer (CISO-DOWR)
Mail : hessel.bremer@dowr.nl

Februari 2021

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Inhoud

Management samenvatting 4
1. Roadmap informatieveiligheid DOWR 2021-2024 7
2. Activiteiten 2021 8
3. Nieuwe ontwikkelingen 2020 en 2021 12
4. Planning 14
5. Begroting 2021 15
Bijlage Afkortingenoverzicht 16

Versiebeheer

Versie	***Datum***	***Review door/ verstrekt aan***
1e concept	04-2-2021	Hessel Bremer, CISO (eigenaar)
0.9	05-2-2021	Wessel Hemels, ISO
1.0	10-2-2021	René Passchier, Manager DOWR-I Lotte Schieving, FG Lucas Klekamp, PO
1.0	15-2-2021	Q-PIT gemeente Olst-Wijhe: Gerard Luijmes Renate Auée – Nijhof Anke Mensen - Wolbert
	16-2-2021	Johannes Grimmerink Wessel Hemels Eric Grotenhuis
1.1	17-2-2021	René Passchier Wessel Hemels
	18-2-2021	Q-PIT gemeente Raalte: Mark Duijtshoff Jeanet van Olst Mieke Lammerts van Bueren
1.2	18-2-2021	Hessel Bremer, CISO René Passchier Johannes Grimmerink Eric Grotenhuis Wessel Hemels
1.3	19-2-2021	Hessel Bremer, CISO
	24-2-2021	Q-PIT gemeente Deventer: Marcel Kossen Denny Lobeek Marije Spakman
1.4	26-2-2021	Hessel Bremer, CISO
	01-4-2021	CIO en Directieoverleg DOWR
1.5	16-4-2021	Hessel Bremer, CISO Wessel Hemels, ISO
	26-4-2021	PFO Ron König

Management samenvatting

Informatiebeveiliging is een dynamisch risico gedreven organisatieproces.
De DOWR-gemeenten hebben een gezamenlijke strategische visie opgesteld, waar informatiebeveiliging als rode draad, randvoorwaarde en succesfactor integraal onderdeel van uitmaakt. Het voorkomen van beveiligingsrisico's is immers beter dan het achteraf 'genezen' of herstellen daarvan.
Voor de DOWR-I is in 2019 het strategische Informatiebeveilingsbeleid 2020-2022 vastgesteld.
Voor u ligt het Informatiebeveiligingsplan DOWR 2021, kortweg IBP. Dit plan geeft aan op welke wijze wij invulling geven aan de uitvoering van het vastgestelde bestaande beleid.

Het Informatiebeveiligingsplan DOWR 2021 geeft inzicht in de uitwerking van de geplande activiteiten voor dit jaar, inclusief prioritering en begroting. Het Informatiebeveiligingsplan DOWR 2021 is een jaarlijkse uitwerking van het strategische thema IV en maakt onderdeel uit van de Roadmap IV 2021-2023 en met dit plan tevens geformaliseerd, zie pagina 7.
De visie dat Informatieveiligheid een jaarlijks 'IT-audit-proces' betreft en of 'enkel een ICT-dingetje' is, is al lang verleden tijd. Daarentegen is het aan elke (overheids-)instantie om de betrouwbaarheid van informatie te waarborgen (garanderen).



Figuur 1 2020 in beeld

Het jaar 2020 gaat als een bijzonder jaar de geschiedenisboeken in door de pandemie COVID-19. Ten gevolge daarvan zijn we als organisaties massaal gaan thuiswerken, waardoor onze ICT-omgeving en verbonden apparaten sindsdien zwaarder worden belast. In deze zelfde periode is de (cyber-)dreiging toegenomen.

Gemeenten krijgen te maken met serieuze risico's en incidenten, met verregaande gevolgen. Denk daarbij aan de hack bij Hof van Twente (2020), de Universiteit van Maastricht (2019) en zeer recentelijk (medio februari 2021) de hack van de Universiteit (UvA) en Hogeschool van Amsterdam recentelijk nog aan kan worden toegevoegd. Beide organisaties werden getroffen door gijzelsoftware waarbij de bedrijfsinformatie ontoegankelijk werd gemaakt (versleuteld) en de bedrijfsprocessen letterlijk tot stilstand kwamen. Gezien de ernst van deze incidenten is onze bedrijfscontinuïteit daarmee in gevaar en dus ook onze dienstverlening naar inwoners, ondernemers en partners waarmee wij samenwerken.

Juist informatieveiligheid kan helpen, en is zelfs een randvoorwaarde om het voorkomen van risico's met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van informatie ook wel tezamen 'betrouwbaarheid van informatie' genoemd, te waarborgen.

We weten dat 100% beveiligen niet bestaat, maar kunnen wel minstens onze risico's in control brengen. Het is dus noodzaak om naast het voorkomen van risico's (Security by Design) ook het crisismanagementproces (BCP en noodprocedures) op orde te krijgen. En daarnaast vanuit concern en Directie het risicomanagementproces tenminste in control.



Figuur 2 Digitale weerbaarheid, bedreigingen en handelingsperspectief

Digitale weerbaarheid

Als organisatie gaan wij daarom op weg naar een digitaal weerbare organisatie/ samenleving. Onderstaande Infographic geeft inzicht in het begrip een ‘digitale weerbare gemeente’.



Figuur 3 Infographic Digitale Veiligheid

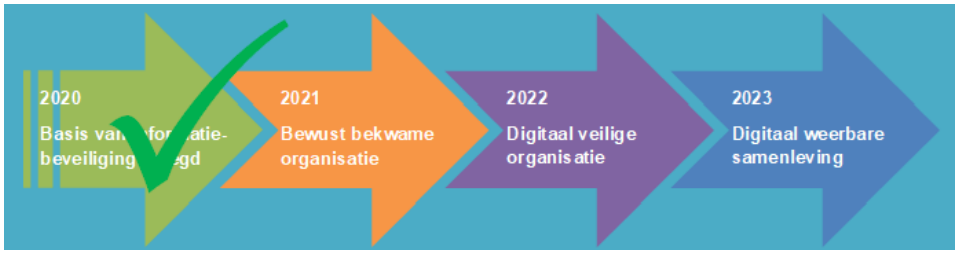
Het bereiken van een digitaal veilige (weerbare) organisatie ontstaat niet in één jaar. Het is een continu proces van risicomanagement waarbij de organisatie bij iedere stap en elk incident (!) continu verbeterd[1].

Echter digitale veiligheid is niet alleen informatiebeveiliging, maar van, en betrekking hebbende op de gehele organisatie. Dit begint bij het inrichten van integraal risicomanagement, waarbij ook de afdelingen Concern control, DOWR-I, lijnmanagement, HR, directie, informatiebeveiliging en privacy nauw betrokken zijn.

Verder professionalisering zal ontstaan als er ook een juiste balans gevonden wordt voor wat betreft de regie op de onderwerpen integrale veiligheid (OOV-Cybercrime), crisismanagement en bedrijfscontinuïteit, zowel organisatorisch als technisch vanuit DOWR-I (ICT). En in het verlengde hiervan de inrichting van organisatie breed Portfoliomanagement (regie en standaardisatie), waarin de security- en architectuurprincipes (risk-based) geïntegreerd worden.
Dit alles om de digitale weerbaarheid vanuit de organisaties afdoende te waarborgen.

[1] Deming circle Plan, Do, Check, Act cyclus

1. Roadmap informatieveiligheid DOWR 2021-2024



Figuur 4 Roadmap informatieveiligheid 2021-2023

In de roadmap[2] Digitale weerbaarheid 2021-2023 is het kader geschetst om te komen tot een digitaal weerbare gemeente. De feitelijke uitwerking van de doelstellingen wordt jaarlijks beschreven in een Informatiebeveiligingsplan. Dit alles wordt gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), geregisseerd vanuit een geïntegreerde en samenhangende aanpak met Privacy (AVG Algemene Verordening Gegevensbescherming).

In de bijbehorende planningen voor het betreffende jaar zijn de onderwerpen zoveel als mogelijk op elkaar afgestemd.



Figuur 5 Strategische thema's IV DOWR gemeenten 20-23

Het is van belang dat ook de Roadmap IV DOWR 2021-2023 met dit plan wordt vastgesteld als visuele stip op de horizon gedurende deze periode.

[2] Roadmap 'Digitale weerbaarheid', zoals eerder besproken in het Directie overleg DOWR

2. Activiteiten 2021

Bewust bekwame organisatie (strategisch thema IV)

Dit jaar staat in het teken van een bewust bekwame organisatie waarbij het van belang is dat medewerkers, managers en directie zich bewust zijn van de risico's, dreigingen en melden van incidenten om zichzelf maar ook de organisatie naar een meer volwassen organisatie te brengen.

Bewustwording

Een bewust bekwame organisatie neerzetten is een enorme uitdaging. Iedere functie heeft daarbij een eigen verantwoordelijkheid, ongeacht het niveau van de functie (strategisch, tactisch, operationeel). Het creëren van bewustzijn binnen de organisatie en het eventueel trainen van medewerkers en management op het gebied van informatiebeveiliging en privacy is daarbij essentieel. Dit gebeurt doormiddel van een bewustwordingsprogramma voorzien van tools (o.a. e-learning, introductietraining-game), als ook het simuleren van crisissituaties.
Ten aanzien van bewustwording en uiteindelijk digitale vaardigheden om uiteindelijk te komen tot een digitaal weerbare organisatie worden komende jaren de volgende fasen doorlopen:



Figuur 6 Ontwikkelingsfasen bewustwording

In samenwerking met de afdeling HR/opleidingen en privacy wordt hiervoor een MD-traject[3] uitgewerkt om bovengenoemde ambitie te behalen. ***(Actiepunt 1)***

De onderwerpen welke worden besproken zijn onder andere dataclassificatie **(*Actiepunt 2*)** (vertrouwelijkheid), proceseigenaarschap en crisismanagement. Deze zullen op verschillende momenten door het jaar heen plaatsvinden.

[3] MD – Management development

Informatiebeveiligingstoets (BBN-toets)

Naast het voldoen aan de BIO-norm, wordt specifiek het risicomanagementproces georganiseerd in de DOWR-organisatie. Door middel van een Informatiebeveiligingstoets (systematiek) worden de informatiebeveiligingsrisico's door de systeemeigenaren in beeld gebracht en een vooraf gedefinieerde set aan beveiligingsmaatregelen (BBN-niveau) voorgesteld om de risico's te mitigeren.

Verwachting is dat de DPIA (AVG) en de Informatiebeveiligingstoets geïntegreerd gaan worden tot één proces, gebaseerd op de plan-do-check-act-cyclus. Vanuit de VNG wordt momenteel gewerkt aan deze integrale risico tool voor privacy en informatiebeveiliging (***Actiepunt 6***) Dit proces wordt mede ondersteund door de nieuwe ISMS-tool die wordt ingezet om het proces te borgen binnen DOWR.

Bedrijfscontinuïteit

Aanvullend op het project 'Noodprocedures' (2019), dient de crisisorganisatie ingericht te worden. Want wie heeft de leiding in welke situatie of zelfstandig organisatie als we gehackt worden? En gaan we wel of niet de Bitcoins betalen als onze bedrijfsinformatie is versleuteld? Hier wil ik graag van tevoren over nadenken, aldus Martijn Dadema, burgemeester Raalte, tijdens zijn gesprek met de CISO (PFO, januari 2021). Aanleiding is het toegenomen risico op (cyber-)incidenten, waardoor de bedrijfsvoering tot stilstand kan komen met alle gevolgen van dien.

Borging en samenhang van het crisismanagementproces en bedrijfscontinuïteit, zorgen voor transparantie in risicomanagementproces voor de deelnemende gemeenten (overstijgend). Naast de crisisstructuur dient ook de verantwoordelijkheden (en afhankelijkheden voor wat betreft ICT-infrastructuur) inzichtelijk te worden gemaakt, om in geval van een noodsituatie adequaat te kunnen handelen. Hoewel informatiebeveiliging geen eigenaar is van dit proces, is het risicomanagementcyclus (BBN-toets, risico's en maatregelen) een randvoorwaarde voor de organisatie om verder in controle te komen op dit proces.

Bij het implementeren van thema's rondom informatiebeveiliging en privacy en het functioneren van de processen rondom risicomanagement, incidentmanagement en bedrijfscontinuïteit moet duidelijk zijn wie waarvoor verantwoordelijk is. Zo is het lijnmanagement verantwoordelijk voor de werkprocessen die zij onder zich hebben en de bijbehorende informatiesystemen. Vanuit deze verantwoordelijkheden worden bijvoorbeeld de noodprocedures (BCP) voor de meest kritische processen en systemen (kroonjuwelen) van de gemeente ingericht. Zo wordt de bedrijfscontinuïteit gewaarborgd bij verstoring of uitval van ICT ten gevolge van een technisch- en of cyberincident. (***Actiepunten 3/4***)

Vanuit de betrokken afdelingen dient door middel van een RACI inzichtelijk te komen, wie waarvoor verantwoordelijk is in de DOWR-organisatie. Waarbij we onderscheid

kunnen maken in de reguliere bedrijfsvoering en de crisis(-management) situatie die specifiek de DOWR-I-organisatie raakt.
Een BCP-plan geeft hierbij de overkoepelende verbinding aan tussen de gemeenten, waarvan de logische eigenaar nog nader moet worden bepaald.

Voldoen aan de BIO (GAP-analyse)

Jaarlijks voeren wij een GAP-analyse uit waar we onze organisatie toetsen op het voldoen aan de BIO. Deze meting kijkt naar de verschillende onderdelen uit de BIO. Denk hierbij aan bijvoorbeeld communicatiebeveiliging, veilig personeel en leveranciersrelaties.

Uit de huidige GAP-analyse komen de volgende onderwerpen naar voren:

Naleving gaat om het voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen. Het gaat hier om de organisatorische aspecten en (wettelijke) kaders. Hier gaat het bijvoorbeeld om bewaartermijnen van informatie, de invoering van een ISMS-systeem, maar ook de controle van de inrichting van de bestaande systemen/informatie (***Actiepunt 8***). Door middel van BBN-toetsen kunnen wij inzichtelijk maken wat voor informatie in een proces aanwezig is en wat voor beveiligingseisen hierbij horen, deze zullen een vast onderdeel worden van het ISMS-systeem (***Actiepunt 5***).

Communicatiebeveiliging gaat om zowel de technische controle op binnenkomende en uitgaande informatie (monitoring) maar ook over de rechten van onze collega's, partners en burgers binnen die in aanraking komen met onze systemen en organisatie. Met name het laatste deel is waar wij nog enkele stappen zullen gaan zetten. Er dienen namelijk voor elke groep of rol gedefinieerde rechten te zijn; wie mag waarbij en waarom? Wie voert hier de toetsing op uit? Dit zal veelal bij de proceseigenaar komen te liggen, echter moeten zij hier wel van op de hoogte zijn en ondersteund worden waar mogelijk. (***Actiepunt 11)***

Acquisitie, ontwikkeling en onderhoud van informatiesystemen gaat over onder andere de eisen die verband houden met informatiebeveiliging voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. Deze eisen dienen een vast onderdeel te zijn van aanbestedingen, maar ook bij de aanschaf van software en/of diensten. Hier zal bij elke aanschaf voorafgaand een informatiebeveiligingstoets moeten plaatsvinden. Dit om ook af te wegen of hier met vertrouwelijke informatie of privacygegevens wordt gewerkt. Dit zal samen met contractbeheer en privacy opgepakt en verbeterd worden met een set van beveiliging- en contract eisen tot gevolg. ***(Actiepunt 12/13)***

Dataclassificatie wordt ook wel rubricering genoemd. Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan. Classificatie van deze data maakt het mogelijk voor te schrijven welke maatregelen moeten worden genomen om die bepaalde data adequaat

te beschermen. Hierbij worden voorafgaand en organisatie breed DOWR-afspraken gemaakt over de gewenste duiding van vertrouwelijkheid van informatie, immers niet alle informatie is voor eenieder, ook buiten onze gemeenten van belang. De gewenste classificatie zal in nauw overleg met de collega's van privacy en uiteraard de lijnorganisatie onderzocht en geïmplementeerd worden. ***(Actiepunt 14)***

SIEM-SOC vanuit GGI-Veilig (Securitymonitoring)[4]

Onlangs is DOWR als pilotgemeente aangesloten op het SIEM-SOC van de aanbesteding vanuit VNG Realisatie met betrekking tot Securitymonitoring.

Naast de technische realisatie door DOWR-I in samenwerking met KPN is de volgende stap om het bijbehorende proces in de DOWR-organisatie te implementeren. Van groot belang hierbij is de aansluiting op het crisisteam en incidentmanagement van de DOWR-gemeenten, als ook crisisorganisatie inclusief ‘piketdienst’.

Het zal duidelijk zijn dat informatiebeveiliging maar ook specifiek bedrijfscontinuïteit en crisismanagement niet iets wat bij een 8 tot 5 cultuur past, maar iets dat 24/7 gebeurt. Vandaar het belang van het tijdig op orde krijgen van dit proces. (***Actiepunt 9***)

Incidentmanagement

Naast bedrijfscontinuïteit en crisismanagement bestaat er ook een directe relatie met incidentmanagement, want ‘je bent een held als je meldt’, en continu verbeteren (PDCA). Hierbij kan zelfs aansluiting gevonden worden bij de kwaliteitscyclus van DOWR-I (NTA 9001).

Fouten overkomt en maakt iedereen. Sterker nog menselijk handelen blijft de ‘zwakste schakel’ binnen elke organisatie. Daarom is een goed functionerend incidentmanagementproces en tijdige bij-sturing van verbeteringen naar aanleiding van incidenten (lessons learned en PDCA) juist van groot belang. De nieuwe ISMS-tooling zal worden ingezet om dit te realiseren en transparant te maken voor de interne organisatie.

Als verantwoordelijken voor het waarborgen van privacy en/of informatieveiligheid is het lastig om te weten wat er in de hele organisatie speelt en om de hele organisatie te bereiken. Daarom zijn wij, in lijn met ‘je bent een held als je het meldt’, voornemens om op elke afdeling te werken met ambassadeurs (ntb). Zij zullen op hun eigen afdeling functioneren als aanspreekpunt/ doorgeefpunt/ vraagbaak omtrent informatieveiligheid. Door middel van key-users blijft het mogelijk om in een grote organisatie zoals DOWR toch nog dicht op de afdelingen en hun problematiek te blijven. ***(Actiepunt 10)***

[4] GGI-Veilig | VNG Realisatie

3. Nieuwe ontwikkelingen 2020 en 2021

Zoals gezegd is informatiebeveiliging een continu, niet statisch, proces. De kracht van implementatie zit in het telkens, waar nodig, aanpassen bijsturen van de maatregelen. Ook raakt het onderwerp de gehele organisatie, want informatiebeveiliging is niet van iemand, maar juist van alle collega's die dagelijks met (risico's van) informatie omgaan.

Ontwikkelingen 2020

Digitale veiligheid topprioriteit

Afgelopen jaar is de externe (cyber-)dreiging meer relevant geworden waarmee wij als digitale organisatie rekening moeten houden. ‘Het is niet de vraag of wij gehackt worden, maar bekend wordt dat wij gehackt zijn’, wordt vaak gebruikt om aan te geven wat de ernst van de huidige situatie is. Onderstaand een overzicht van de digitale dreigingen in ons land van de afgelopen 14 maanden.



Figuur 7 Informatieveiligheid in het nieuws 2019-2020

Dagelijks ondervindt onze stad en regio de gevolgen van data-incidenten en worden we geconfronteerd met risico’s op het gebied van privacy en informatiebeveiliging. Digitaliseringsontwikkelingen nemen alsmaar toe evenals de afhankelijkheid van betrouwbare informatie(-systemen).

Kritische kennisdeling (regio IJsselland)

In het belang van digitale veiligheid en cyberincidenten in het bijzonder is kritische kennisdeling buiten de organisatie met betrokken partners van groot belang om de digitale weerbaarheid te vergroten.
In 2020 is vanuit DOWR in samenwerking met Zwolle en andere IJsselland gemeenten hiervoor een CISO-overleg gestart. In 2021 wordt dit overleg verder geconcretiseerd en aansluiting gezocht daar waar nodig bij ondersteunde partners zoals bijvoorbeeld de IBD (VNG Realisatie) en het NCSC van het Ministerie van Justitie en Veiligheid.
Doelstelling hierbij is enerzijds te leren van elkaars incidenten en hierin proactief

(preventief) te kunnen bijsturen, maar ook integratie bij Integrale Veiligheid (OOV), met betrekking tot deze nieuwe vorm van (cyber-)criminaliteit.
Onder regie van Deventer is hiervoor in 2019 een Coördinator Integrale Veiligheid aangesteld om dit proces binnen de regio te initiëren. (***Actiepunt 7)***

Ontwikkelingen 2021

Resolutie Digitale Veiligheid (VNG)

In februari 2021 wordt de Resolutie Digitale Veiligheid vastgesteld op de Bijzondere Algemene Ledenvergadering van de VNG. Hiermee wordt het onderwerp vanuit de bestuurstafel geborgd en kunnen middelen worden gealloceerd om ons als gemeenten te helpen digitaal weerbaar te worden.

Bestuurlijke principes (handelingsperspectief)

Om te komen tot een (programma) digitaal veilige gemeente is het nodig om de bijbehorende bestuurlijke principes voor directie en management (bron: Dreigingsbeeld Nederlandse gemeenten 2021/2022 VNG-realisatie, 2020) vast te stellen. Vanuit het handelingsperspectief worden de volgende maatregelen voorgesteld;

- Voer de regie over risicomanagement
- Techniek is niet de belangrijkste factor
- Cultiveer een veilige organisatie
- Bied veilige gereedschappen
- Zorg voor een open cultuur
- Faciliteer dat de basis op orde komt
- Oefen en wees voorbereid op incidenten

Op advies van de CISO (januari 2021) is aansluitend op de VNG resolutie Digitale Veiligheid (BALV d.d. 12-2-2021) geadviseerd aan Directie en College B&W om akkoord te gaan met deze resolutie.

Vanuit de Informatiebeveiligingsdienst (VNG-realisatie) is inmiddels een ondersteunend programma Verhogen Digitale Weerbaarheid gestart om gemeenten hierbij te helpen. Moet gezegd dat elke gemeente uiteraard zelf verantwoordelijk is voor verdere inrichting.

Extra inspanningen?

Met vaststelling van de VNG Resolutie (februari 2021) behoort Digitale Veiligheid voor de komende jaren tot één van de meest belangrijke kerntaken van de gemeente.

Naar verwachting zullen er komende jaren extra inspanningen en middelen vrijgespeeld moeten worden om aan deze kerntaak te voldoen cq de digitale veiligheid te bergroten. Onduidelijk is echter op dit moment nog welke inspanningen en aanvullende maatregelen hiervoor nodig zijn.
In samenwerking met DOWR-I, F&C en Directie DOWR zal dit komend halfjaar onderzocht moeten gaan worden, waarna bijstelling van dit Informatiebeveiligingsplan 2021 en of 2022 opgemaakt kan worden om tot concrete resultaten te komen.
(Actiepunt 15)

4. Planning

- Onderstaande planning is daar waar van toepassing gesynchroniseerd met de planning Privacy. Bij de actiepunten met een hoge prioriteit is dit Q1 en Q2;
- Bij de actiepunten met een gemiddelde prioriteit is dit Q3 en Q4; en
- Bij de actiepunten met een lage prioriteit is dit Q4 en verder.

		Periode				
		2021				2022 e.v.
#	**Actiepunt**	Q1	Q2	Q3	Q4	>
	Bewustwording					
1	Ontwikkelen communicatie- en bewustzijnsplan icm privacy (hoog)		X			
2	Aandacht voor het communicatie- en bewustzijnsthema ‘dataclassificatie’ (midden)				X	
3	Aandacht voor het communicatie- en bewustzijnsthema ‘crisismanagement’ (midden)			X		
	Bedrijfscontinuïteit					
4	Bedrijfscontinuïteit BCP/Crisismanagement (hoog)	X	X			
5	Inrichting ISMS d.m.v. informatieveiligheidtoetsen in lijn met doorontwikkeling GRC-riskmanagement (hoog)		X	X		
6	Ontwikkelen BIO-procedure m.b.v. ENSIA tool tbv jaarlijkse zelfevaluatie in opdracht van VNG/ Ministerie BiZa (hoog)		X	X		
7	Kritische Kennisuitwisseling (midden)			X		
8	Toetsing huidige systemen op huidige en toekomstige standaarden (midden)			X	X	
	Inbedding organisatie					
9	Inrichting GGI-veilig organisatie		X	X		
10	Aanwijzen domeinspecifieke key-users informatiebeveiliging (hoog)	X	X			
11	Toegangsrechten communicatiebeveiliging (midden)			X		
	Contractbeheer					
12	Security by design bij inkoop (hoog)		X			
13	Passend niveau van beveiliging bij geautomatiseerde systemen (midden)			X		
	Beleid					
14	Ontwikkelen dataclassificatie (vertrouwelijkheid) beleid (midden)			X		
15	Onderzoeken extra maatregelen VNG Resolutie Digitale Veiligheid			X	X	X

5. Begroting 2021

Actiepunten	***Noemer***	***Euro***
5,***6 (?)***	ISMS (informatie veiligheid management instrumentarium)	*25.000,00*
9	SIEM (logging en signalering) – GGI Veilig	*70.000,00*
1, 2, 3, ***10***	Onderhouden awareness	*50.000,00*
12, 13, 14	Vertrouwelijkheid gegevens	*55.000,00*
9/ ***4 (?)***	Respons cyberincidenten	*20.000,00*
8, 11, 13	IDM (toegangsbeveiliging)	*100.000,00*

Bijlage Afkortingenoverzicht

AVG	Algemene Verordening Gegevensbescherming
BALV	Bijzondere Algemene Leden Vergadering VNG
BBN	Basis beveiligingsniveau (BIO)
BCP	Businesscontinuïteitsplan
BIO	Baseline Informatiebeveiliging Overheid (voorheen BIG, BIR)
CISO	Chief Information Security Officer
COVID-19	Corona pandemie 2019-2021
DOWR	Samenwerkende gemeenten Deventer Olst-Wijhe en Raalte
DPIA	Data Privacy Impact Assessment
GAP analyse	Kloof (Engels)
GGI Veilig	Gemeentelijke Gemeenschappelijke Infrastructuur
IB	Informatiebeveiliging
IBD	Informatiebeveiligingsdienst (VNG Realisatie)
IBP	Informatiebeveiligingsplan
IDM	Identity management (Toegangsbeveiliging)
ISMS	Information Security Management Systeem (BIO)
IV	Informatieveiligheid
MD-traject	Management development traject
NCSC	Nationaal Cyber Security Centrum (Ministerie J&V, NCTV)
NEN	Nederlands Normalisatie-instituut (NEN)
NTA-9001	Nederlands Technische Afspraken
OOV	Openbare Orden en Veiligheid (proces)
PDCA	Plan Do Check Act (Deming circle)
PFO	Portefeuillehouder overleg
RA(S)CI matrix	Responsible (Verantwoordelijk) Accountable (Eindverantwoordelijk Supportive (Geraadpleegd) Informed (Geïnformeerd)
SIEM	Security Incident and Event Management
SOC	Security Operations Center
VNG	Vereniging Nederlandse Gemeenten