Zwolle dataveilig?

Onderzoek naar informatieveiligheid binnen de gemeente Zwolle

15 september 2025

Rekenkamer Zwolle

Inhoudsopgave

Voorwoord

Een cyberaanval waardoor de dienstverlening van de gemeente wordt verstoord, gegevens worden gestolen of losgeld wordt geëist. Onbevoegde toegang tot informatie, misbruik van vertrouwelijke gegevens, of het wijzigen van bijvoorbeeld WOZ-waarden of stemuitslagen. Datalekken waarbij gevoelige persoonsgegevens van inwoners zoals BSN-nummers, adressen en medische gegevens op straat komen te liggen.

De gemeente beheert een enorme hoeveelheid gegevens. Systemen en processen draaien erop en steeds vaker geautomatiseerd en online. De complexe samenleving vraagt inwoners en organisaties hun digitale ziel en zaligheid te overleggen aan overheden en uitvoeringsinstanties. Zijn al die data in veilige handen? Hoe gaat de gemeente Zwolle om met deze verantwoordelijkheid?

Niet voor niets stellen wetten en regels steeds strengere eisen aan informatieveiligheid binnen gemeenten. Toch kan nooit worden voorkomen dat er soms iets fout gaat. Uiteindelijk blijft informatie verwerken mensenwerk en een ongeluk zit in een klein hoekje. Maar een klein foutje kan grote gevolgen hebben: overlast, fraude, schade. En uiteindelijk voor het aanzien van en vertrouwen in de overheid. Het belang van informatieveiligheid kan dan ook niet overschat worden.

Als rekenkamer vroegen wij PRAE-advies onderzoek hiernaar te doen in Zwolle. Naast de gebruikelijke analyse van documenten en interviews met betrokkenen, is met mystery guests en phishingmails in de praktijk getest of je fysiek of digitaal binnen kunt dringen bij de gemeente Zwolle. Ook is goed gekeken naar de audits en testen van de gemeente en het Shared Service Centrum ONS (SSC ONS).

Wij bedanken Etienne Lemmens van PRAE-advies voor zijn deskundige en secure blik en de plezierige samenwerking. Met zijn bevindingen komt de Rekenkamer tot de conclusie dat veel goed gaat, maar dat er ook aandachtspunten. Wij doen in dit rapport belangrijke aanbevelingen over wat nog beter kan.

Wij vertrouwen erop met dit onderzoek een goed beeld te geven of data bij de gemeente Zwolle in veilige handen zijn. Ook draagt dit onderzoek hopelijk bij aan de aandacht voor dit belangrijke onderwerp, het risicobewustzijn en de voortdurende alertheid bij medewerkers, bestuurders en raadsleden. En Rekenkamerleden natuurlijk: ik heb om te beginnen mijn wachtwoord maar weer eens vernieuwd.

Namens de Rekenkamer Zwolle

Dirk Jan Droogh (voorzitter)

Leden Rekenkamer: Bert-Jan Buiskool, Ilja Jacobs, Karin Ligthart, Magdaléna Ritmeijer

Ambtelijk secretarissen: Evert-Jan Bagerman en Iris Gosemeijer

Samenvatting, conclusies en aanbevelingen

Aanleiding en doel

Als samenleving zijn we in transitie naar een informatiesamenleving. Deze transitie brengt nieuwe kansen, maar ook een groeiend aantal risico's met zich mee. Steeds meer systemen en processen zijn gedigitaliseerd en de samenleving is hier in toenemende mate afhankelijk van geworden. Dit maakt dat informatieveiligheid een beleidsterrein is dat volop in beweging en ontwikkeling is. Er is sprake van toenemende dreiging van kwaadwillende actoren. Verschillende overheidsinstanties - Hof van Twente, Buren, Universiteit Maastricht en TU Eindhoven zijn enkele voorbeelden - zijn in de afgelopen jaren slachtoffer geworden van een cyberaanval.

De accountant van Zwolle heeft in de afgelopen jaren verschillende malen gewezen op de risico's. Daarbij is vastgesteld dat in de afgelopen jaren weliswaar verbeterstappen zijn gerealiseerd, maar dat er nog veel stappen te zetten zijn om tot een kwalitatief goede beheersing van IT-risico's te komen.

Mede vanwege de toenemende dreiging is de Europese en landelijke wet- en regelgeving in de afgelopen jaren aangescherpt. Het beleid dat overheden op dit beleidsterrein formuleren en uitvoeren moet risicogestuurd zijn. Daarbij is tegelijkertijd duidelijk dat het volledig uitsluiten van risico's onmogelijk is.

Tegen de hiervoor genoemde achtergronden hebben wij onderzoek gedaan naar de uitvoering van het informatieveiligheidsbeleid van de gemeente Zwolle. Het doel van het onderzoek is inzicht te geven in de manier waarop Zwolle invulling geeft aan informatiebeveiliging en in beeld te brengen hoe het is gesteld met de informatieveiligheid van de gemeente Zwolle. Een daarvan afgeleid doel is de raad in staat te stellen zijn kaderstellende en controlerende rol op het gebied van informatiebeveiliging te kunnen uitvoeren.

Onderzoeksbureau PRAE-advies heeft dit onderzoek voor ons uitgevoerd. Het onderzoek vond plaats van december 2024 tot maart 2025 en richtte zich op drie kernterreinen van informatieveiligheid: organisatie, mens en techniek. Daarnaast is de betrokkenheid van de raad op deze thema's onderzocht.

Het onderzoek is uitgevoerd met behulp van documentanalyse, interviews met functionarissen en bestuurders en verschillende testen zoals phishing mails en een inlooptest met mystery guests. Het onderzoek betrekt ook de intensieve samenwerking met Shared Service Centrum ONS (SSC ONS), een gemeenschappelijke regeling[1] die de IT-dienstverlening voor de gemeente voor een belangrijk deel verzorgt. De gemeente en het Shared Service Centrum ONS (SSC ONS) voeren zelf ook audits en testen uit. De testen in het kader van het rekenkameronderzoek waren aanvullend op deze audits en testen en geven een beeld van de veiligheid van systemen en het risicobewustzijn bij medewerkers, bestuurders en raadsleden.

[1] Een gemeenschappelijke regeling is een besluit tot samenwerking tussen bestuursorganen van gemeenten, provincies, waterschappen of andere openbare lichamen om één of meer bepaalde belangen van die bestuursorganen te behartigen. In de gemeenschappelijke regeling SSC ONS werken de gemeenten Zwolle, Kampen, Dalfsen, Westerveld, Zwartewaterland, Ommen en de provincie Overijssel samen. SSC ONS verzorgt de taken op het gebied van ICT, Inkoop en HR.

Samenvatting / beantwoording centrale onderzoeksvraag

De volgende onderzoeksvraag stond in dit onderzoek centraal:

Hoe is het gesteld met de informatiebeveiliging van de gemeente Zwolle, wat zijn de zwakke plekken en hoe kunnen deze worden verholpen?

De gemeente Zwolle is zich in toenemende mate bewust van het belang van informatiebeveiliging om zo weerbaar te zijn tegen cyberaanvallen. Er zijn in de afgelopen jaren ook serieuze stappen gezet op het gebied van informatiebeveiliging. Er is strategisch beleid gemaakt en verantwoordelijkheden zijn goed vastgelegd. Het college en de directie dragen het belang van informatieveiligheid uit en aan risicobewustzijn in de organisatie wordt aandacht besteed. Testen op de systemen en de menselijke factor worden uitgevoerd om iedereen in de organisatie betrokken en alert te houden. Op basis hiervan worden rapportages en verbeterplannen opgesteld. Dat is positief.

Op veel onderdelen is echter nog verbetering nodig om op informatiebeveiliging en privacy te kunnen voldoen aan de wettelijke verplichtingen en zo voldoende weerbaar te zijn. Dat geldt zowel voor de nu geldende als voor de binnenkort verhoogde eisen met betrekking tot de cybersecurity. De Rekenkamer constateert dat het risicobewustzijn in de organisatie aanwezig is en er steeds meer inspanning wordt gepleegd om ‘in control’ te komen. Volledig alle risico’s uitsluiten is wensdenken, maar bewust zijn van de risico’s die de organisatie loopt en daarop acteren moet het streven zijn. Om op informatieveiligheid ‘in control’ te raken en te voldoen aan Europese en landelijke wet- en regelgeving is extra inzet en aandacht nodig. In de conclusies en aanbevelingen op de volgende pagina’s wordt dit nader uiteengezet.

Organisatie

Wat gaat goed?	Wat kan beter?	Welke aanbevelingen hebben we?
1.1 De gemeente beschikt over (algemeen) privacybeleid en strategisch informatieveiligheidsbeleid voor de periode 2022-2026. De ambities van de gemeente en de verschillende taken/rollen met betrekking tot informatiebeveiliging en privacy zijn hierin helder beschreven. Vanwege aangescherpte Europese wetgeving wordt dit jaar al een nieuw strategisch beleid opgesteld. 1.2 College en directie zijn doordrongen van het belang van informatieveiligheid. De gemeente heeft sinds 2022 een continuïteitsplan ICT om langdurige stagnatie van kritische bedrijfsprocessen te voorkomen. 1.3 Op privacygebied zijn de door de AVG voorgeschreven protocollen aanwezig, zoals voor inzageverzoeken en het melden van datalekken. 1.4 Voor overheden geldt de Baseline Informatiebeveiliging Overheid (BIO). In 2021 bleek de BIO-compliance van de gemeente met 19% ver onder de maat. In de afgelopen jaren is een inhaalslag gemaakt om de beleidsstukken, protocollen en richtlijnen op tactisch niveau op orde te brengen. 2.1 Op tactisch en operationeel niveau zijn de benodigde 'tools' aanwezig. Zo is er een Identity Acces Management (IAM)-systeem dat de toegangsrechten/autorisaties van medewerkers tot systemen en gegevens regelt. Dit geldt ook voor het leveranciersmanagementsysteem en een zogenoemd Information Security Management Systeem (ISMS) waarin activiteiten op het gebied van informatieveiligheid vastgelegd kunnen worden. 3.1 Er is een Functionaris Gegevensbescherming (fulltime) en een Chief Information Security Officer (CISO) (0,5 fte) aangesteld. Voor de doorvertaling naar tactisch en operationeel niveau zijn onlangs drie Privacy en Information Security Officers aangesteld. Dit kan helpen de achterstand op het beleidsterrein van informatieveiligheid in te lopen.	1. Het strategisch beleid op het gebied van informatiebeveiliging staat en wordt in 2026 geactualiseerd. Op tactisch en operationeel niveau zijn echter nog lacunes aanwezig. De gemeente is bezig, onder andere door extra personeel aan te trekken, deze lacunes in te vullen. 2. De 'tools' die op tactisch en operationeel niveau aanwezig zijn worden nog niet optimaal gebruikt, waardoor risico's buiten beeld blijven of niet goed vastgelegd worden in de PDCA-cyclus. Dit geldt voor het IAM-systeem, het leveranciersmanagement-systeem en het ISMS. De gemeente voldoet op basis van bovenstaande slechts gedeeltelijk aan de gestelde normen op informatiebeveiligings- en privacygebied en loopt daardoor serieuze risico's. Ook laat de gemeente hiermee kansen liggen om informatieveiligheid in een breder risicomanagement in te passen. 3. Een belangrijke stap voor beheersing van de informatiebeveiligingsrisico's is een juiste omvang en positionering van de CISO-functie. De omvang van de CISO-functie (0,5 fte) in Zwolle is niet conform de zwaarte van de functie. Ook de positie in de organisatie (onderdeel van de afdeling Informatievoorziening) past niet bij de functie. De CISO zou gelet op zijn strategische rol een directe lijn met directie en bestuurders moeten hebben om zo onafhankelijk te kunnen opereren.	1. **Actualiseer en completeer het beleid op tactisch en operationeel niveau en informeer de raad hierover in het kader van de jaarlijkse ENSIA-rapportage.** 2. **Benut de aanwezige systemen beter en informeer de raad hierover in het kader van de jaarlijkse ENSIA-rapportage.** 3. **Waardeer de functie van CISO op naar 1,0 fte en positioneer de functie zodanig dat de CISO onafhankelijk van de lijn functioneert en een directe lijn met directie en bestuurders heeft.**

Mens en techniek

Wat gaat goed?	Wat kan beter?	Welke aanbevelingen hebben we?
4. Het bewustzijn van risico's bij het werken met (persoons)gegevens is de afgelopen jaren toegenomen. In 2022 is een vierjarige bewustwordingscampagne voor medewerkers gestart met als doel om eigenaarschap, verantwoordelijkheid en bewustwording in de lijn beter belegd te krijgen.	4. De volwassenheidsgraad op informatieveiligheid ligt tussen niveau 2 en 3, terwijl niveau 3 als doel is gesteld. Het eigenaarschap in de lijn kan versterkt worden. Hier wordt weliswaar aandacht aan besteed, onder andere door een (niet-verplichte) e-learning, maar hier wordt nog niet op gestuurd.	**4. Versterk het risicobewustzijn en het eigenaarschap van de medewerkers op het gebied van informatieveiligheid, onder andere door e-learnings verplicht te maken.**
5.1 In het kader van het onderzoek zijn een phishing mail test en inlooptests uitgevoerd. Bij de phishing mail test onder medewerkers en bestuurders werd iets beter gescoord dan de benchmark. 5.2 SSC ONS en de gemeente zijn aangesloten bij de Informatiebeveiligingsdienst (IBD) voor kwetsbaarheidsmeldingen. Bij meldingen zijn functionarissen aan zet om eventueel benodigde acties in gang te zetten. In het kader van het project Verhoogde Digitale Weerbaarheid is een applicatie geïnstalleerd waarmee verdacht verkeer op het netwerk kan worden gedetecteerd en ondervangen. Er is ook zogenaamde 'endpoint protection' ingericht, waarbij verdachte activiteiten op een computer of laptop kunnen worden gedetecteerd en geïsoleerd.	5.1 Bij de inlooptest op het stadskantoor konden mystery guests met personeel meelopen naar niet-publieke ruimtes zonder aangesproken te worden. Ook in het stadhuis konden ze bij toegangspoorten met paslezer meelopen zonder opgemerkt te worden. De resultaten van deze test leiden tot een 'gemiddeld' risico op ongeoorloofde fysieke toegankelijkheid. 5.2 In het kader van het rekenkameronderzoek zijn een Active Directory (AD) audit en een wifi-netwerk test uitgevoerd. Bij de AD-audit werden accounts met een zwak wachtwoord aangetroffen, accounts met een wachtwoord van een jaar of ouder, accounts met niet-unieke wachtwoorden en accounts met een verouderde verificatiemethode. Er zijn zeven bevindingen met risicoclassificatie 'hoog' en acht met een 'gemiddelde' risicoclassificatie, wat leidt tot een volledige risicoscore 'hoog'. De wifi-netwerktest resulteerde in een 'laag' risico.	**5. Ga met de bevindingen uit de testen aan de slag, stel hiervoor een verbeterplan (met deadlines en actiehouders) op en informeer de raad over de opvolging van de verbetermaatregelen.**
6 Er is een crisisplan van SSC ONS en een continuïteitsplan ICT van de gemeente Zwolle voor het geval dat door stroomuitval of een andere calamiteit de dienstverlening aan burgers, bedrijven en instellingen in het geding komt. De dienstverlening kan verplaatst worden naar een uitwijklocatie.	6. De uitwijk- en bedrijfscontinuïteitsplannen voor calamiteiten worden slechts oppervlakkig getest.	**6. Voor periodiek diepgaande en fysieke testen uit op de uitwijk- en bedrijfscontinuïteitsplannen, zo nodig in samenwerking met SSC ONS.**

Betrokkenheid raad

Wat gaat goed?	Wat kan beter?	Welke aanbevelingen hebben we?
7.1 De raad wordt jaarlijks geïnformeerd via de ENSIA-rapportage, waarin het college aangeeft in welke mate de gemeente 'in control' is op het gebied van informatiebeveiliging en privacy. Ook de FG en de CISO brengen jaarlijks verslag aan de raad uit over hun bevindingen. De accountant voert jaarlijks een IT-controle uit en rapporteert hierover in de boardletter die met de auditcommissie besproken wordt. 7.2 Er worden incidenteel sessies georganiseerd om de raad bij te praten over informatieveiligheid.	7. De raad is nog niet goed aangesloten op beleid en uitvoering van de thema's informatiebeveiliging en privacy. De sessies die incidenteel georganiseerd worden om de raad mee te nemen op deze thema's worden matig bezocht.	**7. Bespreek de ambities, opzet en uitvoering van het beleid op informatieveiligheid geregeld (minimaal één keer per jaar) met elkaar. Agendeer de ENSIA-rapportage voor een vergadering van de auditcommissie en bespreek deze gelijktijdig met de boardletter van de accountant, waarin gerapporteerd wordt over de IT-audit.**

Bestuurlijke reactie

Memo

Aan Rekenkamer Zwolle

Van College van burgemeester en wethouders

Datum 9 september 2025

Onderwerp Collegereactie rekenkameronderzoek informatieveiligheid

Inleiding
De Rekenkamer deed onderzoek naar de informatieveiligheid van de gemeente Zwolle. De centrale vraag die de Rekenkamer onderzocht: *Hoe is het gesteld met de informatieveiligheid van de gemeente Zwolle, wat zijn de zwakke plekken en hoe kunnen deze worden verholpen?*

Om deze vraag te beantwoorden keek de Rekenkamer zowel naar de organisatie, de mens als de techniek. Daarnaast kreeg de betrokkenheid van de raad bij het onderwerp informatieveiligheid apart aandacht. De Rekenkamer voerde het onderzoek uit met als doel de raad in zijn kaderstellende en controlerende rol te ondersteunen.

De resultaten van het onderzoek staan in het rapport "Zwolle Dataveilig?". Dit rapport is aangeboden aan het college voor een bestuurlijke reactie op de conclusies en aanbevelingen. Het college van burgemeester en wethouders heeft het onderzoeksrapport met veel interesse gelezen en dankt de Rekenkamer voor haar inzet en aanbevelingen. Het rapport geeft een herkenbaar beeld van de stand van onze informatieveiligheid en het toont opnieuw aan welke urgentie het onderwerp heeft, en dat het onderwerp voor alle onderdelen van onze organisatie, van raad tot de medewerkers, van groot belang is.

Daarnaast geeft het onderzoek waardevolle aanbevelingen om op het onderwerp informatieveiligheid samen met de raad een volgende stap in volwassenheid te zetten.

Hieronder vindt u de bestuurlijke reactie van het college van burgemeester en wethouders. Het rekenkameronderzoek geeft zeven concrete aanbevelingen, met een zwaartepunt op tactische en operationele bedrijfsvoering. Per aanbeveling geven we hier een bestuurlijke reactie op, waarbij we, waar dit relevant is, de verschillende perspectieven uit het onderzoek (organisatie, mens, techniek en rol van de raad) benoemen. Bij meerdere aanbevelingen doen we concrete toezeggingen voor vervolgstappen.

Kader
IBD-Dreigingsbeeld-informatiebeveiliging-2025-2026.
Raadsvoorstel Robuuste Informatievoorziening

Kernboodschap
Door verdergaande digitalisering is de afhankelijkheid van ICT (-middelen) toegenomen, evenals de hoeveelheid informatie die in onze organisatie wordt verwerkt. De beschikbaarheid, integriteit en

vertrouwelijkheid van deze informatie is van cruciaal belang voor de continuïteit en kwaliteit van onze gemeentelijke processen.

In Zwolle werken we al geruime tijd actief aan het versterken van onze informatieveiligheid. Dit vraagt om een continue herbeoordeling van onze processen, waarbij we gericht verbeteringen doorvoeren om risico's te beheersen en onze organisatie toekomstbestendig te houden.

Ook dit rekenkameronderzoek draagt hieraan bij, door aanbevelingen te doen die de organisatie mee kan nemen in haar doorlopende inspanningen voor verdere professionalisering op dit gebied.

Toelichting
De Rekenkamer illustreert in haar onderzoek hoe digitalisering steeds meer aan maatschappelijk belang wint. Of een inwoner zich nu verplaatst in het verkeer, een huis zoekt in een veilige omgeving of een paspoort aanvraagt: steeds meer gemeentelijke processen zijn afhankelijk van techniek, data en informatie. En daarmee is data- en informatieveiligheid een essentieel onderwerp.

Het is daarom waardevol dat de Rekenkamer het onderwerp data- en informatieveiligheid bij de gemeente Zwolle heeft onderzocht. We zien in het onderzoek belangrijke onderwerpen langskomen, waarop we graag een betrokkenheid van de raad zien. Gezamenlijk hebben we de taak om zorgvuldig met de gegevens van inwoners, bedrijven en andere organisaties om te gaan, en de informatieveiligheid op een adequate wijze te waarborgen. Ook het rekenkameronderzoek draagt hieraan bij.

<u>Aanbeveling 1: Actualiseer en completeer het beleid op tactisch en operationeel niveau en informeer de raad hierover in het kader van de jaarlijkse ENSIA-rapportage.</u>

Reactie: Deze aanbeveling wordt herkend en sluit aan bij eerder geconstateerde bevindingen van onder andere de accountant en Functionaris Gegevensbescherming. We zijn al volop bezig met actualiseren en completeren van beleid en zien het rekenkameronderzoek als extra steun in de rug. Ook stellen we voor om een periodieke afstemming tussen college en raad te organiseren over deze onderwerpen.

Belangrijke stappen op dit onderwerp zetten we nu al. Zo is eerder in 2025 een project gestart met als doel om een kwaliteitsmanagementsysteem (KMS) in te voeren. Het invoeren van een kwaliteitsmanagementsysteem helpt ons om zowel voor informatiebeheer, informatiebeveiliging als privacy de juiste structuur en samenhang aan te brengen. Met een kwaliteitsmanagementsysteem leggen we eenduidige afspraken vast, creëren we inzicht in onze processen en borgen we dat we continu verbeteren. Het identificeren, plannen, uitvoeren en monitoren van verbeteracties wordt ondergebracht in het kwaliteitsmanagementsysteem. Het volgen van een continue verbetercyclus stelt ons in staat om aantoonbaar te voldoen aan relevante wet- en regelgeving, onder meer de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) en de Europese *Network and Information Security 2* richtlijn (NIS2).

Verbeteracties variëren van het opstellen van encryptiebeleid tot het inrichten van een proces voor meldings-plichtige incidenten. Daarnaast krijgen diverse bestaande beleidsstukken, zoals het wachtwoordbeleid en incidentmanagementproces, een opfrisbeurt. Alle bestaande en nieuwe processen die we voor informatieveiligheid vormgeven, leggen we in de komende periode vast in een processenboek. Voor de eerste BIO2 implementatie trekken we, zoals ook al genoemd in het Raadsvoorstel Robuuste Informatievoorziening, twee jaar uit. Daarna moet het continu verbeteren en monitoren van informatieveiligheid op deze onderwerpen onderdeel van het dagelijks werk zijn.

Ook geeft het onderzoek aan dat de beheersing van risico's in het kader van de AVG onvoldoende op orde is. Op basis van een eerder signaal hierover van de Functionaris Gegevensbescherming, hebben we al opdracht gegeven voor een inhaalslag in zogenoemde *Data Protection Impact Assessments* (DPIA's) van onze processen. Deze DPIA's leggen eventuele privacy-risico's bloot. De inhaalslag ronden we in 2027 af.

Daarnaast verwijst het rekenkameronderzoek naar de boardletter van de accountant. Daarin stond een oproep om werk te maken van de IT general controls. Om te komen tot nog duidelijkere procedures die de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-systemen waarborgen, hebben we inmiddels extra capaciteit toegevoegd aan het team voor service delivery management. Hiermee is de benodigde formatie beschikbaar om een actieplan te maken met IT-beheersmaatregelen, zoals het verbeteren van toegangsbeleid, wijzigingsbeheer en afspraken met ketenpartners.

In onze overtuiging is het wenselijk om periodiek een afstemming te organiseren tussen college en raad, waarbij de weerbaarheid, continuïteit en risico's van onze organisatie in een bredere context worden besproken. Wij stellen daarmee een overleg voor dat een stap verder gaat dan zoals beschreven in de aanbevelingen van de Rekenkamer. Dit overleg biedt ruimte voor een inhoudelijke dialoog, zodat de raad goed geïnformeerd is en er gezamenlijk richting kan worden gegeven aan strategische keuzes.

De samenhang met de behandeling van de ENSIA-rapportage lijkt daarmee niet het juiste moment te zijn om de raad hierover te informeren, aangezien dit een gerichte evaluatie is en een proces van bestuurlijke verantwoording kent op specifieke onderdelen van onze dienstverlenende organisatie.

Aanbeveling 2: Benut de aanwezige systemen beter en informeer de raad hierover in het kader van de jaarlijkse ENSIA-rapportage.

Reactie: Momenteel lopen er twee belangrijke projecten die bijdragen aan het waarborgen van informatieveiligheid. Ook hierover willen we informeren tijdens de voorgestelde periodieke afstemming tussen college en raad.

Het rekenkameronderzoek verwijst naar het lopende Identity & Access Management (IAM)-project, dat bijdraagt aan de digitale weerbaarheid van onze organisatie. We verwachten in de tweede helft van 2025 de eerste applicaties op de nieuwe IAM-tooling aan te sluiten. Deze stap stelt ons in staat om bestaande systemen beter te benutten door toegangsbeheer te centraliseren en te automatiseren. Op basis van de eerste ervaringen bepalen we de vervolgstappen, zoals uitbreiding naar andere systemen en aanscherping van het toegangsbeleid. IAM helpt ons om risico's te beperken, processen te stroomlijnen en te voldoen aan wet- en regelgeving.

Daarnaast zijn we in 2025 gestart met het project voor de invoering van een kwaliteitsmanagementsysteem, waarmee een belangrijke stap richting structurele borging en aantoonbare naleving van wet- en regelgeving op het gebied van informatiebeheer, informatiebeveiliging en privacy wordt gezet.

Als aangegeven bij aanbeveling 1 kan inhoudelijke afstemming plaatsvinden in de dialoog tussen college en raad. Behandeling van de ENSIA verantwoording staat hier los van, maar kan uiteraard wel een inhoudelijk onderwerp van gesprek zijn.

Aanbeveling 3: Waardeer de functie van CISO op naar 1,0 fte en positioneer de functie zodanig dat de CISO onafhankelijk van de lijn functioneert en een directe lijn met directie en bestuurders heeft.

Reactie: We herkennen de noodzaak dat bewaakt moet worden dat de CISO voldoende onafhankelijkheid heeft om zijn werk te doen. De ureninzet is daarbij een vraag met een breder organisatorisch perspectief.

Allereerst zien wij, net als de Rekenkamer, dat we de bemensing op het onderwerp informatieveiligheid stevig versterkt hebben: met alleen al in 2025 een aanzienlijke groei van het team privacy en informatiebeveiliging, de aanstelling van een eerste IT-auditor en extra capaciteit om werk te maken van IT-beheersmaatregelen. De recente uitbreiding van capaciteit biedt kansen om verantwoordelijkheden scherper te positioneren en processen beter te stroomlijnen. Het lijkt ons passend om eerst deze structuur te verankeren en te benutten, zodat we vervolgens gerichter kunnen beoordelen of een verdere uitbreiding van fte daadwerkelijk bijdraagt aan effectievere risicobeheersing en strategische sturing.

Als we de eventuele uitbreiding en herpositionering van de CISO-functie overwegen, willen we dit zorgvuldig doen. Daarbij telt onder meer de afweging of dit noodzakelijk is voor het bereiken van ons gewenste volwassenheidsniveau op informatieveiligheid, hoe de organisatie aankijkt tegen de ontwikkeling en positie van 2e en 3e lijns functionarissen en ook het zicht op de eventuele risico's. Zonder extra geld vrij te maken, betekent dit bijvoorbeeld dat we een halve fte voor een strategisch adviseur informatieveiligheid zouden kwijtraken.

Voor de ureninzet en de positionering van de CISO geldt dat dit in breder organisatieperspectief gewogen moet worden, zodat een goed systeem van checks en balances ontstaat. Wel nodigt de aanbeveling ons uit om voldoende onafhankelijkheid in de huidige werkzaamheden van de CISO te blijven borgen, ongeacht waar deze voor HR-verantwoordelijkheden is gepositioneerd.

Aanbeveling 4: Versterk het risicobewustzijn en het eigenaarschap van de medewerkers op het gebied van informatieveiligheid, onder andere door e-learnings verplicht te maken.

Reactie: Deze aanbeveling onderschrijven we. Als college vinden we het belangrijk om risicobewustzijn te bevorderen binnen alle onderdelen van de organisatie, van medewerkers tot raad. We maken daarbij gebruik van verschillende methoden, onder andere e-learning. Voor het versterken van risicobewustzijn en eigenaarschap lopen al initiatieven. Daar zijn de uitkomsten van dit onderzoek helpend bij. De e-learning voor informatieveilig werken maken we daarentegen niet voor alle medewerkers verplicht. We kiezen voor verschillende medewerkers soms bewust voor andere methoden of aanpak, waarbij het vergroten van bewustwording altijd centraal staat.

We bevinden ons momenteel in een tussenfase omdat we overstappen van het bestaande bewustwordingsprogramma naar een vernieuwde, meer toekomstbestendige aanpak. De veranderende dreigingen, aangescherpte wet- en regelgeving (zoals NIS2), en de behoefte aan meer maatwerk vragen om een herijking van ons huidige plan. Deze fase biedt ruimte om bestaande maatregelen te evalueren, nieuwe interventies te ontwerpen en deze beter te laten aansluiten op de rollen en verantwoordelijkheden binnen de organisatie. Uiteindelijk is het doel het volwassenheidsniveau voor bewustwording te verhogen, waarmee de competenties van medewerkers en leidinggevenden aantoonbaar op het gewenste niveau komen.

De training informatieveilig werken blijft een verplicht onderdeel van het inwerktraject voor nieuwe medewerkers. Met als doel om te groeien naar een bewust bekwame organisatie. Daar is de raad zelf ook een onderdeel van. Het rekenkameronderzoek geeft een goede aanleiding om teamleiders en griffie op dit onderwerp in positie te brengen.

Daarnaast komen er aanvullende trainingen voor bestuurders en (hoger) management. Dit is een verplichting die is opgenomen in de nieuwe NIS2-wetgeving. Uiterlijk in het tweede kwartaal van 2026 willen we deze trainingen uitgevoerd hebben en periodiek herhalen.

Aanbeveling 5: Ga met de bevindingen uit de testen aan de slag, stel hiervoor een verbeterplan (met deadlines en actiehouders) op en informeer de raad over de opvolging van de verbetermaatregelen.

Reactie: De bevindingen uit de testen zijn inmiddels opgepakt. Net als bij andere meldingen pakken we deze op via ons werkende changemanagement- en meldingenproces.

We (pen-)testen elk jaar meerdere delen van onze informatievoorziening. We zijn blij dat het rekenkameronderzoek gebruik maakte van vergelijkbare methoden. Dit geeft – los van de onderzoeksinzichten – operationele verbeterkansen voor onze informatieveiligheid.

De onderzoeken tonen opnieuw aan hoe organisatie, techniek en mens samen verantwoordelijk zijn voor informatieveiligheid. Er ligt bijvoorbeeld een wachtwoordbeleid dat termijnen aan geldigheid en complexiteit van wachtwoorden stelt. Dit beleid moet door applicaties vervolgens technisch mogelijk gemaakt of afgedwongen worden, waarbij de medewerkers in het zorgvuldig omgaan met hun wachtwoorden zelf ook een verantwoordelijkheid hebben.

Voor de fysieke toegang hebben we vorig jaar verkend waar verbetering mogelijk is. Dit leidde al tot concrete aanvullende veiligheidsmaatregelen. Daarnaast gaan we medewerkers binnenkort onder meer ondersteunen met technische oplossingen die de veiligheid vergroten. Over de inhoud, opvolging en timing van dit soort specifieke veiligheidsmaatregelen delen we nog geen verdere informatie. Uiteindelijk is ook het gedrag van een medewerker hierin belangrijk. Fysieke toegang krijgt de komende jaren een specifiek accent bij de inspanningen rond bewustwording.

Aanbeveling 6: Voer periodiek diepgaande en fysieke testen uit op de uitwijk- en bedrijfscontinuïteitsplannen, zo nodig in samenwerking met SSC ONS.

Reactie: Het college hecht grote waarde aan een goede bedrijfscontinuïteit en testen is daar een belangrijk onderdeel van. Nieuwe plannen zijn gedeeltelijk uitgewerkt en deels nog in ontwikkeling.

Dit thema krijgt terecht veel aandacht van de Rekenkamer. Informatieveiligheid raakt steeds meer processen in de stad. Risico’s variëren van de uitval van dienstverlening, waardoor mogelijk onveilige situaties ontstaan, tot verstoringen in de energievoorziening of verkeerssituaties.

Medio 2025 is een interne werkgroep geformeerd met veiligheidsspecialisten, de concern controller en de CISO. In afstemming met de Gemeentesecretaris bereiden zij een directieopdracht voor om de weerbaarheid en continuïteit van onze organisatie beter te waarborgen. Dit voorstel wordt later dit jaar besproken door de directie, waarna verder alloceren van middelen en uitwerking kan plaatsvinden.

De bestaande uitwijk- en bedrijfscontinuïteitsplannen worden inmiddels al periodiek getest. Voor de gemeentelijke IT-infrastructuur in het samenwerkingsverband SSC-ONS, is een agenda ontwikkeld voor het opleiden, trainen en oefenen (OTO) van de gezamenlijke crisisorganisatie. Op dit proces is de Veiligheidsregio IJsselland aangehaakt. Deze beheersmaatregelen worden straks jaarlijks geëvalueerd en bijgesteld waar nodig.

Aanbeveling 7: Bespreek de ambities, opzet en uitvoering van het beleid op informatieveiligheid geregeld (minimaal één keer per jaar) met elkaar. Agendeer de ENSIA-rapportage voor een vergadering van de auditcommissie en bespreek deze gelijktijdig met de boardletter van de accountant, waarin gerapporteerd wordt over de IT-audit.

Reactie: Wij onderschrijven het belang van een jaarlijkse bespreking van de ambities, opzet en uitvoering van het beleid op informatieveiligheid. Wel kiezen wij voor een andere route dan door de Rekenkamer voorgesteld.

We vinden het belangrijk dat zowel de raad als – waar passend – de auditcommissie actief betrokken is bij dit onderwerp. Informatieveiligheid raakt immers elk domein en elk onderdeel van onze organisatie: of het nu gaat om de uitwisseling van zeer gevoelige persoonsgegevens in het sociaal domein, of de digitale aansturing van verkeerssystemen in de fysieke leefomgeving tot aan de beveiliging van de iPads van de leden van uw raad. Door het onderwerp structureel te betrekken in het bredere gesprek over weerbaarheid en continuïteit, zorgen we voor samenhang, bestuurlijke betrokkenheid en een gedeeld inzicht in de voortgang en uitdagingen.

We gaan graag minimaal één keer per jaar met de raad in gesprek over de ambities, opzet en uitvoering van het informatieveiligheidsbeleid. Daarbij willen we een stap verder gaan en kiezen we voor een bredere en meer integrale benadering dan de rekenkamer voorstelt. De ENSIA-rapportage en de boardletter van de accountant kunnen hierbij als input dienen. Afhankelijk van het onderwerp en de actualiteit kan ook de auditcommissie worden geïnformeerd of betrokken bij de bespreking van deze stukken. Dit biedt ruimte om bevindingen uit de IT-audit en ENSIA in samenhang te duiden en bestuurlijke reflectie te organiseren.

Vervolg
De in de bestuurlijke reactie opgenomen acties worden opgepakt en de resultaten daarvan komen, waar nodig, terug in de Raad. In elk geval zorgen wij ervoor dat het onderwerp informatieveiligheid minimaal een keer per jaar apart als onderwerp wordt geagendeerd voor bespreking met de Raad.

Burgemeester en wethouders van Zwolle,

burgemeester, Peter Snijders

secretaris, Dick Emmer

Nawoord

Op 9 september ontvingen wij de bestuurlijke reactie van het college van burgemeester en wethouders op het rapport ‘Zwolle dataveilig’. Wij zijn blij te lezen dat het college veel van onze bevindingen herkent en de meeste van onze aanbevelingen onderschrijft. Bij een aantal aanbevelingen plaatst het college kanttekeningen. De bestuurlijke reactie geeft ons aanleiding de volgende aandachtspunten mee te geven aan de raad.

Aandachtspunt 1: benutting systemen

Eén van de belangrijkste conclusies van ons onderzoek is dat op veel onderdelen nog verbetering nodig is om op het gebied van informatiebeveiliging en privacy te kunnen voldoen aan de wettelijke verplichtingen en zo voldoende weerbaar te zijn. Hiervoor is extra inzet en extra aandacht nodig. Het college benoemt in zijn bestuurlijke reactie veel acties en projecten die in gang zijn gezet om dit te realiseren. Ook de Rekenkamer heeft dit in het kader van het onderzoek vastgesteld en als positief beoordeeld.

Het college geeft onder andere aan:

- bezig te zijn met een inhaalslag in de *Data Protection Impact Assessments* van de processen (af te ronden in 2027);
- extra capaciteit te hebben toegevoegd voor *service delivery management*;
- dat in de tweede helft van 2025 de eerste applicaties worden aangesloten op een nieuw *Identity & Access Management* systeem;
- in 2025 te zijn gestart met een project voor de invoering van een kwaliteitsmanagementsysteem.

Het spreekt voor zich dat wij het belang van deze acties en projecten onderschrijven. Tegelijkertijd stellen wij vast dat beperkt wordt ingegaan op onze constatering dat de gemeente “slechts gedeeltelijk voldoet aan de gestelde normen op informatiebeveiligings- en privacygebied en daardoor serieuze risico’s loopt”. Ook wordt niet ingegaan op hoe en wanneer het leveranciersmanagementsysteem en het *Information Security Management Systeem* beter benut gaan worden.

Aandachtspunt 2: Omvang en positionering CISO

Bijzondere aandacht vragen wij voor de omvang en de positionering van de CISO-functie. Uit de reactie op onze aanbeveling en verwijzing naar een afweging in breder perspectief lezen wij geen instemming of voornemen tot opvolging van deze aanbeveling. Met de expliciete suggesties ten aanzien van de positie en formatie van de CISO wil de Rekenkamer concreet maken hoe deze beter kunnen aansluiten bij een gemeente met de omvang van Zwolle. Uiteraard kan de noodzakelijk geachte rol van de CISO ook anders vorm krijgen maar het college geeft in zijn reactie geheel niet aan of en hoe hij invulling denkt te geven aan onze aanbeveling.

Wij zijn positief gestemd dat het college periodiek afstemming en inhoudelijk overleg wil voeren over het informatieveiligheidsbeleid. De motivering waarom dit niet op basis van de ENSIA-rapportage zou kunnen is voor ons niet helder, maar dit laten wij aan raad en college. Wat in ieder geval punten van gesprek zouden moeten zijn, zijn de hiervoor genoemde risico’s over de benutting van de systemen en de omvang en de positionering van de CISO-functie.

Het college sluit zijn bestuurlijke reactie af met de zin “De in de bestuurlijke reactie opgenomen acties worden opgepakt en de resultaten daarvan komen, waar nodig, terug in de Raad”. In dit verband wijzen wij op de wettelijke verplichting hiertoe in art. 185a van de Gemeentewet. Op grond hiervan is het college verplicht “jaarlijks een overzicht van de aan het college gedane voorstellen van de

rekenkamer, vergezeld van zijn standpunt daaromtrent en van de wijze waarop aan de voorstellen vervolg is gedaan.”

Wij zullen de vervolgstappen op het gebied van de informatieveiligheid met belangstelling blijven volgen en zien uit naar de behandeling van ons rapport in uw raad

Onderzoeksrapport PRAE-advies

Eindrapport

Informatiebeveiliging en privacy Gemeente Zwolle

Rekenkamer Zwolle

Juni 2025

Auteur: drs. Etienne Lemmens

Prae Advies en onderzoek, Utrecht

Inhoudsopgave

1 Inleiding

Gemeenten zijn kwetsbaar

Onder andere door de toegenomen taken in het sociaal domein beheren en verwerken gemeenten meer en meer persoonsgegevens en gevoelige data. Dat doen gemeenten in toenemende mate met behulp van digitale hulpmiddelen. Gemeenten zijn daarbij kwetsbaar gebleken, zoals onder andere blijkt uit datalekken en hacks bij gemeenten. Wat gebeurt er bijvoorbeeld als gevoelige informatie op straat komt te liggen of op het dark web[1] wordt aangeboden? Of als de gegevens worden gegijzeld en de digitale dienstverlening aan burgers niet meer mogelijk is?[2] Naast ernstige financiële, juridische en technische gevolgen kunnen deze crises de privacy van burgers en het imago van de gemeente aantasten. Het beveiligen van de toegang tot systemen en verwerking van gegevens is een essentiële taak van gemeenten.

Rekenkameronderzoek

Dat zijn redenen voor de Rekenkamer Zwolle geweest om een onderzoek te doen naar opzet, bestaan en werking van het informatiebeveiliging- en privacybeleid in de gemeente Zwolle. Met als doel de gemeenteraad inzicht te verschaffen in de stand van zaken met betrekking tot informatieveiligheid binnen de gemeente Zwolle. En deze in zijn kaderstellende en controlerende rol op dit dossier positioneren. Dat onderzoek is in december 2024 tot en met februari 2025 uitgevoerd. De Rekenkamer bedankt de ambtelijke organisatie en SSC ONS voor de medewerking die de onderzoekers tijdens de loop van het onderzoek hebben ervaren.

Leeswijzer

In hoofdstuk 2 behandelen we de doelstelling, onderzoeksvragen en de aanpak van het onderzoek. De hoofdstukken 3 tot en met 8 bevatten de bevindingen, geordend aan de hand van de onderzoeksvragen. De bevindingen zijn getoetst in het kader van ambtelijk hoor en wederhoor.

In bijlage 1 zijn de onderzoeksvragen en de bijbehorende normen opgenomen. In bijlage 2 zijn de volledige beschrijvingen van de twee casestudies opgenomen, die in het kader van dit rekenkameronderzoek zijn uitgevoerd. Die betreffen de aspecten op informatieveiligheid in het proces van de aanvraag van een Wmo-voorziening en een omgevingsvergunning. De casestudies zijn in een korter bestek en in een apart kader na de hoofdstukken 4 en 5 opgenomen. In bijlage 3 worden de meest gebruikte termen en afkortingen uitgelegd die voorkomen op het gebied van informatiebeveiliging en privacy. In bijlage 4 is de lijst opgenomen met geraadpleegde stukken en de lijst met functies van de respondenten. Bijlage 5 bevat een tabel over volwassenheidsniveaus die in hoofdstuk 5 aan bod komen.

---

1 Het dark web is de diepste en verborgen laag van het internet. Het is onderdeel van het ‘deep web’, omdat het niet toegankelijk is via reguliere zoekmachines. Het staat bekend als een plek waar illegale activiteiten plaatsvinden. Hoewel dit inderdaad gebeurt, bestaat het uit meer dan alleen illegale sites.

2 Ransomware is malware (software met kwaadaardige bedoelingen) die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld.

2 Onderzoeksvragen, visie en aanpak

2.1 Onderzoeksvragen

De centrale onderzoeksvraag is: Hoe is het gesteld met de informatie-veiligheid van de gemeente Zwolle, wat zijn de zwakke plekken en hoe kunnen deze worden verholpen?

De centrale onderzoeksvraag is uitgewerkt naar deelvragen op de drie terreinen, bekend van informatieveiligheid: organisatie-mens-techniek. Tevens wordt de rol van de gemeenteraad geadresseerd, omdat de rekenkamer het onderzoek uitvoert met als doel de raad in zijn kaderstellende en controlerende rol te ondersteunen. De deelvragen, met de bijbehorende normen zijn opgenomen in bijlage 1.

Daar waar sprake is van relevante samenwerking op informatieveiligheid in Shared Service centra ONS (SSC ONS) verband betreffen de onderzoeksvragen ook het SSC ONS.

De hoofdstukken 4 tot en met 7 bevatten de antwoorden op de onderzoeksvragen. Hieronder gaan we kort in op informatiebeveiliging en gegevensbescherming (gezamenlijk ook aangeduid als informatieveiligheid).

2.2 Korte inleiding op informatiebeveiliging en privacy

In de onderstaande afbeelding wordt, binnen informatieveiligheid, de samenhang tussen enerzijds informatiebeveiliging en anderzijds privacy (of gegevensbescherming) weergegeven.

Gegevensbescherming

Privacy oftewel gegevensbescherming of betreft de regels voor de verwerking van persoonsgegevens door bedrijven, instellingen en overheden. Doel is de privacy van burgers op een adequate manier te beschermen. De Europese General Data Protection Regulation (GDPR), in Nederland bekend als de Algemene Verordening Gegevensbescherming (AVG), is sinds mei 2018 van kracht. Europese Verordeningen zijn rechtstreeks van toepassing in EU lidstaten en hoeven niet omgezet te worden in de nationale wetgeving.

Informatieveiligheid

De AVG schrijft onder andere voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeenten zelf. De twee onderwerpen informatiebeveiliging en gegevensbescherming (privacy) hebben dus onderling een grote overlap. Een deel van de protocollen en procedures op beide terreinen komen met elkaar overeen. Overkoepelend wordt vaak de term informatieveiligheid gebruikt, zie onderstaand afbeelding 2.1.

Afbeelding 2.1. Informatieveiligheid met privacy en informatiebeveiliging.

Bron: Rekenkamer Utrecht, 2021.

Informatiebeveiliging

Informatiebeveiliging gaat over de maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de informatie binnen een organisatie garanderen.[3] Doel is de continuïteit van de informatie en de informatievoorziening of dienstverlening te waarborgen en eventuele gevolgen van (beveiligings)incidenten te beperken. Het beleid dat overheden, inclusief gemeenten, hierop hebben afgesproken is neergelegd in de Baseline Informatiebeveiliging Overheid (BIO).[4] De BIO bevat maatregelen die gemeenten op basis van een risicoanalyse kunnen nemen om aan het basisniveau voor informatiebeveiliging te voldoen.

Door de toenemende internationale geopolitieke cyberdreiging zijn strengere beveiligingseisen binnen Europa gaan gelden. De Network and Information Security Directive 2 (NIS2) is Europese regelgeving, die een zorgplicht op informatiebeveiliging oplegt aan overheden. NIS2 is een Europese richtlijn die omgezet moet worden in de nationale wetgeving. De Nederlandse overheid geeft invulling daaraan door onder andere de richtlijnen van de BIO vanaf oktober 2024 verplicht te stellen voor overheidsorganisaties, dus ook voor gemeenten. Naar verwachting treden in dat kader de Cyberbeveiligingswet (Cbw) in oktober 2025 in werking.

Alle overheden zijn eind 2023 door het Ministerie aangewezen als essentiële entiteiten voor de (digitale) veiligheid van Nederland. Dit betekent dat gemeenten aantoonbaar moeten voldoen aan de nieuwe Cyberbeveiligingswet.

---

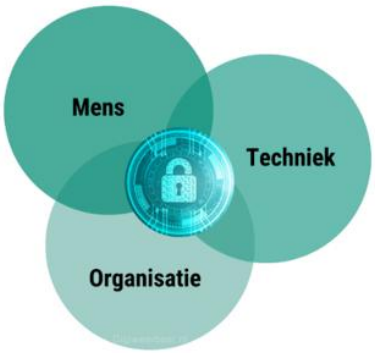
3 Volledig geformuleerd: Informatiebeveiliging gaat over het geheel aan preventieve, detectieve (opsporings-) en correctieve maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de informatie binnen een organisatie garanderen.

4 Gemeenten hebben in 2013 in VNG-verband afgesproken te voldoen aan de maatregelen van de Baseline Informatie-beveiliging Gemeenten (BIG). De BIG is vanaf 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De baseline is gebaseerd op de kwaliteitsnormen NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017.

In dit onderzoek worden beide onderwerpen, informatiebeveiliging en privacy, geadresseerd.

Mens, techniek, organisatie

Informatieveiligheid wordt vaak nog enkel vanuit een technische invalshoek benaderd. De ervaring leert evenwel dat technische oplossingen te organiseren zijn, hoewel deze natuurlijk ook in de praktijk moeten werken ("the proof of the pudding is in the eating"). Naast techniek zijn mens en organisatie essentieel bij informatiebeveiliging en privacy. Cruciale factoren die de informatieveiligheid bepalen zijn houding en gedrag van de menselijke actor, kortom bewustwording op risico's bij medewerkers en lijnmanagement. Ook moeten de organisatorische randvoorwaarden gecreëerd zijn om techniek en mens te ondersteunen. Beleid en protocollen moeten daarvoor opgesteld en vastgesteld zijn en in de praktijk worden toegepast. Om dat optimaal te laten slagen moet beleid op informatiebeveiliging en privacy gedragen en uitgedragen worden door bestuur en directie van de gemeente.



2.3 Aanpak

Methoden

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch, interviewverslagen en testen. De documenten bevatten beleid en rapportages van de gemeente. De documenten die zijn bestudeerd zijn in bijlage 3 opgenomen, evenals de functies van de bestuurders en functionarissen van de gemeente Zwolle die zijn geïnterviewd. De deskresearch vond plaats in de periode november-december 2024. De interviews zijn in februari 2025 afgenomen.

Pentesten

In december 2024 – februari 2025 zijn in het kader van het rekenkameronderzoek verschillende pentesten uitgevoerd op de systemen.[5] Door SSC ONS zijn eerder pentesten uitgevoerd op de systemen. De resultaten van deze test zijn gedeeld met de rekenkamer en besloten is deze niet in het kader van rekenkameronderzoek nogmaals uit te voeren.

In een vroeg stadium is door de rekenkamer en de onderzoeker overleg gevoerd met ambtenaren over de scope van de testen in het kader van het rekenkameronderzoek. Besloten is een wifi netwerk test, een Active Directory (AD) audit en een inlooptest met mystery guests uit te voeren. Daartoe is besloten, deels omdat deze testen nog niet of lang geleden zijn uitgevoerd, deels omdat deze een goed beeld geven van de veiligheid van de systemen. Voor een nadere uitleg van deze testen en de resultaten zie §8.1.

Ook zijn in het kader van het rekenkameronderzoek phishing mails verstuurd naar een steekproef van medewerkers en bestuurders van de

[5] Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt kunnen worden om in deze systemen in te breken.

gemeente, inclusief raadsleden.[6] Voor een uitleg van deze test en de resultaten zie §5.1.

De nota van bevindingen is op … mei 2025 voor de ambtelijke hoor en wederhoor (feitencheck) aangeboden. Het definitieve rapport is op … voor de bestuurlijke hoor en wederhoor aan het College van B&W aangeboden.

[6] Phishing is een vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens.

3 Organisatie

Onderzoeksvragen 1-4

In dit hoofdstuk gaan we in op de bevindingen met betrekking tot de onderzoeksvragen 1 t/m 4, de factor beleid. De normen die hiervoor gelden zijn als volgt beoordeeld, zie tabel 4.1. Hierbij wordt onder andere nagegaan of het beleid risicogebaseerd is en op strategisch, tactisch en operationeel niveau actueel is om informatieveiligheid en gegevensbescherming te borgen. En of de functionarissen op deze terreinen adequaat gepositioneerd en geëquipeerd zijn.

Tabel 4.1. Onderzoeksvragen 1 - 4, normen en beoordeling.[7]

Onderzoeksvragen	Normen	Oordeel
1: Wat is het beleid van de gemeente Zwolle op het gebied van informatieveiligheid en voldoet dit aan de actuele standaarden?	De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat op onderdelen is uitgewerkt in specifieke procedures en/of richtlijnen. De inhoud van het informatiebeveiligingsbeleid sluit aan op good practices, zoals de BIO2 en andere relevante wet- en regelgeving (zoals de AVG).	Voldoet deels
	De gemeente beschikt over een actueel informatie-beveiligingsplan met concrete activiteiten om nader invulling te geven aan diverse onderdelen van het informatiebeveiligingsbeleid. Op basis van de activiteiten is er een urenraming en budget opgesteld.	Voldoet deels
	De gemeente besteedt 10% van het ICT-budget aan maatregelen ter bevordering van informatieveiligheid.	Onbekend
2: Hoe gaat Zwolle om met risico's en incidenten op het gebied van informatieveiligheid?	Er worden met voldoende frequentie GAP- en risicoanalyses uitgevoerd. In de analyses zijn de belangrijkste risico's geïdentificeerd en worden verbetermaatregelen getroffen op de risico's die niet geaccepteerd worden.	Voldoet
3: Zijn de functionarissen op informatiebeveiliging en gegevensbescherming met betrekking tot hun taak juist gepositioneerd?	Taken en verantwoordelijkheden rond informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens zijn duidelijk belegd in de organisatie.	Voldoet
	De functionarissen op informatiebeveiliging zijn goed gepositioneerd om hun rol te kunnen vervullen.	Voldoet deels
4: Hoe wordt dit beleid uitgevoerd op strategisch, tactisch en operationeel niveau?	Het beleid zoals vastgesteld op strategisch niveau wordt op tactisch niveau ingevuld met de benodigde protocollen en op operationeel niveau uitgewerkt in richtlijnen en werkwijzen	Voldoet deels
	Het beleid wordt op strategisch, tactisch en operationeel uitgevoerd zoals is vastgelegd	Voldoet deels
	Het normenkader van de BIO2 en de doelstellingen van de gemeente op informatieveiligheid worden gerealiseerd	Voldoet deels

3.1 Strategisch beleid

Het informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te

[7] De onderzoeksvragen en de normen waarop beoordeeld wordt zijn in de tabel opgenomen, zie voor alle normen onderzoeksvragen en normen bijlage 2. De beoordeling varieert van: voldoet = voldoet volledig aan de gestelde norm; voldoet deels = voldoet niet geheel aan de norm; voldoet niet = voldoet geheel niet aan de norm; onbekend = niet na te gaan.

waarborgen, waarmee de gemeente voldoet aan relevante wet- en regelgeving en zodat de dienstverleningsambities en bedrijfsvoering worden gefaciliteerd.

Strategisch beleid

Er is een algemeen privacybeleid en een strategisch informatieveiligheids-beleid 2022-2026 vastgesteld door het college. Maar door de nieuwe Europese cybersecurity-wetgeving (zie §4.2) wordt dit jaar al een nieuw beleid opgesteld. In het strategische informatieveiligheidsbeleid zijn de ambities van de gemeente opgenomen en de rollen en verantwoordelijkheden beschreven. “Het is de ambitie om als gemeente Zwolle in de informatiemaatschappij een volwaardige en betrouwbare plek in te nemen, nu en in de toekomst. Om de ambitie te kunnen realiseren zorgen we er voor dat de ambtelijke organisatie op zijn taken is toegerust: de basis is en blijft op orde. Dit betekent dat medewerkers op hun taken zijn toegerust, bijbehorende risico’s onderkennen en de processen, gegevens en systemen op orde zijn.” De gemeente Zwolle wil deze ambitie uitstralen naar burgers, bedrijven en ketenpartners. De verschillende strategische doelen zijn als volgt geformuleerd:

- Het managen van de informatiebeveiliging.
- Het minimaliseren van risico’s van menselijk gedrag.
- Het garanderen van betrouwbare en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op en afhandelen van incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

De gemeenteraad is opgenomen als partij die geïnformeerd wordt, maar heeft geen rol als adviseur/controleur toebedeeld gekregen.

Governance

De directie en het bestuur van de gemeente worden door respondenten ervaren als doordrongen van het belang van informatieveiligheid en gegevensbescherming. Wat betreft bestuurders zijn twee portefeuille-houders van belang. Een op de Digitale transitie (Smart City) en privacy (AVG) en een op bedrijfsvoering en ICT. De burgemeester is betrokken, onder andere vanuit de landelijke rol als voorzitter VNG-commissie Informatiesamenleving, verantwoordelijk voor de totstandkoming van de Digitale Agenda 2024-2028, de en veiligheidsregio IJsselland.

Continuïteitsplan ICT Zwolle 2022

Vanaf 2022 heeft de gemeente Zwolle een continuïteitsplan ICT. Doel is om om langdurige stagnatie van kritische bedrijfsprocessen van de gemeente te voorkomen. Daarvoor is een proces voor continuïteitsbeheer ingericht. Om de noodzakelijke stappen zo effectief en efficiënt mogelijk te nemen na het optreden van een calamiteit is volgens het continuïteitsplan oefening noodzakelijk. Het SSC ONS heeft in 2024 een eigen Crisisplan opgezet.

SSC ONS

De IT is uitbesteed aan de gemeenschappelijke regeling van het Shared Service Centre ONS (SSC ONS), daarin werkt de gemeente Zwolle op een aantal uitvoeringstaken samen met de provincie Overijssel en de gemeenten Kampen, Dalfsen, Westerveld, Zwartewaterland en Ommen. Het informatieveiligheidsbeleid is onderling met de partners afgestemd, de

gemeente Zwolle loopt daarbij wat betreft timing iets voor. SSC ONS wil zoveel mogelijk afspraken uniformeren om de maximale potentie van de ‘economies of scale’ te benutten.

Datagedreven werken

In 2021 is door de gemeente Zwolle het programma Datagedreven werken (DGW) opgezet om het gebruik van data en het ontwikkelen van datagedreven oplossingen binnen de gemeente te stimuleren. In oktober 2023 is een DGW werkgroep samengesteld, bestaande uit medewerkers uit de organisatie én de afdeling Informatievoorziening (IV) onder begeleiding van een externe partij. In 2024 zijn Datateams in de organisatie goedgekeurd.

In het kader van eigenaarschap van DGW en de constatering dat de gemeente Zwolle verantwoordelijk is voor de juiste inwinning en gebruik van gegevens worden als uitgangspunten onder andere vastgesteld:

- Alle medewerkers zijn verantwoordelijk voor het uitvoeren van beleid rond privacy, veiligheid en ethiek.
- Eigenaarschap van de data ligt op operationeel niveau in de organisatie.

Hiervoor zouden de medewerkers in de lijn ondersteund moeten worden door ‘ambassadeurs’ op informatiebeveiliging en privacy. Die ‘functionarissen’ zijn niet dekkend over alle afdelingen gerealiseerd. In de plaats daarvan wordt gewerkt met contactpersonen, die de relatie tussen enerzijds de afdeling en anderzijds CISO, FG en Privacy en Information Security Officers (PISO) onderhouden.

3.2 Tactisch en operationeel

Tactisch niveau privacy

Op privacygebied zijn de protocollen er zoals de AVG die heeft voor-geschreven. Dat zijn onder andere voorschriften voor de inzageverzoeken, die via DigiD ingediend kunnen worden. Het melden van datalekken, zodat medewerkers weten waar ze datalekken kunnen melden en dat er gestructureerd opvolging aan wordt gegeven. En er is een verwerkingsregister met de informatie over de persoonsgegevens die de gemeente verwerkt, of die namens de gemeente worden verwerkt. Uit de interviews blijkt dat het register nog geen volledige dekking heeft. Uit het verslag van de FG blijkt dat op het aantal data protection impact assessments (dpia), bedoeld om de risico’s bij verwerkingsprocessen in kaart te brengen een inhaalslag gemaakt moet worden. Daardoor zijn niet alle risico’s met betrekking tot de verwerking van persoonsgegevens bekend.

Wet politiegegevens (WPG)

Gemeente Zwolle is werkgever van buitengewone opsporingsambtenaren (boa’s) die in het kader van hun opsporingstaak persoonsgegevens verwerken. Sinds 2019 moeten gemeenten in het kader van de Wet politiegegevens (WPG) periodiek audits laten uitvoeren op deze verwerking en daarover rapporteren aan de Autoriteit Persoonsgegevens (AP). Op basis daarvan constateerde de FG over 2023 significante vooruitgang.

Tactisch niveau Informatiebeveiliging

Op gebied van informatiebeveiliging is de laatste jaren, mede in overleg met SSC ONS, een inhaalslag gepleegd om de beleidsstukken, protocollen en richtlijnen op tactisch niveau op orde te brengen. Dat zijn onder andere beheersmaatregelen in het kader van wachtwoordenbeleid, authenticatie,

incidentafhandeling enzovoort. In totaal kent de BIO2 203 van dergelijke maatregelen, geclusterd in thema's.

In 2021 bleek de BIO-compliance, met 19%, onder de maat. De accountant adviseerde in 2023 een inhaalslag op BIO-maatregelen, en voorzag de noodzaak van een meerjarenplan daartoe. Om BIO-compliant te worden is de afgelopen jaren samen met SSC ONS en de partners onder andere het project Verhoging Digitale Weerbaarheid (VDW) opgezet. Het programma VDW bestond uit 35 hoofdzakelijk technische beheersmaatregelen en activiteiten, zoals Monitoring and Response applicaties (SIEM/SOC), Identity and Access Management (IAM, zie hierna), kwetsbaarheidsmetingen en -management, uitwijk- en hersteltesten, veilig mailen en veilig grote bestanden uitwisselen, oefenen met cybercrime scenario's enzovoort.

Medio 2024 is bij SSC ONS en de partners een scan uitgevoerd om inzichtelijk te krijgen in hoeverre zij op tactisch niveau voldoen aan de BIO2. Geen enkele partner, ook SSC ONS niet, bleek volledig te voldoen. Uit de NIS2 scan blijkt dat Zwolle nog stappen heeft te zetten op: governance (beleidsafspraken), beleid, beveiliging toeleveringsketen, cyberhygiëne en opleiding, cryptografie en encryptie en rapportageverplichtingen. Volledig dekkend conform de eisen van de BIO2 is het geheel aan protocollen en richtlijnen in 2025 nog niet. De verwachting, volgens enkele geïnterviewden, is dat het nog 1-2 jaar duurt voordat de gemeente Zwolle voor 90% BIO-compliant is.

Operationeel niveau

Op operationeel niveau gaat het om werkprocessen waarin informatie-beveiligingsaspecten zijn verwerkt. De risico's op informatieveiligheid zijn in kaart gebracht in het kader van het jaarplan van de Internal audit, CISO en FG. Deze functionarissen vormen de zogenoemde derde lijn die onafhankelijk toezicht houdt en adviseert over de naleving van de gestelde doelen. Zo zijn in het jaarplan 2024 significante risico's gesignaleerd op een viertal processen. Daarnaast zijn er 17 processen met een verhoogd risico. Vanuit de tweede lijn worden op basis van deze risicoanalyses de activiteiten opgepakt om de proceseigenaren lijn te ondersteunen bij het compliant maken van de operationele processen. Daar is volgens respondenten nog veel werk in te verzetten, samen met de proceseigenaren in de lijn.

De rapportage van de FG ziet toe op opzet, bestaan én werking van het privacybeleid. Medio 2024 constateert de FG over 2023 dat de AVG-processen nog onvoldoende worden nageleefd als het gaat over beheersing van risico's van gegevensverwerking in de keten waar de gemeente mee samenwerkt. Op gebied van beleid, processen, organisatorische inbedding, rechten van betrokkenen, onderdelen van gegevensbescherming en verantwoording is volgens de rapportage van de FG nog vooruitgang te boeken. Dat betekent dat de werking van het privacybeleid nog niet optimaal is en de gemeente risico's loopt.

Werking van het beleid

De gemeente bevindt zich momenteel in een transitiefase wat betreft informatiebeveiliging en privacy. Hoewel er een basis aan beleid en systemen aanwezig is, kan geconstateerd worden dat er nog aanzienlijke verbeteringen nodig zijn om te voldoen aan wettelijke verplichtingen en best practices. De ervaring bij andere gemeenten is dat het niet alleen afhangt van opzet en bestaan van beleid, maar ook de werking ervan.

Hieronder gaan we in op enkele beleidsonderdelen op tactisch en operationeel niveau die aandacht behoeven. Dat zijn achtereenvolgens het Identity and Access Management (IAM) dat de toegang van medewerkers tot systemen en gegevens regelt, het leveranciersmanagement dat de risico's op informatieveiligheid in de ketens waarmee de gemeente samenwerkt regelt en het informatiemanagement systeem op informatiebeveiliging (ISMS).

Identity and Access Management (IAM)

Een kritiek proces is het instroom, doorstroom- en uitstroomproces (IDU) voor medewerkers. Het gaat daarbij om het toekennen en ontnemen van rechten van medewerkers wanneer zij de organisatie binnenkomen, doorstromen naar een andere functie of de organisatie verlaten. Dat kan geregeld worden in een zogenoemd Identity Access Management (IAM), waarmee SSC ONS bezig ie te implementeren. De gemeente haakt daarop aan met het IDU-proces en heeft een stuurgroep IDU opgezet. De rapportage lag begin 2025 bij de afdeling HR. Relatief voordeel is dat er een nieuw financieel systeem geïmplementeerd wordt, zodat de systemen sowieso opnieuw ingericht moesten worden.

Via IAM worden toegangsrechten (autorisaties) tot systemen en informatie binnen die systemen niet meer aan personen toegekend, maar aan specifieke rollen die medewerkers in een bepaalde functie vervullen. Bij instroom van medewerkers gaat het toekennen van autorisaties meestal goed, want de (nieuwe) medewerker moet aan de slag kunnen en heeft systemen, programma's en gegevens nodig. Bij doorstroom blijven autorisaties soms nog een tijd doorlopen, terwijl de medewerker de rechten niet meer zou mogen hebben. Daarover zijn afspraken om de autorisaties periodiek door de leidinggevende te laten controleren. De frequentie waarop dat gebeurt verschilt per afdeling, van 2 tot 4 keer per jaar, zo blijkt uit de interviews en de casebeschrijvingen.

Het IAM is nog niet volledig geïmplementeerd. Uit de interviews blijkt dat de verwachting is dat dat nog 2 jaar kan duren.

Leveranciersmanagement

De gemeente wil werken met betrouwbare partners. Nieuwe contracten die afgesloten worden voldoen aan de standaarden op het gebied van informatieveiligheid en privacy. Zo is er een kwaliteitsboard ingericht die wijzigingen en nieuwe aankopen toetst en adviseert. Sommige langlopende contracten, die niet recent zijn herzien, kunnen risicovol zijn. Controle op de afspraken rond gegevensverwerking en informatiebeveiliging zijn cruciaal bij leveranciers en samenwerkingspartners. Dat kan geregeld worden via verwerkingsovereenkomsten of zogenoemde Third Party Memoranda (TPM).

SSC ONS bedient op een aantal bedrijfsvoeringdomeinen (inkoop- en contractmanagement, IT en HR) als gemeenschappelijke regeling de provincie Overijssel en de gemeenten Zwolle, Kampen, Dalfsen, Westerveld, Zwartewaterland en Ommen. Op twee punten van deze ketensamenwerking raakt leveranciersmanagement de relatie van de gemeente met het SSC. Een betreft de inkoop van de gemeente van diensten van het SSC en de andere is de inkoop van software en diensten door het SSC. Op dit laatste is het volgens respondenten lastig voor de gemeente om een goed overzicht te krijgen. Vooral vanwege de versnippering van taken, deels in eigen huis en deels uitbesteed aan SSC ONS.

Wat betreft de inkoop van IT-diensten bij SSC ligt het functioneel applicatiebeheer bij de partners en wordt het technisch beheer bij SSC ONS ingekocht. De dienstverlening is beschreven in een product- en dienstcatalogus en Service Level Agreement (SLA). Specifiek op HR is een ISAE3402 verklaring aanwezig. Onder de dienstverleningsovereenkomst (DVO) met afspraken met het SSC ONS ligt geen TPM of gelijkwaardig document. Terwijl SSC ONS, naast samenwerkingspartner een van de meest cruciale leveranciers is. De accountant merkte eind 2023 op: "Er vindt momenteel nog geen verantwoording plaats over de kwaliteit en effectiviteit van de IT-beheersmaatregelen die door SSC ONS uitgevoerd worden. Hierdoor is niet vast te stellen waar de gemeente momenteel risico's loopt op cybercriminaliteit."[8]

Information Security Management System (ISMS)

Onder andere door de FG, CISO en accountant wordt geconstateerd dat het concreet vastleggen en verantwoording van activiteiten op informatiebeveiliging en privacy nog kan verbeteren. Tegelijk wordt geconstateerd dat er in de praktijk meer gebeurt dan waarover verantwoording wordt afgelegd. Er is tooling aanwezig om de lijn, die integraal verantwoordelijk is voor deze processen, daarin te ondersteunen. Dat is het zogenoemde Information Security Management System (ISMS). Dat wordt momenteel voornamelijk standalone gebruikt voor ENSIA (Eenduidige Normatiek Single Information Audit). Er wordt nog weinig input gegeven via het ISMS om te kunnen verantwoorden. Een cruciale tekortkoming daardoor is het ontbreken van een volledige Plan-Do-Check-Act beleidscyclus (PDCA-cyclus). Het streven is om dit risicogestuurd te maken en te integreren in een breder kwaliteitsmanagementsysteem. Dit duidt op een nog onvoldoende gestructureerde aanpak van informatiebeveiliging en gegevensbescherming.

NIS2

Ter voorbereiding op NIS2 en de nationale cybersecuritywetgeving waarin NIS2 geïmplementeerd wordt heeft de CISO in 2024 een uitvoeringsplan geschreven. Daarin worden verbindingen gelegd van integraal risicomanagement naar het kwaliteitsmanagementsysteem en de implementatie van de BIO2 en de NIS2-richtlijn. Daaronder ligt risicomanagement en de bedoeling is dat meer integraal op te pakken, breder dan alleen informatieveiligheid. Daarnaast zijn er nog processen die ingericht moeten worden, zoals de nieuwe zorgplicht [9] en de meldplicht.

---

8 De accountant adviseert dan ook in de managementletter van 2023 aan: “Wij adviseren het college om een evaluatie uit te voeren op de kwaliteit van dienstverlening en kwaliteit van interne beheersing van de diensten die door de serviceorganisatie worden uitgevoerd. Vervolgens adviseren wij uw college een plan van aanpak op te stellen om de huidige uitbestede taken en de interne beheersing op een voldoende niveau te brengen.”

9 De 10 zorgplichtmaatregelen: 1. Een risicoanalyse en beveiliging van informatiesystemen; 2. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets; 3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen; 4. Incidentenbehandeling; 5. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging; 6. Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden; 7. Beveiliging van de toeleverancierskеten; 8. Beleid en procedures over het gebruik van cryptografie en encryptie; 9. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen; 10. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico’s te beoordelen.

3.3 Functies

De organisatie gaat in het strategisch beleid uit van de zogenoemde ‘3 lines of defence’. Schematisch ziet zo’n model er als volgt uit:

Schema 4.1 Three lines of defence.

In de (eerste) lijn zijn de medewerkers en management als de proceseigenaren verantwoordelijk voor de uitvoering van het informatiebeveiligings- en privacybeleid. In de tweede lijn is de ondersteuning van de eerste lijn voor deze processen. Voor privacy en informatiebeveiliging zijn dat de ‘privacy en information security officers’. In de derde lijn is de onafhankelijke advies en controle gepositioneerd, gevormd door de Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG).

FG en CISO

De FG is fulltime aangesteld onder HR-verantwoordelijkheid van Juridische Zaken. Hij is verantwoordelijk voor het toezicht op de naleving van de regelingen en beleid ten aanzien van de bescherming van persoons-gegevens. Aangewezen voor de medewerkers, college, burgemeester en afzonderlijk voor de gemeenteraad. De CISO is voor 50% van de tijd CISO en de andere 50% heeft hij strategische digitale veiligheid in de portefeuille. Hij valt onder de afdeling Informatievoorziening (IV) met een algemene functieomschrijving, breder dan de CISO-functie sec.

In principe moeten beide functies, gelet op de strategische rol die zij hebben, een directe lijn met de directie en bestuurlijk verantwoordelijke hebben. De reden dat de CISO in de lijn aanwezig is, is omdat een functie HR-technisch onder een afdeling moeten vallen. De CISO zou vanuit zijn functie een directe lijn met de directie en bestuur moeten hebben. CISO en FG geven aan die link sporadisch en niet structureel in te vullen.

ISO’s

Voor de doorvertaling van strategisch beleid naar tactisch en operationeel beleid zijn Information Security Officers aangesteld. Begin 2025 zijn drie ISO’s op een gecombineerd taakveld van informatiebeveiliging en privacy actief. Vandaar dat ze Privacy and Information Security Officers worden genoemd. De bedoeling is nog in 2025 een vierde zogenoemde PISO te werven. Het zijn gecombineerde functies, maar elk heeft een preferente taak op informatiebeveiliging of privacy.

Zij vallen onder de afdeling IV, waar sinds de reorganisatie een aparte sectie voor informatiebeheer en kwaliteit in opgezet. De achterstand in BIO-compliance, zie hiervoor, lijkt vooral het resultaat van een tekort aan bemensing om activiteiten op te pakken en de lijn te ondersteunen. Met binnenkort 4 ISO’s gecombineerd op informatiebeveiliging en privacy laat de gemeente zien de ambitie te hebben de achterstand snel in te willen lopen.

Internal Audit (IA)

Team Internal Audit is onder andere toetst de interne beheersing van risicovolle processen. De interne audit trekt samen met de CISO en FG als controleur en adviseur uit de derde lijn op. Zij faciliteren bij de taken die voortkomen uit de IT audit van de accountant. Dat kan op aspecten van

informatiebeveiliging en privacy met betrekking tot leveranciers-management of sociaal domein zijn, als ook voor de interne beheersing van het financiële proces. Respondenten signaleren dat het risicomanagement nog hoofdzakelijk financieel van aard is en dat er nog winst op een brede en integrale aanpak te behalen is, met een verwijzing naar informatiebeveiliging en privacy.

Gezamenlijk jaarplan

Medio 2022 is gestart met het versterken van de samenwerking tussen de derdelijnsfuncties, namelijk Internal audit (IA), CISO en FG. In 2023 heeft dit geleid tot het eerste gezamenlijk jaarplan 3e lijn.

Crisisorganisatie

Er is ook sprake van een crisisorganisatie. Vanuit de driehoek wordt indien nodig de veiligheidsproblematiek opgeschaald. Door respondenten wordt aangegeven dat dit proces op veiligheid in het algemeen goed is geborgd. Zij geven tegelijk aan dat de onderwerpen informatieveiligheid en cybersecurity in die crisisstructuur nog beter meegenomen zouden kunnen worden. In de planning staat nog een opdracht om vanuit Zwolle een strategisch crisisplan op te stellen, met bedrijfscontinuïteit als onderwerp. Vanuit SSC ONS is zo'n crisisplan in 2024 opgesteld.

3.4 Overleggen en rapportages

Informatiebeveiliging en privacy komen in een aantal interne en externe overleggen ter sprake.

Intern overleg

Er is een werkgroep Informatiebeveiliging die tot doel heeft de gemeentebrede afstemming van activiteiten en beleid ten aanzien van informatiebeveiliging. Minimaal vier keer per jaar komt deze onder voorzitterschap van de CISO bijeen. Deelname door contactpersonen op informatiebeveiliging vanuit de afdelingen/teams Burgerzaken, Informatievoorziening, HR, IA, Inkoop, Privacy, Services, Suwinet en Website.

De functionarissen in de derde lijn (FG, CISO en IA) hebben elke 6-8 weken overleg, deels operationeel deels over planning en rapportages. CISO en FG komen ad hoc, maar met enige regelmaat, langs bij de portefeuillehouder of het gehele college om verslagen te bespreken of naar aanleiding van incidenten.

CISO en PISO's hebben een gezamenlijke dagstart. Er is intern overleg van de afdeling Informatievoorziening (IV) en er is een vast vierwekelijks overleg tussen FG, CISO en PISO's (privacy en informatiebeveiliging). Doel van dat laatste overleg is bespreken van de voortgang en afstemming op privacy en informatiebeveiliging en voorbereiden beleids- en rapportagestukken. Het hoofd van de afdeling Informatievoorziening (IV) heeft met de portefeuillehouder een strategisch overleg (SO). Daarin komen alle disciplines van Informatievoorziening langs, zoals informatiebeveiliging.

Het zogenoemde Kwaliteitsboard is aanwezig dat wordt gevormd door vertegenwoordigers van de verschillende aspecten van informatievoorziening: security, privacy, informatiemanagement, recordmanagement, service delivery, datakwaliteit, ethiek en architectuur. Het Kwaliteitsboard stemt de verschillende aspecten van informatievoorziening, strategische en tactische activiteiten op elkaar af en

toetst de verschillende plannen van de organisatie en haar (keten)partners/verbonden partijen op beleid, principes en wetgeving.

Informatiebeveiliging en privacy komen regelmatig ter sprake in managementbijeenkomsten, met de teamleiders, afdelingshoofden en directeuren. IA, FG en CISO bespreken de procesbevindingen uit de audits met de proceseigenaren in de lijn.

Extern overleg

Bij SSC ONS komt informatiebeveiliging langs bij het bestuurlijk overleg, waar de portefeuillehouder bij aanwezig is. Er is bij ONS ook een partneroverleg security met de CISO's van de deelnemende partners. Daarnaast is er een tactisch overleg informatiebeveiliging en privacy, onder andere over afstemming van het tactisch beleid, zoals logbeleid of dataklassificatiebeleid. Specifiek op bedrijfsvoering is er bij SSC ONS een Bedrijfsvoeringsberaad (BVB) waarin ook informatieveiligheid als onderwerp wordt geagendeerd. In het BVB is onder andere de NIS2 scan van 2024 geagendeerd om een inzicht te krijgen in de weerbaarheidsstatus van de partners in het SSC (zie §4.2).

Extern neemt de CISO deel aan verschillende overleggen met CISO, in de Kring IJsselland en de VNG. En hij neemt deel aan het Expertteam Cyber Overijssel, cyberexperts van Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en Politie over cybercrime.

De FG heeft geen structureel overleg met SSC ONS, maar doet wel soms samen met SSC ONS een onderzoek op specifieke onderwerpen, zoals gegevensverwerking door applicaties. En de FG heeft een ad hoc overleg met Deventer en andere gemeenten en de provincie. Daarnaast heeft de FG periodiek sessies met de Informatie Beveiligingsdienst (IBD) en Vereniging Nederlandse Gemeenten (VNG). Zoals sessies in het kader van intervisie of over specifieke thema's, bijvoorbeeld de ontwikkeling van AVG-producten of kaders op privacy voor datawarehouse.

Crisisoverleg SSC

De CISO van Zwolle was de voorzitter van het partneroverleg security van SSC in het kader van het continuïteitsplan ICT. Vanuit die functie vervult hij de rol van verbindingspersoon in de richting van de strategische teams. Hij praat ze bij over de actuele stand van zaken met betrekking tot de oorzaak van een storing of de uitval van systemen en de mogelijke impact van de uitval op de gemeentelijke dienstverlening. Lastig, maar niet onoverkomelijk, is het dat de partners van SSC onder drie verschillende veiligheidsregio's vallen, nl. IJsselland, Drenthe en Twente. In 2023 heeft SSC ONS een crisisplan op ICT vastgesteld.

Rapportages

De FG en de CISO rapporteren halfjaarlijks aan de directie over de bevindingen op het gebied van informatiebeveiliging en privacy. Eenmaal per jaar rapporteren zij naar directie, college en de raad over de bevindingen. Daarnaast krijgt de raad de door het college vastgestelde ENSIA-rapportage. Deze gaat voornamelijk over de interne en externe audits die verplicht zijn in het kader van ENSIA. Zoals de interne audits op verschillende registraties, de Basisregistratie Personen (BRP), Reisdocumenten, Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO). En de externe audits op SUWInet en DigiD. Deze ENSIA-rapportage wordt, samen met de managementreactie in de directie en college geagendeerd, vergezeld van een oordeel over de mate van 'in

control' zijn. ENSIA is bedoeld voor de verticale verantwoording richting landelijke toezichthouders en voor de horizontale verantwoording richting de gemeenteraad.

ENSIA 2023 [10]

In 2024 is in het kader van ENSIA met de verantwoordingsinformatie over 2023 gemeld dat op enkele onderdelen van de BAG en BRO de score niet 100% is op datakwaliteit of proces/organisatie. Daarvoor zijn verbetermaatregelen voorgesteld en genomen, overigens niet met grote wijzigingen. Door de auditor is wel opgemerkt dat het vastleggen van de verbeteractiviteiten een aandachtspunt is. En dat betrokkenen, de proceseigenaren in de lijnorganisatie, continu hierop gewezen moeten worden.

Accountant

Tot slot rapporteert de accountant over een uitgevoerde IT audit, ondersteund door het team IA van de gemeente. In de managementletters worden bevindingen gedaan met betrekking tot cybersecurity in het kader van de interne beheersings-omgeving.[11] Veelal ligt de focus van de accountant op de financiële beheersingsmaatregelen, maar meer en meer nemen zij ook een breder perspectief op informatiebeveiliging en privacy mee in de bevindingen en adviezen.

Zo constateert de accountant eind 2023 dat rechtenbeheer, gebruikersbeheer en toegangsvereisten verbetering behoeven. Wat dezelfde aandachtspunten uit 2022 waren. De aanbeveling luidde om meer op actie in te zetten en minder op beleid. Dit is een bevinding en advies die in lijn is met bevindingen en adviezen uit andere audits.

De intentie is in de toekomst de gehele IT audit intern uit te voeren. Vanaf maart 2025 is een IT auditor in dienst van de gemeente Zwolle getreden. IA is bezig met de ontwikkeling van een geïntegreerde auditaanpak met aandacht voor IT, informatiebeveiliging en privacy bij de procesaudits die zij gaan uitvoeren.

3.5 Middelen

10%-norm, IBD

De respondenten vinden over het algemeen dat bestuur en directie van de gemeente doordrongen is van de noodzaak voldoende te investeren in informatieveiligheid. De Informatie Beveiligingsdienst (IBD) van de VNG hanteert de maatstaf van investering in informatieveiligheid van ca. 10% van de kosten van de organisatie voor ICT. Bij de 10% horen de kosten van personeel en middelen voor onder andere pentesten en (bewustzijns-) campagnes.

Het is lastig om te bepalen of er voldoende middelen en capaciteit zijn op gegevensbescherming bij de gemeente Zwolle. Enerzijds omdat de middelen verspreid over verschillende posten in de begroting aanwezig zijn. N Anderzijds is het lastig om de risico-bereidheid ('risk-appetite') goed in te schatten en wat daarvoor wat betreft capaciteit nodig is om daarop te handelen. Dat wil zeggen, de risico's zijn niet compleet inzichtelijk, onder andere vanwege ontbreken van een sluitende beheersingssystematiek zoals

[10] Op moment van deze rapportage was de ENSIA-rapportage over 2024 nog niet gereed.

[11] Uit de ambtelijke reactie blijkt dat de accountant vanaf dit jaar geen afzonderlijke managementletter uitbrengt, maar een boardletter. Het verschil is dat een managementletter vooral operationeel gericht is, terwijl de boardletter meer strategisch van aard is.

een ISMS, geen compleet verwerkingsregister en geen volledig dekkend beeld uit de dpia's. Op de risico's die gekend worden en besloten wordt deze weg te nemen kan capaciteit berekend worden. De risico's die niet gekend worden, worden impliciet geaccepteerd. Daarop kan ook geen capaciteit worden berekend.

Bij navraag bij SSC ONS geven de respondenten aan dat deze waarschijnlijk wel aan de norm voldoet. Heel hard is het bewijs dat de rekenkamer kreeg evenwel niet.

Casus Wmo

Korte casusbeschrijving: Informatiebeveiliging en privacy bij WMO-aanvragen [12]

In de gemeente worden WMO-aanvragen (Wet Maatschappelijke Ondersteuning) behandeld door vijf Sociale Wijkteams (SWT) die fungeren als schakel tussen inwoners en de gemeentelijke organisatie. Inwoners kunnen contact opnemen via inloopspreekuren, Klantcontactcentrum (KCC), website of worden doorverwezen door andere partijen zoals huisartsen. Bij het eerste contact worden persoonsgegevens geregistreerd in het systeem, waaronder contactgegevens, BSN, geboortedatum, gezinssituatie en een probleemomschrijving. Inwoners worden geïnformeerd over deze gegevensverwerking en het feit dat er een dossier wordt aangemaakt.

Voor de opslag en bescherming van gegevens gebruikt het SWT een SaaS-oplossing van Topicus met verschillende componenten voor dossiervorming, casemanagement en financiële afhandeling. De toegang tot deze gegevens is gereguleerd via een autorisatiestructuur: medewerkers hebben alleen toegang tot dossiers binnen hun eigen wijkteam, moeten voor toegang tot een specifiek dossier een reden opgeven, en de dossierhouder krijgt een melding wanneer iemand anders het dossier raadpleegt. Alle acties in het systeem worden gelogd, waarbij wordt vastgelegd wie welk dossier heeft bekeken, welke wijzigingen zijn aangebracht en wanneer de raadpleging heeft plaatsgevonden. Het management controleert steekproefsgewijs welke dossiers door medewerkers zijn geraadpleegd, die daarvoor geen reden hebben hoeven aangeven.

Gegevens worden intern besproken waarbij medewerkers dossiers toegewezen krijgen, intervisies met collega's en overleg met gedragswetenschappers hebben. Voor gevoelige casussen, zoals aanvragen van bekende inwoners, collega's of familieleden van medewerkers, geldt een speciaal protocol. Deze casussen kunnen worden doorverwezen naar een ander wijkteam of zelfs naar een andere gemeente om privacy en objectiviteit te waarborgen.

Bij het delen van gegevens met externe partijen worden de volgende principes gevolgd: doelbinding (alleen als noodzakelijk), minimale gegevensdeling (niet meer dan nodig), toestemming van de inwoner, en functionele omschrijvingen in plaats van medische diagnoses. Gegevens worden gedeeld met zorgaanbieders via beveiligd landelijk berichtenverkeer (uitgezonderd materiële WMO-voorzieningen), huisartsen, scholen (bij jeugdhulp), familieleden die als belangenbehartiger optreden en het CAK voor de eigen bijdrage.

Voor de communicatie gebruikt het SWT beveiligde e-mail via Zivver voor externe communicatie met professionals. Voor de zorgaanbieders is er het beveiligd berichtenverkeer via het Gemeentelijk Gegevensknooppunt (GGK), de WMO berichtendienst en e-mail. Reguliere post voor formele communicatie met inwoners en Microsoft Teams voor interne communicatie. In de praktijk wordt ook WhatsApp gebruikt voor laagdrempelig contact met inwoners, wat privacyrisico‘s met zich meebrengt.

Het SWT heeft verschillende maatregelen getroffen om privacy te waarborgen, waaronder een Data Protection Impact Assessment (dpia) in 2020, een register van gegevensverwerkingen, verwerkersovereenkomsten met leveranciers, een datalekprocedure en e-learning over informatieveiligheid. Ondanks deze maatregelen worden verschillende verbeterpunten erkend: reductie van datalekken, verbetering van beveiligde gegevensuitwisseling met inwoners, aansluiting van materiële WMO-voorzieningen op het berichtenverkeer, betere sturing op deelname van medewerkers aan e-learning, duidelijkere richtlijnen voor het gebruik van WhatsApp en betere bewustwording rond het registreren van medische gegevens.

Na de initiële opbouwfase van de wijkteams (vanaf 2015) is er nu meer ruimte voor doorontwikkeling van ondersteunende processen, waaronder informatieveiligheid. De gemeente werkt aan het updaten van de dpia’s en het verfijnen van het primaire proces, met specifieke aandacht voor informatieveiligheid en privacy.

[12] Voor de gehele casusbeschrijving zie bijlage 2.

4 Mens

In dit hoofdstuk gaan we in op de bevindingen met betrekking tot de onderzoeksvragen 5 en 6, de factor mens. De normen die hiervoor gelden zijn als volgt beoordeeld, zie tabel 5.1.

Tabel 5.1. Onderzoeksvragen 5 en 6, normen en beoordeling.[13]

Onderzoeksvragen	Normen	Oordeel
5: Op welke wijze wordt aandacht besteed aan de bevordering van bewustwording en eigenaarschap met betrekking tot risico's op het gebied van informatiebeveiliging bij bestuurders en medewerkers van de gemeente en bij raadsleden?	Informatieveiligheid en gegevensbescherming is een onderdeel van de 'onboarding' van medewerkers	Voldoet
	Medewerkers en bestuurders krijgen regelmatig scholing op de risico's op informatieveiligheid	Voldoet deels
	Raadsleden worden door de gemeente voorgelicht op de risico's op informatieveiligheid en gegevensbescherming en door de gemeente daarin gefaciliteerd	Voldoet deels
6: Zijn de rollen die medewerkers hebben t.a.v. informatiebeveiliging duidelijk voor de medewerkers? Hoe is de 'tone at the top' en hoe werkt dit door in de organisatie? Krijgen de risico's met betrekking tot informatiebeveiliging voldoende aandacht in alle organisatielagen?	Op bestuurlijk en directieniveau van de gemeente wordt informatiebeveiliging en gegevensbescherming regelmatig geadresseerd en bestuurders en directieleden dragen het belang van deze onderwerpen uit, onder andere door voorbeeldgedrag	Voldoet
	De medewerkers van de gemeente zijn op de hoogte van hun rol op informatieveiligheid en gegevensbescherming en gedragen zich daarnaar	Voldoet deels

Zoals in §3.2 reeds is geconstateerd wordt de mens vaak gezien als de zwakste schakel in informatieveiligheid. De systemen kunnen nog zo goed en veilig zijn ingericht, de mens is de bepalende factor bij het handelen conform het informatiebeveiligings- en privacybeleid. Alle respondenten beantwoorden de vraag 'Wat gaat er goed op het gebied van informatiebeveiliging en privacy' dat de afgelopen jaren het bewustzijn van de risico's bij het werken met (persoons)gegevens en informatie is toegenomen. Tegelijk wordt erbij gemeld dat het ook altijd nog beter kan. Daarom is de factor 'mens' op verschillende manieren in het onderzoek meegenomen, namelijk via een phishing mail, een mystery guest test, interview en casestudies.

SSC

Hiervoor is gemeld dat SSC ONS een crisisplan heeft opgesteld, op papier. In het strategisch crisisplan is vastgelegd wat ieders rol is en waarop iedereen

[13] De onderzoeksvragen en de normen waarop beoordeeld wordt zijn in de tabel opgenomen, zie voor alle normen onderzoeksvragen en normen bijlage 2. De beoordeling varieert van: voldoet = voldoet volledig aan de gestelde norm; voldoet deels = voldoet niet geheel aan de norm; voldoet niet = voldoet geheel niet aan de norm; onbekend = niet na te gaan.

elkaar kan aanspreken. Daarin is ook een kalender opgenomen voor 2 jaar opleiding, training, en oefenen voor de medewerkers van SSC. Er is ook een linking pin naar de partners, maar hoe de partners dat hebben georganiseerd is aan hen, daar gaat SSC niet over. Crux bij alle plannen op bewustzijn en toekomstig handelen is regelmatig blijven oefenen.

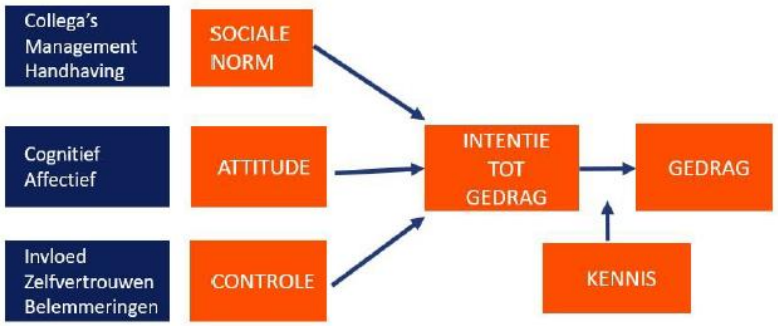
Medio 2023 is een oefening geweest samen met de partners van SSC met betrekking tot het crisisplan. Dat was een tabletop sessie [14] met een nog niet geheel afgerond plan. SSC ONS zelf heeft eind 2024 zonder partners geoefend met het crisisplan met zogenaamde walkthroughs, het doorlopen van een aantal casussen. Aandachtspunt is nog steeds wel dat het alleen nog maar op papier staat, zeker in relatie tot de partners.

Gemeente

Kortom, de gemeente is zelf aan zet. In 2022 is een 4-jarig bewustwordings-campagne op informatieveiligheid gestart, zoals afgesproken in het informatieveiligheidsbeleid. De ambitie was om het informatiebeveiligings-bewustzijn te verhogen, zodat door medewerkers van Gemeente Zwolle veilig wordt omgegaan met de persoons(gegevens) die ze wordt toevertrouwd en waarmee zij werken. In 2024 zijn een cultuurscan, leerplatform, communicatie en een managementsessie onderdeel van het bewustwordingsprogramma.

Volgens respondenten moet de campagne leiden tot het functioneel krijgen van eigenaarschap, verantwoordelijkheid en bewustwording in de lijn. Dat is een behoorlijke transformatie. Dat betekent een gedrags- en cultuurverandering die in beeld werd gebracht met onderstaand schema.

Schema 5.1. Bewustwordingscampagne



Doelen

Om bovenstaande doelen te bereiken moeten werknemers van de gemeente Zwolle uiteindelijk:

- Weten waar informatiebeveiligingsincidenten en datalekken gemeld moeten worden;
- Herkennen van informatiebeveiligingsincidenten en datalekken en deze ook melden;
- Medewerkers aanspreken op gedrag (bijvoorbeeld "vreemden" aanspreken, medewerkers aanspreken op het niet vergrendelen van de werkplek);
- Weten wanneer je een DPIA moet uitvoeren en wanneer je persoonsgegevens veilig moet mailen en dit ook doen.

[14] Bij een tabletop-oefening, letterlijk oefening op een tafelblad, wordt een crisissituatie nagebootst door een plattegrond en pionnen te gebruiken.

Doelgroepen

Daarbij werden de volgende doelgroepen onderscheiden: medewerkers die werken met de informatiesystemen; directie en afdelingshoofden; functioneel beheerders; ambassadeurs. Zoals eerder opgemerkt is de laatste doelgroep, de ambassadeurs, nooit gerealiseerd. Dat zijn de contactpersonen bij de afdelingen en teams geworden. Goed om op te merken dat raadsleden niet als doelgroep werden aangemerkt.

Media

Voor het bewustwordingsprogramma werd en wordt een combinatie van media ingezet: Intranet; de introductiemodule (de 'onboarding'); opleidingsprogramma met verschillende modules e-learning; een trainingsprogramma; een regelmatig te publiceren nieuwsflits; posters; op afdelings- en teamoverleg bespreken van incidenten; de inzet van een mystery guest, een phishingmail campagne en een pubquiz.

E-learning

De e-learning is niet verplicht, vanuit de directie is de verwachting dat het als vanzelfsprekend wordt beschouwd dat de doelgroepen de modules volgen. Er wordt wel bijgehouden wie aan de e-learning deelneemt, maar er wordt niet actief op gestuurd. Er worden bijvoorbeeld geen deelname-percentages per afdeling of team gepubliceerd, of ter sprake gebracht bij de team- of afdelingsoverleggen.

Naast informatie over richtlijnen en bewustzijn van risico's promoten moet volgens een aantal respondenten het eigenaarschap in de lijn aangewakkerd worden en de bewustwording vergroot worden welke informatie-beveiligingstaken bij de lijn thuishoren. Wanneer moet een risicoanalyse of een dpia of business impact assessment (bia) gehouden worden. Doel is de lijn bewust bekwaam te maken, onder andere weten wanneer informatie-beveiligings- en privacyaspecten bij beleid en werkprocessen betrokken moet worden. De dpia is bijvoorbeeld een middel om er bij medewerkers voor te zorgen dat het besef van het betrekken van deze aspecten zich ontwikkelt naar voldoende beheersen van de risico's. Dat betekent een volwassenheidsniveau dat proactief bezig is met de bescherming en verwerking van informatie.

Volwassenheid

In de bewustwordingscampagne wordt minimaal niveau 3 tot doel gesteld, zie bijlage 4 voor de verschillende niveaus van NOREA. Op basis van de interviews en de casestudies (zie hoofdstuk 8) is het volwassenheidsniveau gemeentebreed tussen 2 en 3. Het niveau kan per afdeling verschillen. Sommige afdelingen werken al jaren met richtlijnen en procedures op de verwerking van (bijzondere) persoonsgegevens en hebben de werkwijzen geïnternaliseerd. Voor medewerkers van andere afdelingen is het relatief nieuw en komen de richtlijnen en werkwijzen op informatiebeveiliging en privacy als extra erbij.

Digivaardig, leiderschap

In SSC ONS-verband is afgesproken te werken aan digitale vaardigheden en digitaal leiderschap. Dat is breder dan informatiebeveiliging en gaat onder andere over digitalisering, datagedreven werken en Artificiële Intelligentie (AI). Dat raakt zijdelings ook informatiebeveiliging.

4.1 Testen

In het kader van het rekenkameronderzoek zijn eind 2024 en begin 2025 testen uitgevoerd door ethische hackers. De testen die in dit hoofdstuk worden behandeld zijn de phishing mail en inlooptest met een mystery guest op het stadhuis en het stadskantoor.

Phishing mail

Tussen 10 en 17 december 2024 is een phishing mail campagne uitgezet onder een steekproef van medewerkers (interne en externe) en leden van het college en de gemeenteraad. Doel van de campagne is om het bewustzijn van medewerkers en bestuurders te testen met betrekking tot de methodes die cybercriminelen gebruiken om internetgebruikers te misleiden en gegevens te ontfutselen. De resultaten zijn in tabel 5.2 weergegeven.

Tabel 5.2. Resultaten phishingmail campagne

Aantal e-mails	Aantal klikkers	Klik-%	Aantal inloggers	Inlog-%	Inloggers tov klikkers-%
545	124	22,8%	61	11,2	49,2%

In totaal zijn 545 phishing mails met een 'gemiddelde moeilijkheidsgraad' verstuurd, met de vraag om het wachtwoord te wijzigen in verband met een beveiligingslek. 124 geadresseerden (23%) hebben op de link in de mail geklikt. Van degenen die op de link hebben geklikt heeft bijna de helft (49%) een wachtwoord achtergelaten. Als een hacker met malafide intenties de mail had verstuurd, was het via de gegevens van 61 medewerkers mogelijk geweest zich toegang te verschaffen tot de systemen.

Degenen die een wachtwoord hebben achtergelaten kregen op een landingspagina uitleg over de test. Ook kregen ze uitleg over hoe een phishing mail te herkennen. De wachtwoorden zijn overigens niet opgeslagen door de ethische hackers.

Uit de benchmark van dit soort campagnes, met een gemiddelde moeilijkheidsgraad, ligt de score van degenen die op de phishing mail klikken op circa 21%. De overall score van de medewerkers en bestuurders ligt daar iets boven. Enkele afdelingen scoren 33-35%, en één afdeling met 0%. Een derde van de wethouders en raadsleden hebben op de mail geklikt, maar van de raadsleden heeft niemand het wachtwoordgegevens achtergelaten.

Meldingen bij de helpdesk

Het aantal meldingen bij de helpdesk is een graadmeter voor de alertheid van medewerkers. In de ochtend dat de phishingmail is uitgezet is de helpdesk 29 keer benaderd met een melding, 5% van de uitgezette 545 phishingmails. De medewerkers is toen uitgelegd dat dat onderdeel van een bonafide test was. Onbekend is of medewerkers of bestuurders elkaar onderling hebben gewaarschuwd voor de phishing.

Inlooptest

Op 25-2-2025 is een mystery guest assessment uitgevoerd op de locaties van het stadhuis en stadskantoor van de gemeente. Dat is gedaan op basis van een greybox aanpak. [15] Tijdens de test is geprobeerd om onopvallend de panden binnen te komen en vanuit de publieke ruimte te testen of er toegang kon worden verkregen naar diverse niet-publieke ruimtes. Daarmee wordt de effectiviteit van de genomen beveiligingsmaatregelen geverifieerd.

Inlooptest stadskantoor

Op het stadskantoor is het gelukt om met personeel mee te lopen naar de niet-publieke ruimte zonder aangesproken te worden. Vanuit deze ruimte kon er vrij rondgelopen worden, ook weer zonder aangesproken te worden.

[15] Een whitebox test is een teststrategie waarbij de ethische hackers kennis hebben van de technische infrastructuur en systemen en met behulp van die kennis technische zwakheden trachten op te sporen. Dit in tegenstelling tot black- of greybox testen, waarbij de hackers vooraf respectievelijk geen of beperkte kennis hebben van de systemen of omstandigheden.

Na deze toegang was ook vrijwel het gehele pand bereikbaar vanuit de trappenhuizen zonder gebruik van een toegangspas. Wel maakte de open uitstraling van het pand, zoals veel glas en open kantoortuinen, het lastig voor de mystery guests zich ergens echt op hun gemak te voelen of zich ongezien te bewegen.

Verder zijn de mystery guests niet aangesproken op hun aanwezigheid. Er werd vriendelijk deuren opengehouden en vriendelijk gegroet wanneer we personen tegen kwamen. Het is niet gelukt om kritische of technische ruimtes te betreden. Er zijn regelmatig deuren gecontroleerd waarachter technische ruimtes verwacht werden, maar deze waren allemaal gesloten. Verder zijn tijdens het bezoek werkplekken gecontroleerd op onbeheerde badges, documenten of ontgrendelde computers. Er zijn hierbij twee werkplekken gevonden die niet waren vergrendeld. Archiefkasten waren veelal gesloten en stonden ook op centrale plekken waar sociaal toezicht was. Het clean desk beleid was ook goed toegepast.

Inlooptest stadhuis

Tijdens de test in het stadhuis is het gelukt om met personeel mee te lopen naar de niet-publieke ruimte zonder aangesproken te worden. Vanuit deze ruimte was het lastig om zich naar andere plaatsen in het pand te begeven. Er waren veel toegangsdeuren beveiligd met een paslezer, waardoor veel tailgaiting (meelopen met medewerkers naar niet-publieke ruimtes) is toegepast om naar volgende beveiligde zones te komen. Dit is echter niemand opgevallen, waardoor de mystery guests niet zijn aangesproken op opvallend gedrag of wat ze kwamen doen.

Verder zijn tijdens het bezoek werkplekken gecontroleerd op onbeheerde badges, documenten of ontgrendelde computers. Er is op deze locatie geen werkplek gevonden met een niet-vergrendelde werkplek. Opvallend was dat de mystery guests enkele keren toegang hadden tot deuren, waarbij een paslezer aanwezig was, maar deze niet gebruikt hoefde te worden. Toegang tot technische ruimtes is beperkt verkregen bij de technische ruimte voor de lucht/warmte voorziening op de 4e verdieping. Ook toegang tot kamers van wethouders, de raadzaal en andere zalen is zonder problemen verkregen en hier hebben de mysterie guests ook ruim de tijd gehad om zich onopvallend door deze ruimtes te bewegen.

Resultaat inlooptest

Van tevoren zijn acht (aanvals)doelen gedefinieerd. Daarvan hadden drie een hoge risicoclassificatie (impact), drie een gemiddelde en één een lage. Van de hoog impact doelen zijn twee niet behaald en een hoog impactdoel is beperkt behaald. De drie doelen met een gemiddeld impact en één met een lage impact op de veiligheidsrisico's zijn behaald. Op basis van de resultaten van het mystery guest assessment is het risico dat de gemeente Zwolle op de fysieke toegankelijkheid loopt ingeschat op 'gemiddeld'.[16]

[16] Bij de ambtelijke hoor en wederhoor zijn de rapporten van de pentesten overhandigd aan de gemeentesecretaris. Daarmee heeft de organisatie kennis kunnen nemen van de risico's en verbeterplannen kunnen opstellen om de risico's te mitigeren.

Casus Omgevingsvergunning

Korte casusbeschrijving: Informatiebeveiliging en privacy bij omgevingsvergunningen [17]

In gemeente Zwolle worden aanvragen voor omgevingsvergunningen afgehandeld door het team Vergunningen, Toezicht en Handhaving (VTH). Inwoners en bedrijven dienen hun aanvraag vrijwel altijd digitaal in via het landelijk Omgevingsloket, waarbij zij moeten inloggen met DigiD (particulieren) of eHerkenning (bedrijven). Deze identificatiemethode vormt de eerste verificatie van de identiteit van de aanvrager. Na indiening wordt de aanvraag doorgestuurd naar het lokale VTH-systeem IJVI (IJssellandse VTH Informatievoorziening), dat door elf verschillende organisaties wordt gebruikt, waaronder de gemeente Zwolle en de Omgevingsdienst IJsselland.

In IJVI worden diverse persoonsgegevens geregistreerd: BSN-nummer, naam, geslacht, e-mailadres, geboortedatum, geboorteplaats, adresgegevens, naam van partner (indien van toepassing) en eventuele overlijdensgegevens. Deze gegevens worden geverifieerd en actueel gehouden via een directe koppeling met de Basisregistratie Personen (BRP). Om privacy te waarborgen, heeft de gemeente recent een functionaliteit voor dataminimalisatie geïmplementeerd, zodat alleen noodzakelijke persoonsgegevens beschikbaar komen voor het proces.

IJVI werkt met autorisaties om de toegang tot gegevens te regelen. Er zijn verschillende gebruikersgroepen met eigen autorisatieniveaus, zoals medewerkers die zaken mogen registreren, afhandelen, alleen lezen of verwijderen. Medewerkers loggen in via single sign-on, nadat ze eerst met twee-factor-authenticatie hebben ingelogd op hun laptop. Opvallend is dat binnen de gemeente alle geautoriseerde medewerkers toegang hebben tot alle dossiers, ook als ze niet direct betrokken zijn. Deze brede toegang is gekozen om samenwerking te bevorderen. De handelingen zijn wel traceerbaar, want ze worden gelogd in het systeem. De proceseigenaar (leidinggevende) wijst autorisaties toe aan medewerkers, en vier keer per jaar worden deze gecontroleerd op actualiteit.

Voor de gegevensuitwisseling is IJVI gekoppeld aan andere interne systemen: het medewerkersportaal (eSuite) als archiefsysteem, applicatie voor de financiële afhandeling, Smart Documents voor briefsjablonen en applicatie voor communicatie met de gemeenteraad. Extern deelt de gemeente gegevens met de Omgevingsdienst IJsselland (milieuaspecten), Veiligheidsregio (brandveiligheid), Welstandscommissie (esthetische beoordeling), andere overheden (provincie, waterschap, gemeenten) en semi-overheidsorganisaties zoals Vitens. Deze uitwisseling verloopt via de Samenwerkingsfunctionaliteit (SWF) van het Omgevingsloket. Voor alle externe systemen en leveranciers zijn verwerkersovereenkomsten afgesloten.

Er zijn verschillende privacymaatregelen genomen: bij publicatie van aanvragen op overheid.nl worden persoonsgegevens niet gedeeld, belanghebbenden krijgen alleen geanonimiseerde stukken te zien, vertrouwelijke informatie wordt gedeeld via de beveiligde e-maildienst Zivver, en bijzondere persoonsgegevens (zoals medische gegevens die soms ongevraagd binnenkomen) worden niet opgenomen in het dossier.

Er zijn ook aandachtspunten: er is nog geen Data Protection Impact Assessment (dpia) uitgevoerd op het IJVI-systeem, de CISO en FG zijn niet regelmatig bij afdelingsoverleggen aanwezig, de brede toegang tot persoonsgegevens voor alle geautoriseerde medewerkers vormt een potentieel risico, en het grote aantal externe partijen met toegang tot persoonsgegevens vraagt om zorgvuldige monitoring. Er zijn trainingen over informatiebeveiliging en de AVG, is er een protocol voor het melden van datalekken, en tonen de recente aandacht voor dataminimalisatie, de BRP-koppeling en de periodieke autorisatiecontrole aan dat privacy een aandachtspunt is bij de afhandeling van omgevingsvergunningen in de gemeente Zwolle.

[17] Voor de gehele casusbeschrijving zie bijlage 2.

5 Techniek

Onderzoeksvragen 7-9

In dit hoofdstuk gaan we in op de bevindingen met betrekking tot de onderzoeksvragen 7-9. Deze onderzoeksvragen betreffen de techniek. Deze 'harde' kant van informatiebeveiliging en privacy is het geheel van technische maatregelen die gemeente en SSC ONS treffen om ongeautoriseerde toegang tot systemen en gegevens te voorkomen of snel te detecteren, en de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie te waarborgen. De normen die hiervoor gelden zijn als volgt beoordeeld, zie tabel 6.1.

Tabel 6.1. Onderzoeksvragen 7 - 9, normen en beoordeling.[18]

Onderzoeksvragen	Normen	Oordeel
7: Zijn gegevens bij de gemeente voldoende beschermd tegen de toegang door onbevoegden?	De inrichting van de systemen is ingericht op een beleid van 0-tolerance intern en extern	Voldoet
	De systemen zijn ingericht dat zoveel mogelijk voorkomen wordt dat kwaadwillenden toegang krijgen tot de systemen, dat zo snel mogelijk verdacht verkeer wordt gedetecteerd en passende maatregelen worden getroffen om de schade zoveel mogelijk te beperken	Voldoet
8: In hoeverre wordt getoetst of de organisatie 'in control' is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of pentesten, inlooptesten, phishing mails of netwerktesten?	De gemeente Zwolle voert de audits en de (self)assessments in het kader van ENSIA uit	Voldoet
	De gemeente toetst regelmatig fysiek en digitaal de systemen en gedrag en risicobewustzijn van medewerkers	Voldoet deels
	Naar aanleiding van de testen worden verbetermaagregelen geformuleerd en uitgevoerd	Voldoet deels
	De digitale en fysieke infrastructuur van de gemeente doorstaan de testen in het kader van het rekenkameronderzoek	Voldoet deels
9: In hoeverre is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?	De gemeente heeft een integraal beleid op bedrijfscontinuïteit en back-up en herstel geformuleerd en geïmplementeerd	Voldoet deels
	Op de uitvoering daarvan wordt regelmatig geoefend Medewerkers zijn op de hoogte hoe zij incidenten en datalekken moeten melden en de opvolging van de verbetermaatregelen daarop is vastgelegd	Voldoet deels

Testen

Een van de maatregelen in de BIO2 is dat jaarlijks kwetsbaarheidsanalyses of pentesten op de systemen worden uitgevoerd. [19] SSC ONS laat jaarlijks externe en interne netwerkpentesten uitvoeren door een externe partij. De bevindingen uit deze testen worden opgenomen in een verbeterplan. In het kader van doelmatigheid heeft de Rekenkamer Zwolle besloten deze testen

[18] De onderzoeksvragen en de normen waarop beoordeeld wordt zijn in de tabel opgenomen, zie voor alle normen onderzoeksvragen en normen bijlage 2. De beoordeling varieert van: voldoet = voldoet volledig aan de gestelde norm; voldoet deels = voldoet niet geheel aan de norm; voldoet niet = voldoet geheel niet aan de norm; onbekend = niet na te gaan.

[19] Maatregel 18.2.3.1 – 2: Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.

niet over te doen. De Rekenkamer Zwolle heeft aanvullende testen uit laten voeren, namelijk een AD-audit en een wifi-netwerkpentest (zie §6.1).

5.1 Systemen

De eisen die in het informatieveiligheidsbeleid zijn gesteld zijn dat de informatiesystemen tijdens kantoortijd minimaal 95% beschikbaar zijn. Daarbuiten moeten in het kader van rampenbestrijding of handhaving de systemen beschikbaar zijn. En in geval van uitval van processen en systemen als gevolg van een calamiteit, moet de dienstverlening binnen 48 uur hersteld zijn. Uit de NIS2-scan van medio 2024 blijkt dat de gemeente Zwolle en SSC ONS op beveiliging van 'netwerk & informatiesystemen' en 'bedrijfscontinuïteit' nog niet geheel voldoen aan de BIO2-eisen.

Kwetsbaarheden

SSC ONS en de gemeente zijn aangesloten bij de Informatiebeveiligingsdienst (IBD) voor kwetsbaarheidsmeldingen. Incidenten en kwetsbaarheden in software of systemen die relevant zijn voor de gemeentelijke infrastructuur worden door de IBD gemeld. Algemene openbare meldingen komen binnen bij de Algemene Contactpersonen Informatiebeveiliging (ACIB) van gemeente en ONS. Vertrouwelijke meldingen komen binnen bij de Vertrouwde Contactpersoon Informatiebeveiliging (VCIB). Deze functionarissen zijn dan aan zet om de eventueel benodigde acties binnen de eigen organisatie te bespreken of in gang te zetten. Bijvoorbeeld door software te updaten of, als risico en impact kritiek zijn, systemen offline te halen.

Detectie

De dreiging van aanvallen door malafide hackers, tegenwoordig vaak gesteund door statelijke actoren, neemt toe. Het is daarom zaak om de systemen zo goed mogelijk te beschermen tegen aanvallen van buitenaf, 0-tolerance. En als men binnen is, zo snel mogelijk verdacht verkeer te detecteren en isoleren. Daarvoor zijn applicaties die het dataverkeer monitoren, zoals een SIEM/SOC.[20] In de managementletter 2023 werd de gemeente door de accountant aangeraden een dergelijk systeem te installeren. In het kader van het project Verhoogde Digitale Weerbaarheid van SSC ONS was dat een van de actiepunten. Een met SIEM/SOC vergelijkbare applicatie is geïnstalleerd.

Er is in de applicatie M365 van Microsoft 'endpoint protection' ingericht. Als er iets verdachts gebeurt op een endpoint (desktopcomputer, laptop of tablet) dan komt een melding in het security dashboard. Afhankelijk van de ernst van de melding kan actie ondernomen worden en bijvoorbeeld de computer of laptop geïsoleerd worden. Er is een locatie waar een kopie van de systemen aanwezig is en een backup systematiek. Zodat bij een calamiteit de informatie in de systemen tijdig hersteld kan worden.

Crisisplan

Mocht door stroomuitval of een andere calamiteit de dienstverlening in het geding zijn, dan ligt er een crisisplan van SSC ONS en een continuïteitsplan ICT van de gemeente klaar. Daarin zijn de scenario's beschreven en de verantwoordelijkheden belegd. De dienstverlening kan verplaatst worden naar een uitwijklocatie, zodat de kritieke delen van de dienstverlening binnen 48 uur weer operationeel zijn.

[20] Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.

Zoals eerder gemeld is de crux van deze plannen het testen in de praktijk, zoals BIO2 stelt dat de plannen jaarlijks worden getest op “werking, volledigheid en actualiteit”. Er zijn tot nu toe wel oefeningen op papier gedaan, zogenoemde ’tabletop'-sessies of discussie-oefeningen. Goed om vertrouwd te raken met de crisisplannen, maar dat is nog geen test van de werking in de praktijk.

Een ander aspect van de continuïteits- en crisisplannen is dat deze zich voornamelijk op de continuïteit van de ICT-dienstverlening richten. De bedoeling van BIO2 is dat informatiebeveiliging integraal onderdeel wordt van de risicomanagementmethodiek van de organisatie.

5.1 Pentesten

Op de systemen zijn in het kader van het rekenkameronderzoek de volgende testen uitgevoerd: een AD-audit en een wifi-netwerk test.

AD-audit

De Active Directory (AD) staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een organisatie te beheren. De AD bevat een database waarin onder andere accounts en inloggegevens zijn opgenomen. Een AD audit test onder andere het wachtwoordenbeleid en inactieve accounts. De AD audit is in samenwerking met het SSC ONS uitgevoerd, omdat deze de AD van alle partners in de samenwerking beheert. Deze audit beperkt zich tot de 2.533 gebruiker accounts van de gemeente Zwolle, dat zijn gebruikers- en beheerdersaccounts. Niet allemaal worden ze door medewerkers en beheerders gebruikt, maar ze zijn wel met toegangsrechten in de Active Directory opgenomen. Dat kunnen accounts zijn die voor specifieke diensten worden gebruikt.

Er zijn 10 accounts met een zwak wachtwoord aangetroffen. 402 accounts met een wachtwoord van een jaar of ouder of waarvan het wachtwoord nooit verloopt. Daarvan hebben in totaal 26 domain admin rechten, deze hebben meer rechten dan de reguliere accounts.

303 accounts gebruiken niet unieke wachtwoorden, dat wil zeggen een wachtwoord dat vaker wordt gebruikt. En er zijn 48 accounts met een zogenoemd LM hash wachtwoord, op basis van een verouderde verificatiemethode.

Er zijn tijdens de AD audit 7 bevindingen gedaan met risicoclassificatie ‘hoog’ en 8 met een gemiddelde risicoclassificatie. Daarmee wordt de volledige risicoscore op de AD audit op ‘hoog’ ingeschat.

Wifi-netwerktest

Op 15 januari 2025 is wifi netwerk pentest uitgevoerd op de locatie van het stadskantoor van Zwolle. Deze test is uitgevoerd met een zogenoemde black-box aanpak. Om de beveiliging van de wifi te toetsen, hebben de ethische hackers eventuele kwetsbaarheden in kaart gebracht en daar waar mogelijk geëxploiteerd. Met deze pentest wordt de effectiviteit van de genomen beveiligingsmaatregelen geverifieerd. Het algemene risiconiveau dat de uitgevoerde wifi pentest en de uitvoerbaarheid van mogelijke kwetsbaarheden opleverde is als ‘laag’ ingeschat. Er zijn tijdens de test 2 vermeldenswaardige bevindingen gedaan. Het gastennetwerk Zwolle-Publiek was ten tijde van de test toegankelijk, terwijl het netwerk vanaf 1-1-2025 niet meer actief zou zijn. Daarnaast maakt het netwerk ‘govroam’ gebruik van een protocol dat gevoelig is voor reeds bekende kwetsbaar-

heden. [21] Govroam is een landelijk opererend netwerk en valt buiten de invloedssfeer van de gemeente of SSC ONS.

[21] Het protocol dat govroam gebruikt is kwetsbaar voor zogenoemde 'man-in-the-middle'- of bruteforce-aanvallen. Bij een man-in-the-middle-aanval kan een hacker de communicatie tussen twee partijen onderscheppen en meeluisteren ('eaves-dropping'). Een bruteforce aanval is een hackingtechniek waarbij herhaaldelijk verschillende combinaties van wachtwoorden of coderingssleutels worden geprobeerd tot de juiste is gevonden.

6 Betrokkenheid van de raad

Onderzoeksvraag 10

In dit hoofdstuk gaan we in op de bevindingen met betrekking tot onderzoeksvraag 10, de betrokkenheid van de raad bij de onderwerpen informatiebeveiliging en privacy. De normen die hiervoor gelden zijn als volgt beoordeeld, zie tabel 7.1.

Tabel 7.1. Onderzoeksvragen 10, normen en beoordeling.[22]

Onderzoeksvraag	Normen	Oordeel
10. Hoe is de raad betrokken bij het beleid ten aanzien van informatieveiligheid? Op welke manier wordt de gemeenteraad geïnformeerd over de uitkomsten van uitgevoerde audits op het gebied van informatiebeveiliging? Is de raad daarmee adequaat gepositioneerd om zijn kaderstellende en controlerende rol te kunnen vervullen?	De informatievoorziening aan de raad en de overlegmomenten tussen raad en college over informatieveiligheid zijn voldoende om de gemeenteraad te positioneren om de kaderstellende en controlerende rol te laten vervullen	Voldoet deels
	De raad is dusdanig betrokken op het onderwerp informatieveiligheid dat vragen over het beleid en de uitvoering worden gesteld	Voldoet niet

Kaderstellen en controleren

Uitgangspunt op de gemeentelijke governance is dat de raad kaders stelt voor het college en daarna het college controleert op de uitvoering. De raad heeft daarnaast de taak om de gemeentelijke begroting vast te stellen en de jaarstukken te accorderen. In het informatiebeveiligingsbeleid heeft de gemeente Zwolle vastgelegd dat de gemeenteraad geïnformeerd moet worden. De rollen kaderstellen en controleren worden in het beleid niet benoemd.

Beleid

Het beleid wordt grotendeels vastgesteld door directie en college. Informatiebeveiliging is grotendeels belegd bij informatievoorziening en bedrijfsvoering. Dat laatste onderdeel van de overhead valt traditiegetrouw bestuurlijk onder het college. De raad wordt geïnformeerd over de besluitvorming op informatiebeveiliging en privacy.

Begroting

Uiteindelijk moet de gemeenteraad de begroting vaststellen. Informatiebeveiliging en privacy zijn als posten verwerkt en worden in die zin onder de kaderstellende rol van de raad begrepen. Volgens respondenten weet de raad dat het, ondanks beperkte middelen, belangrijk is te blijven investeren in informatieveiligheid. De raad heeft volgens hen het standpunt dat er een goede balans tussen dienstverleningsniveau, gebruiksvriendelijkheid en veiligheid moet worden gezocht. Voor specifieke projecten, zoals Verhoging Digitale Weerbaarheid ter verhoging van de

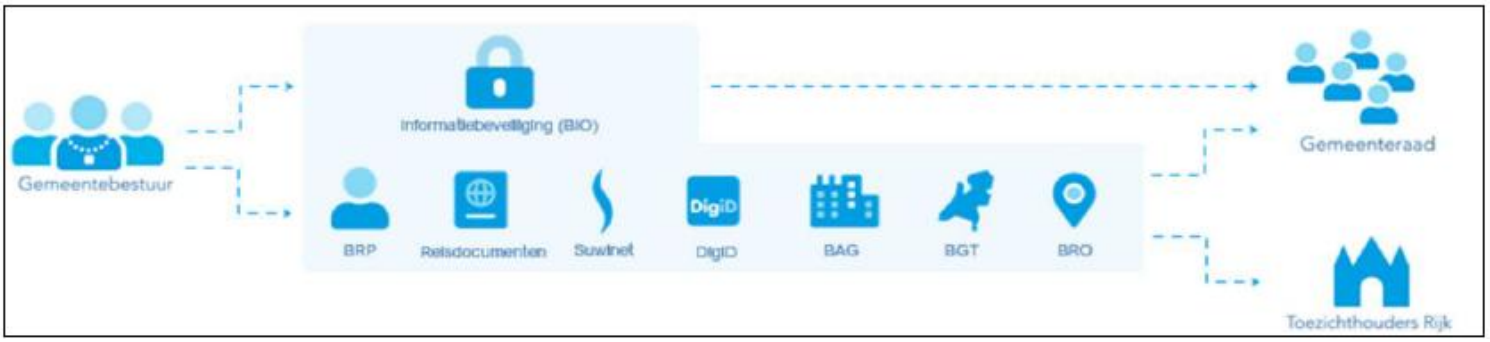
[22] De onderzoeksvragen en de normen waarop beoordeeld wordt zijn in de tabel opgenomen, zie voor alle normen onderzoeksvragen en normen bijlage 2. De beoordeling varieert van: voldoet = voldoet volledig aan de gestelde norm; voldoet deels = voldoet niet geheel aan de norm; voldoet niet = voldoet geheel niet aan de norm; onbekend = niet na te gaan.

robuustheid van het netwerk en de veiligheid van digitale informatie, heeft de raad in 2022 en 2023 ingestemd met extra middelen ten behoeve van SSC ONS. Tevens zijn voorzieningen getroffen om in 2025 de bezetting op informatiebeveiliging en privacy te vergroten met een aantal gecombineerde functies, PISO's.

Controle

De raad van Zwolle wordt in het kader van de horizontale verantwoording jaarlijks geïnformeerd met behulp van de ENSIA-rapportage. Daarmee geeft het college aan de raad aan in welke mate de gemeente op informatiebeveiliging in control is op een aantal voor de gemeente belangrijke verwerkingsprocessen. Op basis van ENSIA doet het college verslag van de zelfaudits op de verschillende basisregistraties: Basisregistratie Personen (BRP), Reisdocumenten, Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO). En geeft een assuranceverklaring over de externe audits op de applicaties Suwinet en DigiD. Daarnaast brengen internal audit, CISO en FG jaarlijks verslag uit aan de raad over de activiteiten op hun terrein. SSC ONS rapporteert ook jaarlijks aan de raden van de partners over de activiteiten, en dus ook over informatiebeveiliging. Daarbij kan de raad een zienswijze geven over verslag van de activiteiten en de begroting.

Figuur 7.1. ENSIA-rapportage



Accountant

De accountant voert een IT-controle uit en rapporteert daarover in de boardletter. Informatieveiligheid wordt daarbij meegenomen, vooral binnen het kader van de toets op de financiële rechtmatigheid van de gemeentelijke financiën. De IT-controle is geen uitputtende toets op informatieveiligheid, maar levert nuttige bevindingen op met betrekking tot de vraag in hoeverre de gemeente voldoet aan de eisen die de wetgever op dat vlak stelt. De boardletters worden in de auditcommissie geagendeerd en besproken. In de brieven van de auditcommissie aan de gemeenteraad wordt zijdelings ingegaan op de vraagstukken op informatiebeveiliging die de accountant aansnijdt. De bedoeling is dat in de toekomst concern control de IT-audit intern gaat uitvoeren. Daarvoor is in 2025 een IT-auditor in de gemeente werkzaam geworden.

Ad hoc

Op deze wijze is de controle door de raad op informatiebeveiliging en privacy ingericht. Ad hoc wordt de raad door college ingelicht bij incidenten met consequenties voor de inwoners en de samenleving. Daarin zullen raad en college steeds een balans moeten vinden tussen enerzijds vertrouwelijkheid van gegevens of gebeurtenis en de impact op betrokkenen.

Sessies	Er worden via de griffie in overleg met de CISO of FG regelmatig sessies georganiseerd om de raad bij te praten over deze onderwerpen of een eventuele kennisachterstand weg te nemen. Vanuit de respondenten wordt de wens te kennen gegeven om meer contact met de raad te hebben. Maar de ervaring tot nu toe is dat deze informatiesessies door raadsleden weinig worden bezocht. Het beeld bij een aantal respondenten is dat de volwassenheid op informatieveiligheid bij de raad hoger kan. Er zijn incidenten op informatiebeveiliging en privacy geweest waarbij de raad betrokken was. Uit de phishingmail test (zie §5.1), die ook onder raadsleden is uitgezet, is een dubbel signaal op te halen. Er blijken relatief veel raadsleden in eerste instantie op de link in een verdachte mail te klikken. Maar opvallend is dat in tweede instantie geen raadslid inloggegevens prijs geeft.

Bijlage 1. Onderzoeksvragen en normen

De onderstaande normen zijn opgesteld op basis van de normen van de Baseline Informatiebeveiliging Overheid (inclusief de 10 bestuurlijke principes informatiebeveiliging), Agenda Digitale Veiligheid 2024-2026 VNG en dreigingsbeelden van de IBD.

Onderzoeksvragen	Normen
Organisatie	
1. Wat is het beleid van de gemeente Zwolle op het gebied van informatieveiligheid en voldoet dit aan de actuele standaarden?	- De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat op onderdelen is uitgewerkt in specifieke procedures en/of richtlijnen. De inhoud van het informatiebeveiligingsbeleid sluit aan op good practices, zoals de BIO2 en andere relevante wet- en regelgeving (zoals de AVG). - De gemeente beschikt over een actueel informatie-beveiligingsplan met concrete activiteiten om nader invulling te geven aan diverse onderdelen van het informatiebeveiligingsbeleid. Op basis van de activiteiten is er een urenraming en budget opgesteld. - De gemeente besteedt 10% van het ICT-budget aan maatregelen ter bevordering van informatieveiligheid.
2. Hoe gaat Zwolle om met risico's en incidenten op het gebied van informatieveiligheid?	- Er worden met voldoende frequentie GAP- en risicoanalyses uitgevoerd. In de analyses zijn de belangrijkste risico's geïdentificeerd en worden verbetermaatregelen getroffen op de risico's die niet geaccepteerd worden.
3. Zijn de functionarissen op informatiebeveiliging en gegevensbescherming met betrekking tot hun taak juist gepositioneerd?	- Taken en verantwoordelijkheden rond informatie-beveiliging en de bescherming van (bijzondere) persoonsgegevens zijn duidelijk belegd in de organisatie. - De functionarissen op informatiebeveiliging zijn goed gepositioneerd om hun rol te kunnen vervullen.
4. Hoe wordt dit beleid uitgevoerd op strategisch, tactisch en operationeel niveau?	- Het beleid zoals vastgesteld op strategisch niveau wordt op tactisch niveau ingevuld met de benodigde protocollen en op operationeel niveau uitgewerkt in richtlijnen en werkwijzen - Het beleid wordt op strategisch, tactisch en operationeel uitgevoerd zoals is vastgelegd - Het normenkader van de BIO2 en de doelstellingen van de gemeente op informatieveiligheid worden gerealiseerd
Mens	
5. Op welke wijze wordt aandacht besteed aan de bevordering van bewustwording en eigenaarschap met betrekking tot risico's op het gebied van informatiebeveiliging bij bestuurders en medewerkers van de gemeente en bij raadsleden?	- Informatieveiligheid en gegevensbescherming is een onderdeel van de 'onboarding' van medewerkers - Medewerkers en bestuurders krijgen regelmatig scholing op de risico's op informatieveiligheid - Raadsleden worden door de gemeente voorgelicht op de risico's op informatieveiligheid en gegevensbescherming en door de gemeente daarin gefaciliteerd
6. Zijn de rollen die medewerkers hebben t.a.v. informatiebeveiliging duidelijk voor de medewerkers? Hoe is de 'tone at the top' en hoe werkt dit door in de organisatie? Krijgen de risico's met betrekking tot informatiebeveiliging voldoende aandacht in alle organisatielagen?	- Op bestuurlijk en directieniveau van de gemeente wordt informatiebeveiliging en gegevensbescherming regelmatig geadresseerd en bestuurders en directieleden dragen het belang van deze onderwerpen uit, onder andere door voorbeeldgedrag - De medewerkers van de gemeente zijn op de hoogte van hun rol op informatieveiligheid en gegevensbescherming en gedragen zich daarnaar

Techniek	
7. Zijn gegevens bij de gemeente voldoende beschermd tegen de toegang door onbevoegden?	- De inrichting van de systemen is up-to-date en ingericht op een beleid van 0-tolerance intern en extern - De systemen zijn ingericht dat zoveel mogelijk voorkomen wordt dat kwaadwillenden toegang krijgen tot de systemen, dat zo snel mogelijk verdacht verkeer wordt gedetecteerd en passende maatregelen worden getroffen om de schade zoveel mogelijk te beperken
8. In hoeverre wordt getoetst of de organisatie 'in control' is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of pentesten, inlooptesten, phishing mails of netwerktesten?	- De gemeente Zwolle voert de audits en de (self)assessments in het kader van ENSIA uit - De gemeente toetst regelmatig fysiek en digitaal de systemen en gedrag en risicobewustzijn van medewerkers - Naar aanleiding van de testen worden verbetermaagregelen geformuleerd en uitgevoerd - De digitale en fysieke infrastructuur van de gemeente doorstaan de testen in het kader van het rekenkameronderzoek
9. In hoeverre is de continuïteit van de gemeentelijke dienstverlening gewaar-borgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?	- De gemeente heeft een integraal beleid op bedrijfscontinuïteit en back-up en herstel geformuleerd en geïmplementeerd - Op de uitvoering daarvan wordt regelmatig geoefend - Medewerkers zijn op de hoogte hoe zij incidenten en datalekken moeten melden en de opvolging van de verbetermaatregelen daarop is vastgelegd
Betrokkenheid van de raad	
10. Hoe is de raad betrokken bij het beleid ten aanzien van informatieveiligheid? Op welke manier wordt de gemeenteraad geïnformeerd over de uitkomsten van uitgevoerde audits op het gebied van informatiebeveiliging? Is de raad daarmee adequaat gepositioneerd om zijn kaderstellende en controlerende rol te kunnen vervullen?	- De informatievoorziening aan de raad en de overlegmomenten tussen raad en college over informatieveiligheid zijn voldoende om de gemeenteraad te positioneren om de kaderstellende en controlerende rol te laten vervullen - De raad is dusdanig betrokken op het onderwerp informatieveiligheid dat vragen over het beleid en de uitvoering worden gesteld

Bijlage 2. Casebeschrijvingen

‘Follow the information’

Voor het rekenkameronderzoek zijn 2 verwerkingsprocessen in de organisatie nader onderzocht. Het doel is op procesniveau te onderzoeken wat er gebeurt met informatie die de organisatie binnenkomt, in welke systemen de gegevens worden verwerkt, wie toegang heeft tot deze informatie en met welke (externe) partijen de informatie wordt gedeeld. Daarmee kan op praktisch niveau een beeld verkregen worden wat informatiebeveiliging en privacy inhoudt voor een gemeente.

Uit de overige onderzoeksbevindingen blijken er uitdagingen te zijn om gegevensbescherming in de operationele werkprocessen onder te brengen. Bij sommige afdelingen en teams is men daar heel actief mee, zoals bij de sociale wijkteams. Andere afdelingen zijn daar minder actief mee bezig.

Wmo-aanvraag

Gekozen is om een proces in het sociaal domein en een proces in het fysieke domein als case te onderzoeken. Voor het sociaal domein is de aanvraag van een Wmo-voorziening nader onderzocht, om meerdere redenen. Enerzijds omdat bij zo’n aanvraag (bijzondere) persoonsgegevens van inwoners verwerkt kunnen worden. Anderzijds omdat een Wmo-aanvraag als een kritisch bedrijfsproces is aangemerkt, omdat de impact van uitval onacceptabel groot is. Het is dan ook door de gemeente als ‘kroonjuweel’ aangemerkt.

Aanvraag omgevingsvergunning

Voor het verwerkingsproces in het fysieke domein is gekozen voor een aanvraag van een omgevingsvergunning. Een proces dat vanwege de Omgevingswet de laatste jaren een forse ontwikkeling heeft doorgemaakt. Maar is door de gemeente niet als kroonjuweel aangemerkt. Om met de twee cases te variëren is voor deze 2 processen gekozen.

Casus Wmo aanvraag Sociaal domein

Inleiding

De gemeente Zwolle heeft de uitvoering van de Wet Maatschappelijke Ondersteuning (Wmo) belegd bij de Sociale Wijkteams (SWT). Zwolle heeft vijf wijkteams, verspreid over de gemeente, die integraal werken en naast Wmo-aanvragen ook vraagstukken op het gebied van jeugdzorg en participatie behandelen. De teams zijn laagdrempelig bereikbaar voor inwoners via inloopspreekuren (twee keer per week per wijkteam) en een dagelijkse telefonische bereikbaarheidsdienst.

De Sociale Wijkteams hebben een eigen e-mailextensie (swt.zwolle.nl) die verschilt van de reguliere gemeentelijke e-mailadressen (zwolle.nl). Dit draagt bij aan hun herkenbare positie tussen inwoners en de gemeentelijke organisatie. Daarnaast hebben zij een eigen webpagina met privacy voorschriften.

Procesbeschrijving WMO-aanvraag

Aanmelding en registratie

Het proces begint wanneer een inwoner contact opneemt met het wijkteam. Dit gebeurt via een van de volgende kanalen:

- Het inloopspreekuur in de wijk
- De telefonische bereikbaarheidsdienst
- Een doorverwijzing door een andere partij

De medewerker die het eerste contact heeft, registreert de aanvraag in het systeem. Hierbij worden de volgende gegevens vastgelegd:

- Contactgegevens (naam, adres, telefoonnummer)
- Persoonsgegevens (BSN, geboortedatum)
- Gezinssituatie (samenstelling huishouden)
- Probleemomschrijving/situatieschets
- Eventueel betrokken andere instanties (huisarts, school)

Bij dit eerste contact wordt de inwoner geïnformeerd over het feit dat er een dossier wordt aangemaakt en dat persoonsgegevens worden geregistreerd. Ook wordt verteld hoe het proces verder zal verlopen en dat er mogelijkheden zijn voor onafhankelijke cliëntondersteuning.

Toewijzing regisseur en onderzoeksfase

Na registratie komt de casus op de wachtlijst van het betreffende wijkteam. Tijdens een verdelingsmoment, waarbij meerdere teamleden aanwezig zijn, wordt bepaald welke medewerker de casus zal oppakken als regisseur.

Voor gevoelige casussen, zoals aanvragen van bekende inwoners, collega's of familieleden van medewerkers, geldt een apart protocol. Deze casussen kunnen worden doorverwezen naar een ander wijkteam of zelfs naar een andere gemeente (zoals Kampen), om privacy en objectiviteit te waarborgen.

De toegewezen regisseur neemt contact op met de inwoner en voert een of meerdere gesprekken om de vraag te verhelderen. Hierbij wordt gekeken naar:

- De precieze hulpvraag
- Eigen mogelijkheden van de inwoner (zelfredzaamheid)
- Mogelijkheden binnen het sociale netwerk
- Mogelijke voorliggende voorzieningen
- Noodzaak van een maatwerkvoorziening

Tijdens deze fase wordt een integrale benadering gehanteerd. Er wordt breed gekeken naar de situatie van de inwoner, waarbij ook andere leefgebieden aan bod komen. Zo kan bijvoorbeeld blijken dat naast een WMO-voorziening ook ondersteuning nodig is op het gebied van schuldhulpverlening of participatie.

Opstellen ondersteunings-plan en beschikking

Op basis van het onderzoek stelt de regisseur samen met de inwoner een ondersteuningsplan op. Dit plan bevat:

- Een beschrijving van de huidige situatie;
- De te bereiken doelen;
- De in te zetten voorzieningen;
- De duur van de ondersteuning.

Het ondersteuningsplan wordt niet formeel ondertekend, maar er moet wel consensus over bestaan tussen de inwoner en de regisseur. Het plan wordt samen doorgenomen en zo nodig aangepast tot er overeenstemming is.

Vervolgens maakt de regisseur in het systeem een conceptvoorziening aan, die naar de backoffice wordt gestuurd. De backoffice werkt dit uit tot een formele beschikking, die per post naar de inwoner wordt verzonden. Deze beschikking bevat ook een bezwaarclausule, zodat de inwoner weet hoe bezwaar kan worden gemaakt tegen de beslissing.

Voor materiële WMO-voorzieningen (zoals rolstoelen en scootmobielen) wordt contact opgenomen met de leverancier (Welzorg of Kerstin). Voor immateriële voorzieningen (zoals huishoudelijke hulp of begeleiding) wordt de aanvraag via het landelijke berichtenverkeer gecommuniceerd met de betreffende zorgaanbieder.

Uitvoering en nazorg

Na toekenning van de voorziening blijft de regisseur betrokken bij de casus. De inwoner kan bij nieuwe vragen direct contact opnemen met de regisseur. Als er geen actieve begeleiding meer nodig is, wordt de casus op 'slapend' gezet in het systeem, maar de regisseur blijft eigenaar van het dossier. Bij nieuwe vragen of ontwikkelingen kan de casus eenvoudig weer geactiveerd worden.

Informatiesystemen en gegevensverwerking

Kernsysteem

Het Sociaal Wijkteam gebruikt een specifiek primair systeem voor dossiervorming en registratie. Dat is een Software as a Service (SaaS) oplossing met verschillende componenten:

- Regie: voor dossiervorming en casemanagement;
- Financieel: voor financiële afhandeling;
- Koppelvlak naar het landelijke berichtenverkeer via het Gemeentelijk Gegevensknooppunt (GGK).

Het systeem wordt niet beheerd door het Shared Service Center (SSC) ONS van de gemeente, maar direct door de leverancier. Het systeem wordt door ongeveer 25 gemeenten gebruikt, wat zorgt voor een robuuste en doorontwikkelde oplossing.

Autorisatiestructuur

Voor het systeem hanteert het SWT een uitgebreid autorisatieschema:

- Medewerkers hebben alleen toegang tot dossiers binnen hun eigen wijkteam;
- Om toegang te krijgen tot een specifiek dossier moet een medewerker een reden opgeven;
- De regisseur krijgt een automatische melding wanneer iemand anders het dossier raadpleegt;
- Toegangsrechten zijn functiegebonden (sociaal werker, backoffice medewerker, etc.)

Het autorisatieschema wordt beheerd door de functioneel beheerder in samenwerking met het management. Bijzondere toegangsverzoeken worden altijd via deze lijn afgehandeld. De management-verantwoordelijkheid voor het autorisatiebeheer is hiermee duidelijk belegd.

Controle en logging

Alle acties in het systeem worden gelogd, waaronder:

- Wie heeft welk dossier bekeken
- Welke wijzigingen zijn aangebracht
- Wanneer heeft de raadpleging plaatsgevonden

Het management controleert elke twee maanden steekproefsgewijs welke dossiers door medewerkers zijn geraadpleegd. Daarnaast wordt het autorisatieschema elke zes maanden gecontroleerd op actualiteit en correctheid. Dit draagt bij aan het waarborgen van de privacy en informatieveiligheid.

Gegevensdeling en privacy

Uitgangspunten bij gegevensdeling

Bij het delen van gegevens met andere partijen hanteert het SWT de volgende uitgangspunten, waarmee voldaan wordt aan de eisen van de AVG:

- Doelbinding: gegevens worden alleen gedeeld als dit noodzakelijk is voor het doel;
- Minimale gegevensdeling: er worden niet meer gegevens gedeeld dan nodig;
- Toestemming: voor het delen van gegevens is in principe toestemming nodig van de inwoner;
- Functionele omschrijving: er worden vooral functionele beperkingen beschreven, geen medische diagnoses (tenzij deze door de inwoner zelf zijn gedeeld).

Gegevensdeling met Zorgaanbieders

Gegevens worden met zorgaanbieders gedeeld via het landelijke berichtenverkeer. De uitzondering hierop zijn materiële WMO-voorzieningen, waarvoor nog geen berichtenverkeer is ingericht. De gedeelde informatie is beperkt tot wat functioneel noodzakelijk is voor de uitvoering van de zorg.

Bij jeugdhulp wordt doorgaans meer contextuele informatie gedeeld dan bij WMO, vanwege de complexiteit van de problematiek en om te voorkomen dat de jongere opnieuw zijn verhaal moet doen bij de zorgaanbieder.

Gegevensdeling met andere partijen

Gegevens kunnen, met toestemming van de inwoner, worden gedeeld met de volgende andere partijen:

- Huisartsen;
- Scholen (bij jeugdhulp);
- Familieleden die als belangenbehartiger optreden;
- Het CAK (voor de eigen bijdrage).

Intern worden gegevens soms besproken tijdens intervisies met collega's, overleg met gedragswetenschappers en verdelingsmomenten. Hierbij is er aandacht voor privacyaspecten, met name bij de verdelingsmomenten waar meerdere teamleden meekijken naar dossiers.

Communicatiemiddelen

Voor het delen van gegevens gebruikt het SWT verschillende communicatiemiddelen:

- Beveiligde e-mail via Zivver voor externe communicatie met andere professionals;
- Berichtenverkeer voor communicatie met zorgaanbieders verloopt via het beveiligde Gemeentelijk Gegevensknooppunt (GGK);
- Reguliere post voor formele communicatie met inwoners;
- Microsoft Teams voor interne communicatie;

In de praktijk wordt ook WhatsApp gebruikt voor laagdrempelig contact met inwoners. Het SWT erkent dat dit privacyrisico's met zich meebrengt. Er zijn geen formele richtlijnen voor het gebruik van WhatsApp, maar medewerkers zijn zich bewust van de beperkte veiligheid en vermijden het delen van persoonsgegevens via dit kanaal.

Privacymaatregelen en verbeterpunten

Bestaande privacy-

Het SWT heeft verschillende maatregelen getroffen om privacy te

maatregelen

waarborgen:

- In 2020 is een Data Protection Impact Assessment (DPIA) uitgevoerd;
- Er is een register van gegevensverwerkingen bijgehouden;
- Er zijn verwerkersovereenkomsten afgesloten met;
- Er is een datalekprocedure ingericht en medewerkers zijn hiervan op de hoogte;
- Er zijn e-learnings over informatieveiligheid beschikbaar;

Het bewustzijn rond informatieveiligheid onder medewerkers wordt als redelijk en groeiende beoordeeld. Medewerkers zijn zich bewust van het werken met vertrouwelijke gegevens en de noodzaak om deze zorgvuldig te behandelen.

Verbeterpunten

Ondanks de getroffen maatregelen zijn er nog verschillende verbeterpunten:

- Reductie van aantal datalekken
- Verbetering van beveiligde gegevensuitwisseling met inwoners
- Aansluiting van materiële WMO-voorzieningen op het berichtenverkeer
- Betere sturing op deelname aan e-learnings over informatieveiligheid
- Duidelijkere richtlijnen voor het gebruik van WhatsApp
- Betere bewustwording rond het registreren van medische gegevens

Het SWT geeft aan zich bewust te zijn van deze verbeterpunten en werkt aan het updaten van de DPIA en het verder verfijnen van het primaire proces, met specifieke aandacht voor informatieveiligheid en privacy.

Toekomstige ontwikkelingen

Het SWT werkt aan een verdere professionalisering van het informatiemanagement. Na de initiële opbouwfase van de wijkteams (vanaf 2015) is er nu meer ruimte voor doorontwikkeling van ondersteunende processen, waaronder informatieveiligheid.

Respondenten geven aan dat de samenwerking met de gemeentelijke informatievoorziening (IV) kolom de afgelopen jaren is verbeterd, wat bijdraagt aan een betere borging van privacyaspecten. Ook komt er meer aandacht voor het actualiseren van procesbeschrijvingen, met daarin expliciete aandacht voor informatieveiligheid en privacy.

Casus Omgevingsvergunning

Inleiding

Deze casebeschrijving geeft inzicht in hoe het team Vergunningen, Toezicht en Handhaving (VTH) van de gemeente Zwolle omgaat met aanvragen voor omgevingsvergunningen. De beschrijving belicht de gebruikte systemen, geregistreerde gegevens, gegevensuitwisseling met andere partijen en de wijze waarop privacyvraagstukken worden behandeld.

De informatie is gebaseerd op interviews met medewerkers van de gemeente Zwolle en de Omgevingsdienst IJsselland, die samen verantwoordelijk zijn voor de afhandeling van omgevingsvergunningen. De case biedt inzicht in de huidige werkwijze binnen het kader van de Omgevingswet.

Procesverloop Omgevingsvergunning

Aanvraagproces

Het proces van een omgevingsvergunning begint wanneer een inwoner of bedrijf een aanvraag indient via het landelijk Omgevingsloket. De aanvrager moet hiervoor inloggen met DigiD (particulieren) of eHerkenning (bedrijven). Deze identificatiemethode zorgt voor een eerste verificatie van de identiteit van de aanvrager.

Hoewel het niet verplicht is om digitaal in te dienen, gebeurt dit in de praktijk vrijwel altijd. Slechts in uitzonderlijke gevallen (één of twee keer per jaar) wordt een aanvraag op papier ingediend. Daarnaast biedt de gemeente eventueel hulp bij het digitaal indienen van een aanvraag.

Na indiening wordt de aanvraag vanuit het landelijk Omgevingsloket doorgestuurd naar het lokale VTH-systeem IJVI (IJssellandse VTH Informatievoorziening) van de gemeente Zwolle.

Publicatie en participatie

De gemeente publiceert alle binnengekomen aanvragen op overheid.nl (bekendmakingen.nl). Dit is wettelijk verplicht. Daarnaast heeft Zwolle een eigen procedure, de "Zwolse Zienswijze", waarbij belanghebbenden in een vroeg stadium worden uitgenodigd om te reageren op de aanvraag. Deze aanpak is bedoeld om in een informele fase al draagvlak te creëren of aanpassingen door te voeren, voordat het definitieve besluit op de aanvraag wordt genomen en het proces formeler wordt in de bezwaarfase. Daarnaast is het de bedoeling om daarmee ook de zienswijzen in de uiteindelijke besluitvorming mee te nemen.

Bij publicatie worden de persoonsgegevens van de aanvrager niet gedeeld. Belanghebbenden die informatie opvragen over een aanvraag, krijgen geanonimiseerde stukken te zien.

Beoordelingsproces

Door middel van taken wordt de aanvraag binnen de gemeente toegewezen aan verschillende specialisten, afhankelijk van de aard van de aanvraag. Bij complexe aanvragen kunnen meerdere adviseurs betrokken zijn, zoals:

- Planologen;
- Verkeersdeskundigen;
- Milieuspecialisten (vaak van de Omgevingsdienst);
- Specialisten op het gebied van brandveiligheid (van de Veiligheidsregio);
- Welstandscommissie.

Deze specialisten beoordelen elk hun eigen aspect van de aanvraag en brengen advies uit. De gemeente Zwolle heeft de regie over het proces, maar betrekt deze partijen voor hun specifieke expertise.

Besluitvorming

Na beoordeling door alle betrokken adviseurs wordt een besluit genomen over de aanvraag. In bepaalde gevallen, wanneer een aanvraag niet past binnen het omgevingsplan (voorheen bestemmingsplan) wordt eerst gekeken of van het plan afgeweken kan worden. Mogelijk kan of moet de omgevingsvisie aangepast worden en dan brengt de gemeenteraad een bindend advies uit. Dit geldt bijvoorbeeld voor plannen met meer dan vijf woningen in een specifiek gebied of voor andere politiek gevoelige kwesties zoals windmolens.

Het uiteindelijke besluit wordt gecommuniceerd met de aanvrager. Als er vertrouwelijke gegevens in het besluit staan, wordt de beveiligde e-

maildienst Zivver gebruikt. Daarnaast wordt het besluit gepubliceerd op de site van overheid.nl.

Gebruikte Systemen en Gegevensregistratie

IJVI

Het centrale systeem voor de verwerking van omgevingsvergunningen is IJVI (IJssellandse VTH Informatievoorziening), dat door twaalf verschillende organisaties wordt gebruikt, waaronder de gemeente Zwolle. Het systeem wordt geleverd door Genetics en het softwarepakket heet Powerbrowser 2020. De Omgevingsdienst IJsselland voert het beheer uit voor tien gemeenten, de Veiligheidsregio en de Omgevingsdienst zelf.

In IJVI worden de volgende persoonsgegevens geregistreerd:

- BSN-nummer;
- Naam;
- Geslacht;
- E-mailadres;
- Geboortedatum;
- Geboorteplaats;
- Adresgegevens;
- Naam van partner (indien van toepassing voor adressering);
- Eventuele overlijdensgegevens.

IJVI is gekoppeld aan de Basisregistratie Personen (BRP) via een BRP API. Dit zorgt ervoor dat persoonsgegevens altijd actueel zijn en worden geverifieerd. Recent is een nieuwe functionaliteit geïmplementeerd die gericht is op dataminimalisatie, waardoor alleen de persoonsgegevens beschikbaar komen die noodzakelijk zijn voor het proces.

Medewerkersportaal (eSuite)

Het medewerkersportaal of eSuite is het zaaksysteem van de gemeente Zwolle. Het fungeert als archiefsysteem voor documentopslag en is gekoppeld aan IJVI. De volgende informatie wordt gedeeld tussen IJVI en het medewerkersportaal:

- Zaakomschrijving;
- Zaakstatus;
- Adresgegevens;
- Aanvraaggegevens;
- Documenten.

Het medewerkersportaal wordt ook gebruikt door het Klant Contact Centrum (KCC) om burgers te informeren over de status van hun aanvraag zonder dat zij direct toegang hebben tot IJVI.

Overige systemen

Naast IJVI en het medewerkersportaal worden verschillende systemen gebruikt voor:

- het financiële systeem voor facturering;
- een module binnen het Omgevingsloket voor samenwerking met externe partijen;
- voor het genereren van briefsjablonen;
- tussenleverancier die koppelingen beheert tussen DSO (Digitaal Stelsel Omgevingswet) en IJVI;
- voor communicatie met de gemeenteraad;
- voor het maken en bewerken van documenten.

Voor al deze systemen en leveranciers zijn verwerkersovereenkomsten afgesloten wanneer zij persoonsgegevens verwerken.

Gegevensuitwisseling en Privacy

Autorisaties en toegang

IJVI werkt met autorisaties om de toegang tot gegevens te regelen. Er zijn verschillende groepen gebruikers met eigen autorisatieniveaus, zoals:

- Medewerkers die zaakregistraties mogen doen;
- Medewerkers die zaken kunnen afhandelen;
- Medewerkers met alleen leesrechten;
- Medewerkers die zaken mogen verwijderen.

Toegang tot IJVI is beperkt tot geautoriseerde medewerkers. De medewerkers loggen in via single sign-on, nadat ze eerst met twee-factor-authenticatie hebben ingelogd op hun laptop.

Opvallend is dat binnen een data-eigenaar (zoals de gemeente Zwolle) alle geautoriseerde medewerkers toegang hebben tot alle zaken, ook als ze niet direct betrokken zijn bij een specifieke zaak. Dit geldt ook voor medewerkers van de Omgevingsdienst en de Veiligheidsregio die werken voor de gemeente Zwolle. Deze brede toegang is gekozen om samenwerking te bevorderen, maar alle handelingen worden wel gelogd in het systeem.

De proceseigenaar (leidinggevende) is verantwoordelijk voor het toewijzen van autorisaties aan medewerkers. Vier keer per jaar worden de autorisaties gecontroleerd om te zien of deze nog actueel zijn.

Gegevensuitwisseling met Externe Partijen

De gemeente Zwolle deelt gegevens uit IJVI met verschillende externe partijen:

1. **Omgevingsdienst IJsselland**: Voor milieu-gerelateerde aspecten van vergunningen
2. **Veiligheidsregio**: Voor brandveiligheid en externe veiligheid
3. **Welstandscommissie**: Voor esthetische beoordeling van bouwplannen
4. **Andere overheden**: Zoals provincie, waterschap en andere gemeenten
5. **Semi-overheidsorganisaties**: Zoals Vitens (waterbedrijf)

De uitwisseling met andere overheden en semi-overheidsorganisaties verloopt via de Samenwerkingsfunctionaliteit (SWF) van het Omgevingsloket.

Externe Inhuur en flexibele Schil

Naast vaste medewerkers werkt de gemeente ook met ingehuurd personeel en een "flexibele schil" via raamcontracten met externe bureaus. Deze externen krijgen ook toegang tot IJVI, maar hebben allemaal een eigen account. Er wordt niet gewerkt met algemene accounts die door meerdere personen worden gebruikt.

Privacymaatregelen en -vraagstukken

Dataminimalisatie en privacybescherming

De gemeente Zwolle en de Omgevingsdienst IJsselland nemen verschillende maatregelen om privacy te waarborgen:

1. **Koppeling met BRP**: Er is een directe koppeling met de Basisregistratie Personen om gegevens te verifiëren en actueel te houden
2. **Dataminimalisatie**: Recent is een nieuwe functionaliteit geïmplementeerd om alleen de persoonsgegevens beschikbaar te stellen die noodzakelijk zijn voor het proces

3. **Beveiligde communicatie**: Bij het delen van vertrouwelijke informatie wordt gebruik gemaakt van Zivver
4. **Anonimisering**: Bij het delen van stukken met belanghebbenden en derden worden persoonsgegevens geanonimiseerd
5. **Beperkte toegang**: Alleen geautoriseerde medewerkers hebben toegang tot IJVI
6. **Loggen van handelingen**: Alle handelingen in IJVI worden gelogd

Omgang met Bijzondere persoonsgegevens

Soms komen ongevraagd bijzondere persoonsgegevens binnen bij aanvragen, bijvoorbeeld medische gegevens bij aanpassingen aan woningen voor mensen met een beperking. Het beleid is om deze gegevens niet op te nemen in het dossier. In plaats daarvan wordt alleen opgenomen dat er contact is geweest met bijvoorbeeld het WMO-team, zonder inhoudelijke medische details vast te leggen.

Data Protection Impact Assessment (DPIA)

Opvallend is dat er noch bij de gemeente Zwolle, noch bij de Omgevingsdienst IJsselland een Data Protection Impact Assessment (DPIA) is uitgevoerd voor het IJVI-systeem en het omgevingsvergunningsproces. Bij sommige andere gemeenten is dit wel gebeurd.

De CISO (Chief Information Security Officer) en FG (Functionaris Gegevensbescherming) lijken geen regelmatige aanwezigheid te hebben bij afdelingsoverleggen om privacyaspecten te bespreken. Wel worden er trainingen gegeven over informatieveiligheid en de AVG, en is er een protocol voor het melden van datalekken.

Risico's en Aandachtspunten

Enkele risico's en aandachtspunten die naar voren komen uit deze casebeschrijving:

1. **Brede toegang tot persoonsgegevens**: Alle geautoriseerde medewerkers hebben toegang tot alle zaken, ook als ze niet direct betrokken zijn
2. **Ontbreken van DPIA**: Er is geen systematische analyse uitgevoerd van privacyrisico's
3. **Informatiebeveiliging**: De balans tussen gebruiksgemak en beveiliging vraagt continue aandacht
4. **Externe partijen**: Veel verschillende externe partijen hebben toegang tot (delen van) de persoonsgegevens

Tegelijkertijd zijn er positieve punten, zoals de aandacht voor dataminimalisatie, de koppeling met de BRP voor accurate gegevens, de periodieke controle van autorisaties en het bewustzijn rondom bijzondere persoonsgegevens.

Bijlage 3. Gebruikte termen en afkortingen

2FA	Zie MFA
Applicatie	Softwareprogramma, zoals SUWInet, DigiD
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband. Deze is in 2019 vervangen door de Baseline Informatiebeveiliging Overheid (BIO)
BIO	Baseline Informatiebeveiliging Overheid
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligingsrisico's van de informatie/applicaties zijn geënt
Blackbox pentest	Zie Pentest
CERT	Computer Emergency Response Team, multidisciplinair samengesteld team dat kan acteren op incidenten en crises
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
CyberSecurity-wet	Ook bekend als Wet Bescherming Netwerken & Informatiesystemen (Wbni)
Dark web	Het dark web is de diepste en verborgen laag van het internet. Het is onderdeel van het ‘deep web’, omdat het niet toegankelijk is via reguliere zoekmachines. Het staat bekend als een plek waar illegale activiteiten plaatsvinden. Hoewel dit inderdaad gebeurt, bestaat het uit meer dan alleen illegale sites.
Dataclassificatie	Betekent inzicht krijgen in de beschikbaarheid, de integriteit en de vertrouwelijkheid van de door of namens de organisatie beheerde en verwerkte informatie (BIV)
DigiD	Digitale Identiteit
DPIA	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
'Endpoint protection'	Of ‘eindpunt-beveiliging’ is het proces van het beschermen van apparaten zoals werkstations, servers en andere apparaten tegen kwaadaardige bedreigingen en cyberaanvallen
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie ook AVG)
GR	Gemeenschappelijke regeling
GRC	Tool om de Governance, Risk and Compliance (GRC) op informatie-beveiliging en privacy te monitoren
Greybox pentest	Zie Pentest

IAM	Zie Identity and Access management
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
Identity and Access management (IAM)	regelt dat de juiste medewerkers het juiste toegangsniveau hebben tot de netwerken en de daarin opgeslagen of verwerkte gegevens. Gebruikersrollen en toegangsrechten worden via een IAM-systeem gedefinieerd en beheerd
ISMS	Information Security Management System, een managementsysteem voor informatiebeveiliging dat gericht is op een continu verbeterproces op basis van de PDCA-cyclus
Logging	In bestanden vastleggen welk dataverkeer over een netwerk gaat. Zo wordt onder andere vastgelegd wie toegang had tot welke persoonsgegevens.
MFA	Multi factor authenticatie is een authenticatie of verificatie methode waarbij twee of meer stappen succesvol doorlopen moeten zijn om ergens toegang tot te krijgen, zoals naast het gebruik van een wachtwoord het gebruik van een token of biometrisch gegeven
NBA	De koninklijke Nederlandse Beroepsorganisatie van Accountants
NIS2	Europese richtlijn Network & Information Systems Versie 2
NOREA	De Nederlandse Organisatie van Register EDP-Auditors
Open source intelligence	onderzoek (Osint) Osint is een techniek om online sporen die op het eerste gezicht verborgen lijken naar de oppervlakte te halen. De techniek maakt gebruik van openbare bronnen
P&C-cyclus	Planning & Control cyclus
PDCA-cyclus	de PDCA-cyclus is een methode voor continue verbetering met vier stappen: Plan, Do, Check, Act. Het wordt gebruikt om processen te verbeteren en problemen systematisch op te lossen
Pentest	Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt kunnen worden om in deze systemen in te breken. Een whitebox test is een teststrategie waarbij de ethische hackers kennis hebben van de technische infrastructuur en systemen en met behulp van die kennis technische zwakheden trachten op te sporen. Dit in tegenstelling tot black- of greybox testen, waarbij de hackers vooraf respectievelijk geen of beperkte kennis hebben van de systemen
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PISO	Privacy and information security officer, komt ook voor indien alleen gericht op privacy als privacy officer (PO) of meer technisch of operationeel als TISO (Technical and information security officer)
Role based access control (Rbac)	Concept waarmee toegang tot gegevens en systemen geschiedt op basis van rollen en functies van de medewerkers. Dat is het concept waarmee Identity Access Management (IAM) wordt uitgevoerd.
SAAS	Software-as-a-Service, is een model waarbij softwaretoepassingen via internet worden aangeleverd
SIEM/SOC	Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort
Suwinet	Gemeenschappelijke elektronische Voorziening Suwi (Wet structuur uitvoering werk en inkomen), of GeVS, ook wel Suwinet genoemd. Is een digitale infrastructuur die is ontwikkeld om ervoor te zorgen dat de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen

TPM	Third Party Memorandum. Verklaring dat een derde partij, die de gegevens voor de gemeente verwerkt, voldoet aan de geldende richtlijnen over informatieveiligheid
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
VNG Realisatie	Kwaliteitsinstituut van de VNG
VNG	Vereniging Nederlandse Gemeenten
Wbni	Wet Bescherming Netwerken & Informatiesystemen (Wbni). De Wbni, beter bekend als de CyberSecurity-wet, wordt aangescherpt met maatregelen voortkomende uit de Europese richtlijn Network & Information Systems V2 (NIS2). Vanaf 2025 Q3 van kracht
Whitebox pentest	Zie pentest

Bijlage 4. Documenten en respondenten

Geraadpleegde documenten

- 20211206 – datastatement gemeente Zwolle
- Aan de slag met Datateams in de organisatie. Implementatieleidraad voor het ontwikkelen van datagedreven oplossingen door Datateams in de organisatie
- Aan de slag met Datateams_Bijlagen_v1.0
- Beleid toegangsbeveiliging/Beheer toegangsrechten, v0.9, 20221011
- Bestuurlijke presentatie digitale veiligheid IJsselland 20240122
- Bijlage 1 - DGW-strategie 2023 - v1.0
- Bijlage 1a - Inrichting Datateams
- Bijlage I Eigenaarschap gemeente Zwolle
- Bijlage II Classificatie gegevenssets
- Brief Auditcommissie over accountantsverslag 2023
- Brief Auditcommissie over accountantsverslag 2024
- BVB - BIO-NIS2 Foto, 20240530
- Checklist Gegevensmanagement 2023
- Clear Screen Clean Desk beleid, Zwolle, 20220222
- Contact met overheidsinstanties en speciale belangengroepen, 20223008
- Continuïteitsplan ICT, gemeente Zwolle, 20220808
- Coordinated vulnerability disclosure, 20220705
- Digitaal Veiligheidsbeeld VCIB-mailinglijst
- Fysiek toegangsbeleid, 20220218
- Gemeente Zwolle - Statement of Work
- Handreiking geheimhoudingsverklaring v0.4, 20220807
- Hoofdlijnen bewustwordingsplan informatieveiligheid 1.0 - Kopie
- Info Blue Fingerprint Detailscenario 20240321,
- Infographic informatieveiligheidsbeleid
- Informatienota prioriteiten FG en CISO voor 2024
- Informatieveiligheidsbeleid 2022-2026, 20220912
- Jaarkalender PO Security 2024-2025
- Jaarverslag FG 2023, 20240531
- Kritische processen (Kroonjuwelen)
- Mailwisseling wereldwijde storing met computers door Crowdstrike, 20240719
- Managementletter 2023
- Managementletter 2024
- Nulmeting BIO, 2021
- Samenvatting DPIA's, FG
- Statement of Work, Zwolle en Awareways, 2024
- Strategisch crisisplan ICT, voor ONS en partners
- Telewerkbeleid, 20220208
- Uitnodiging cyber event Better Safe Than Sorry Zwolle 2 april 2024
- Uitnodiging informatieavond Raads- en statenleden 1-2-2024
- Uitvoeringsplan Cyberbeveiligingswet, gemeente Zwolle,20240923
- Urgent call CISO - aanvulling Directieoverleg 20240612
- VCIB melding vanuit MIVD en AIVD, 20240206
- Verklaring ENSIA 2023 inzake informatieveiligheid DigiD en Suwinet, 20240306
- Wachtwoordbeleid gemeente Zwolle, 20230414

Geïnterviewde respondenten

- CISO, gemeente Zwolle
- FG, gemeente Zwolle
- CISO, SSC ONS
- Portefeuillehouder, gemeente Zwolle
- Directeur, gemeente Zwolle
- Afdelingshoofd IV, gemeente Zwolle
- Sectiehoofd I&K, gemeente Zwolle
- Privacyofficer, gemeente Zwolle
- Medewerkers front- en backoffice Sociaal Wijkteam
- Casemanager Vergunningen, gemeente Zwolle
- Coördinator IJVI-beheerteam, Omgevingsdienst IJsselland
- Concerncontroller
- Coördinator afdeling IA

Bijlage 5. Volwassenheidsniveau NOREA

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, januari 2019, Nederlandse Nederlandse Beroepsorganisatie van Accountants.

Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.