Gemeente
Soest



Informatieveiligheid

25 September 2025

Agenda

1. Aanleiding
2. De wereld om ons heen
3. De afgelopen jaren tot nu
4. Sir Askalot
5. Het aanvalsplan
6. Rapportage
7. Tijdslijn en kostenoverzicht
8. Toekomstige ontwikkelingen
9. Afsluiting en resumé



Gemeente Soest

Aanleiding



Aanleiding: Aanbevelingen

De aanbevelingen uit het rapport Digitale veiligheid van Soest,

- Investeer in een robuuste digitale veiligheidsorganisatie;
- Stel op basis van het strategisch beleid een 'aanvalsplan' digitale veiligheid op dat erop gericht is om aan de wettelijke verplichtingen te voldoen;
- Vraag het college van B en W in samenwerking met u, als gemeenteraad, een begrijpelijke rapportage op te stellen gebaseerd op gangbare normenkaders, risico's en kosten.

Aanleiding: amendement

De volgende wijzigingen in beslispunt 3 door te voeren:

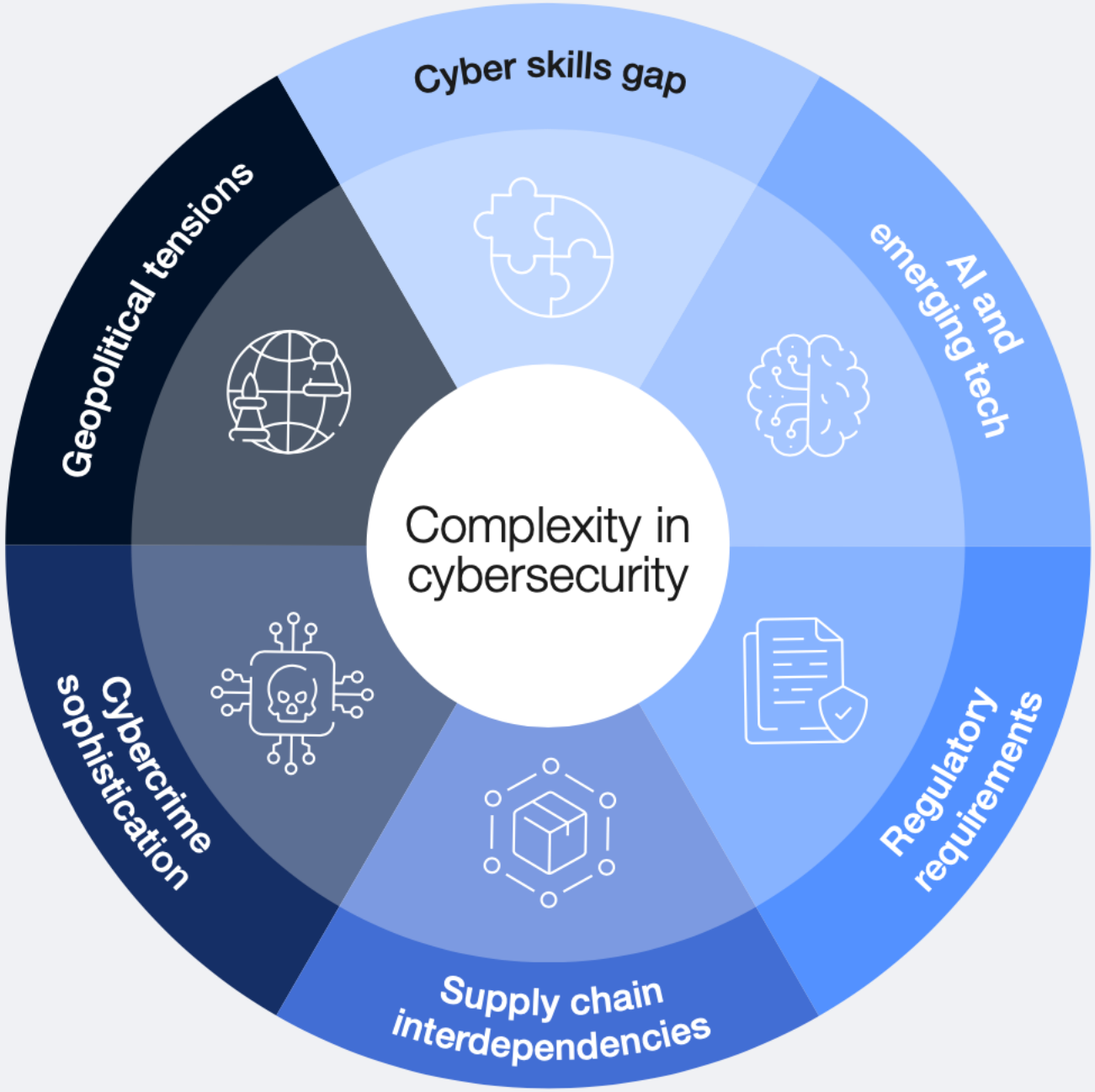
3. Het college van B en W te verzoeken om binnen drie maanden na het raadsbesluit begin september 2025 te rapporteren aan de gemeenteraad over de aanpak of en implementatie van de overgenomen aanbevelingen.

Hierin op te nemen een tijdlijn en kostenoverzicht voor het aanvalsplan Digitale Veiligheid, om vóór eind 2027 aan de normenkaders (BIO2 en NIS2) voor Informatieveiligheid te voldoen.

Gemeente Soest

De wereld om ons heen





Bron: WEF Global Cybersecurity Outlook 2025

Geopolitical tensions



Geopolitical tensions are an influence on cyber strategy in nearly 60% of organizations, with one in three CEOs citing cyber espionage and loss of sensitive information/IP as top concerns.

Cybercrime sophistication



72% of respondents say cyber risks have risen in the past year, with cyber-enabled fraud on the rise, an increase in phishing and social engineering attacks and identify theft becoming the top personal cyber risks.

Supply chain interdependencies



With 54% of large organizations citing third-party risk management as a major challenge, supply chain challenges remain a top concern for achieving cyber resilience.

Regulatory requirements



78% of leaders from private organizations feel that cyber and privacy regulations effectively reduce risk in their organization's ecosystems. However, two-thirds of respondents cited the complexity and proliferation of regulatory requirements as a challenge.

AI and emerging tech



66% of respondents believe that AI will affect cybersecurity in the next 12 months, but only 37% have processes in place for safe AI deployment.

Cyber skills gap



The cyber skills gap has widened since 2024, with two in three organizations reporting moderate-to-critical skills gaps. Only 14% of organizations are confident that they have the people and skills required.

Bron: WEF Global Cybersecurity Outlook 2025

Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

2025 → 2026



VNG

INFORMATIE BEVEILIGINGS DIENST

Samenvatting

Gemeenten staan in 2025-2026 voor een onverminderd complex digitaal dreigingslandschap. Ransomware, datalekken en uitval van processen door incidenten vormen de grootste bedreigingen. Dit vraagt om een proactieve aanpak om digitale veiligheid te waarborgen en vertrouwen van inwoners en ondernemers te behouden. Dit alles in het licht van financiële en personele krapte.

Huidige situatie en uitdagingen

- **Ransomware** blijft de grootste dreiging. Criminelen gebruiken kwetsbare systemen om gevoelige data te stelen en organisaties af te persen, met aanzienlijke gevolgen zoals privacyschendingen, imagoschade en financiële verliezen.
- **Incidenten bij leveranciers** leiden tot verstoringen in gemeentelijke processen. Gemeenten zijn afhankelijk van externe partijen, wat de noodzaak benadrukt van duidelijke afspraken over beveiliging.
- **Beperkte capaciteit, kennis en middelen** bemoeilijken investeringen in digitale veiligheid.

Weerbaarheid

Gemeenten moeten hun digitale weerbaarheid versterken door:

1. **Basismaatregelen** zoals toegangsbeheer met multifactorauthenticatie, netwerkscheiding, back-ups en monitoring in combinatie met bewustwording.
2. **Leveranciersmanagement** te verbeteren met expliciete eisen aan informatiebeveiliging en controle hierop.
3. **Samenwerking** en standaardisatie tussen gemeenten te intensiveren om kosten te verlagen en kennis te bundelen.

Gemeente Soest

De afgelopen jaren



De afgelopen jaren

- Nadruk op implementatie BIO / NIS2
- Vaststelling strategisch informatiebeleid
- Opbouw van kennis op het gebied van Informatieveiligheid
- Invulling rollen functionarissen
- Samenwerking met en binnen RID geïntensiveerd
- Cloudgang
- Leveranciersmanagement (GIBIT)
- Bewustwording op de agenda

Hiermee geven we invulling aan de aanbevelingen van de Rekenkamer



Gemeente
Soest

Sir Askalot



Bewustwording informatiebeveiliging en privacy

Om de bewustwording bij alle medewerkers te verhogen hebben wij een tool genaamd Recourse bewust in control aangeschaft. Deze tool heeft als doel om het informatiebeveiliging- en privacy bewust te verhogen. Dit doen wij op verschillende manieren zoals:

- Wekelijks mail van Sir Ask A Lot
- Jaarlijks een e-learning over informatiebeveiliging & privacy (VERPLICHT)
- Bewustwording via nieuwsberichten

Wekelijks mail van Sir Ask A Lot

Bewust in Control: Weet jij het antwoord?

SA Sir Askalot <sir.askalot@recourse.nl>
Aan Duygu Kara

Beantwoorden | Allen beantwoorden | Doorsturen

di 3-

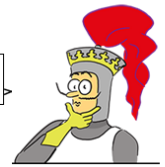
Als er problemen zijn met de weergave van dit bericht, klikt u hier om het in een webbrowser te bekijken.

Bewust in Control

Hallo Duygu,
Hier is weer een vraag voor je.

Sir Askalot is zelfbenoemd expert op het gebied van eigenlijk alles wel maar hij weet het antwoord op juist deze vraag even niet. Jij wel?

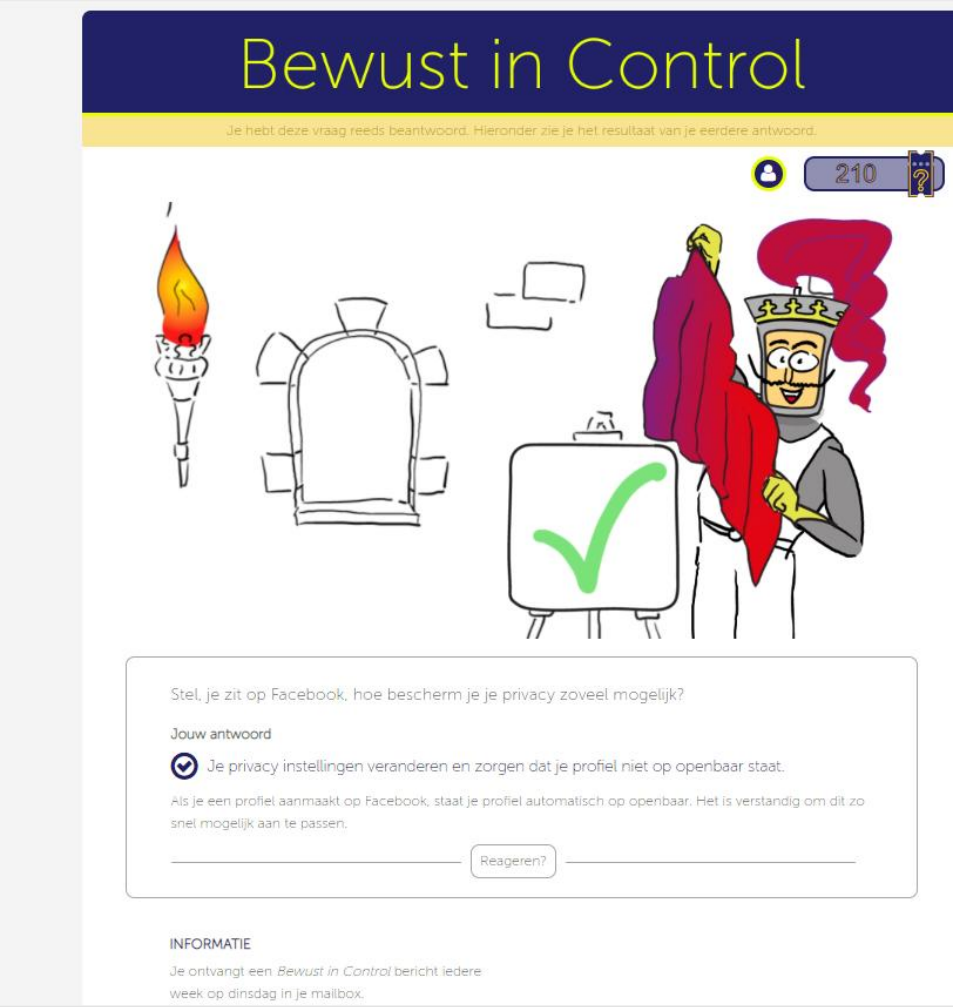
Stel, je zit op Facebook, hoe bescherm je je privacy zoveel mogelijk?



- Niet zo vaak op Facebook komen.
- Zo weinig mogelijk mensen toevoegen in je netwerk.
- Je privacy instellingen veranderen en zorgen dat je profiel niet op openbaar staat.

Over deze e-mail
Deze e-mail is onderdeel van 'Bewust in Control', een programma waar wij met Soest aan deelnemen om de informatieveiligheid binnen onze organisatie te

Wekelijks mail van Sir Ask A Lot





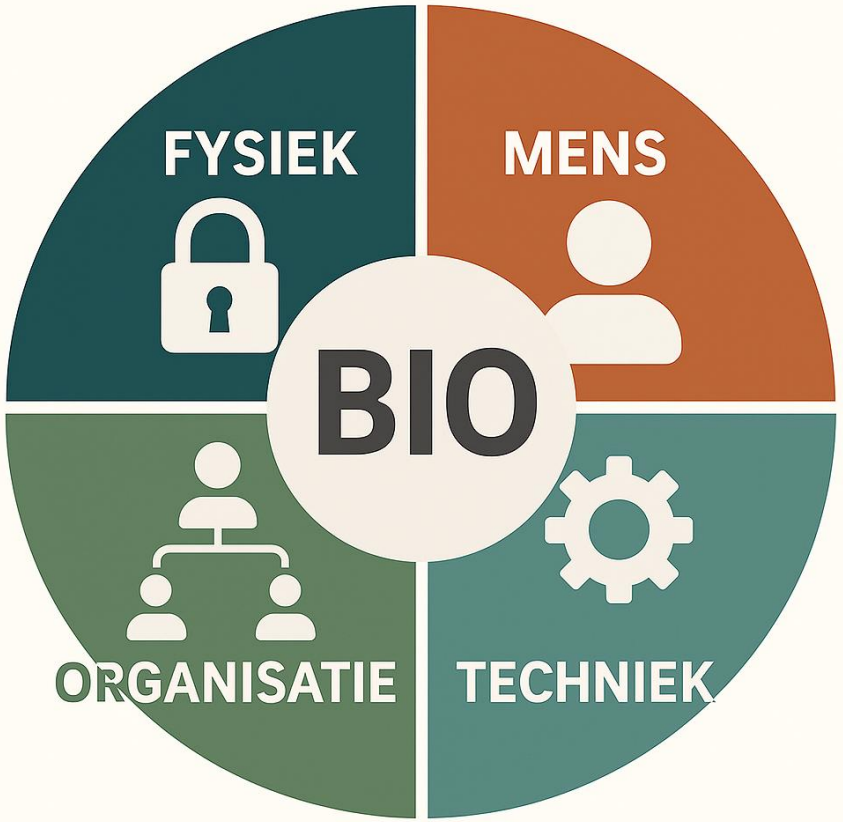
Gemeente Soest

Het aanvalsplan



Aanvalsplan: BIO is de basis





BIO: Risicogericht normenkader met maatregelen om deze risico's te beheersen;

NIS2

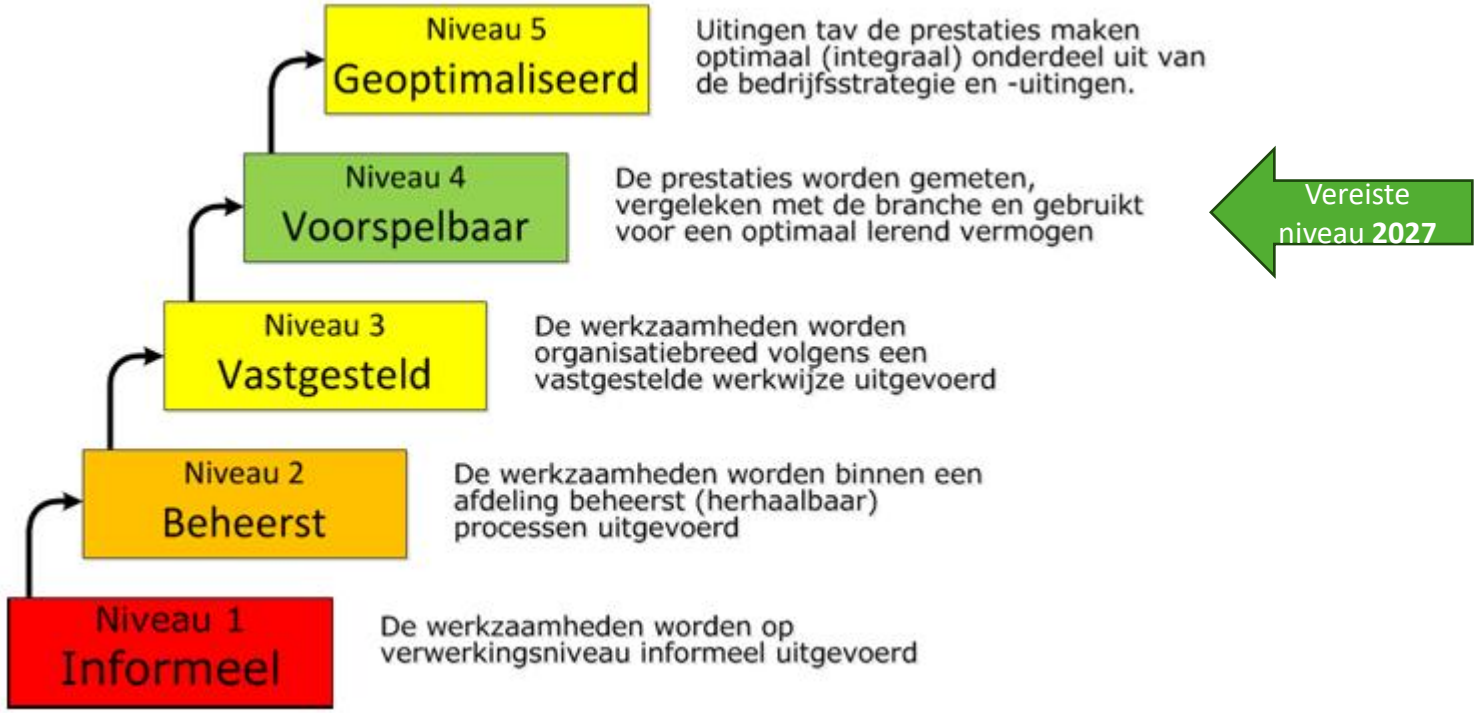
- Niet nieuw maar een wettelijke verankering
- Ambitie op gebied van Informatieveiligheid herijken (volwassenheid van 2 naar 3 naar 4)
- Van een informele inrichting naar formaliseren en verantwoorden
- Naast IT ook OT
- Bestuurlijke aansprakelijkheid inclusief scholing
- Boetes in lijn met AVG

Aanvalsplan: Weerbaarheid vergroten



AANVALSPLAN: HET DOEL

BIO-SA volwassenheidsmodel



UITVOEREN AANVALSPLAN

- Opstellen beleid en proces (groei maar niveau 2)
- Opstellen beheermaatregelen (groei naar niveau 3)
- Sturen en verantwoorden (groei naar niveau 4)
- Doelstellingen per kwartaal bepalen en maandelijks monitoren
- Monitoring middels kwartaalrapportages naar management

Gemeente
Soest

Rapportages



Rapportages: primair via bestaande kanalen

1. Rapportagemomenten als onderdeel van P&C cyclus middels uitbreiding paragraaf in Paragraaf Bedrijfsvoering. Gebaseerd op normenkader is BIO/NIS2
2. AVG via FG (via jaarverslag)
3. ENSIA: regulier (weekbericht)

Status Aanvalsplan

Samenvatting

Toelichting op uitkomsten:



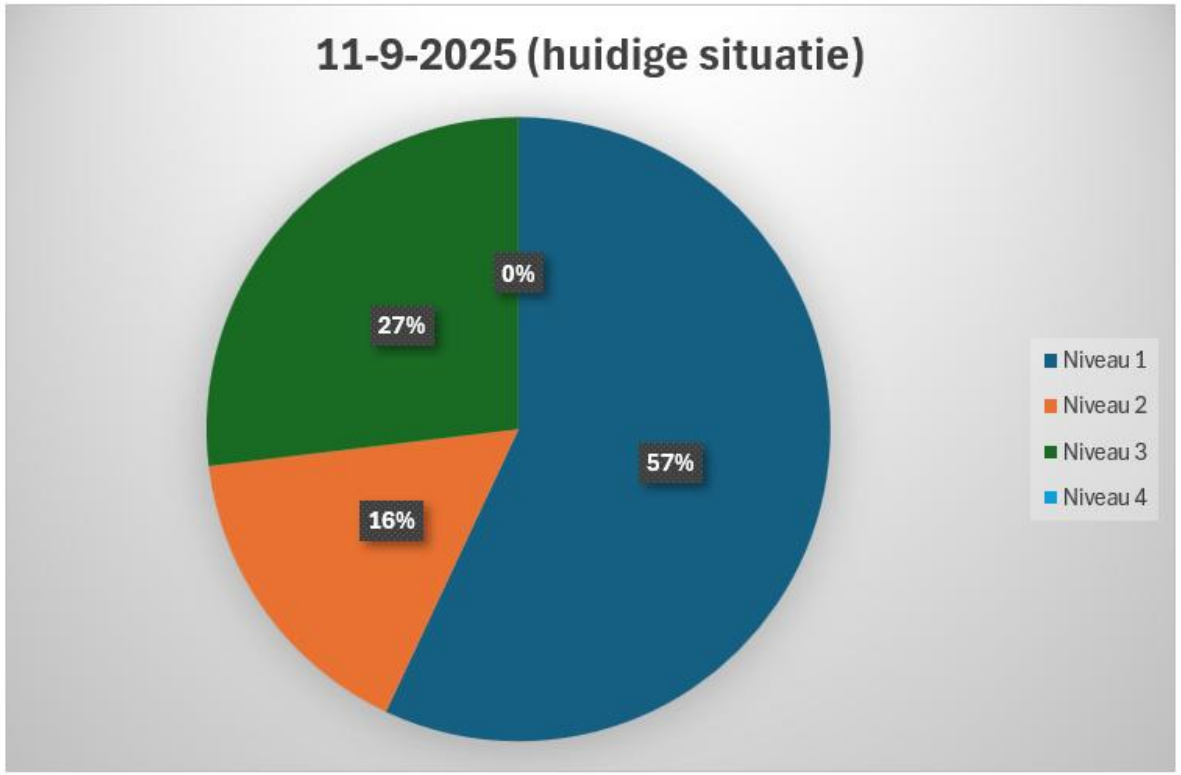
1. OVERALL	
2. FYSIEK	
3. MENS	
4. ORGANISATIE	
5. TECHNIEK	

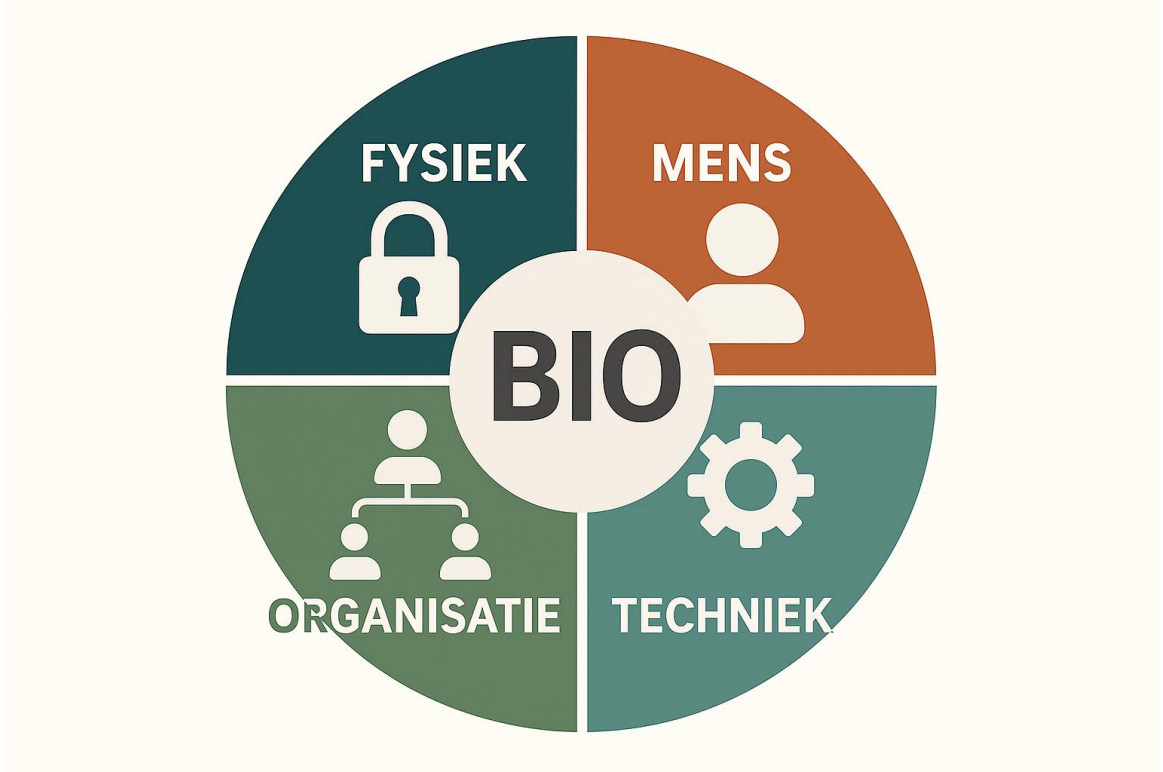
Gemeente Soest

Tijdslijn en kostenoverzicht

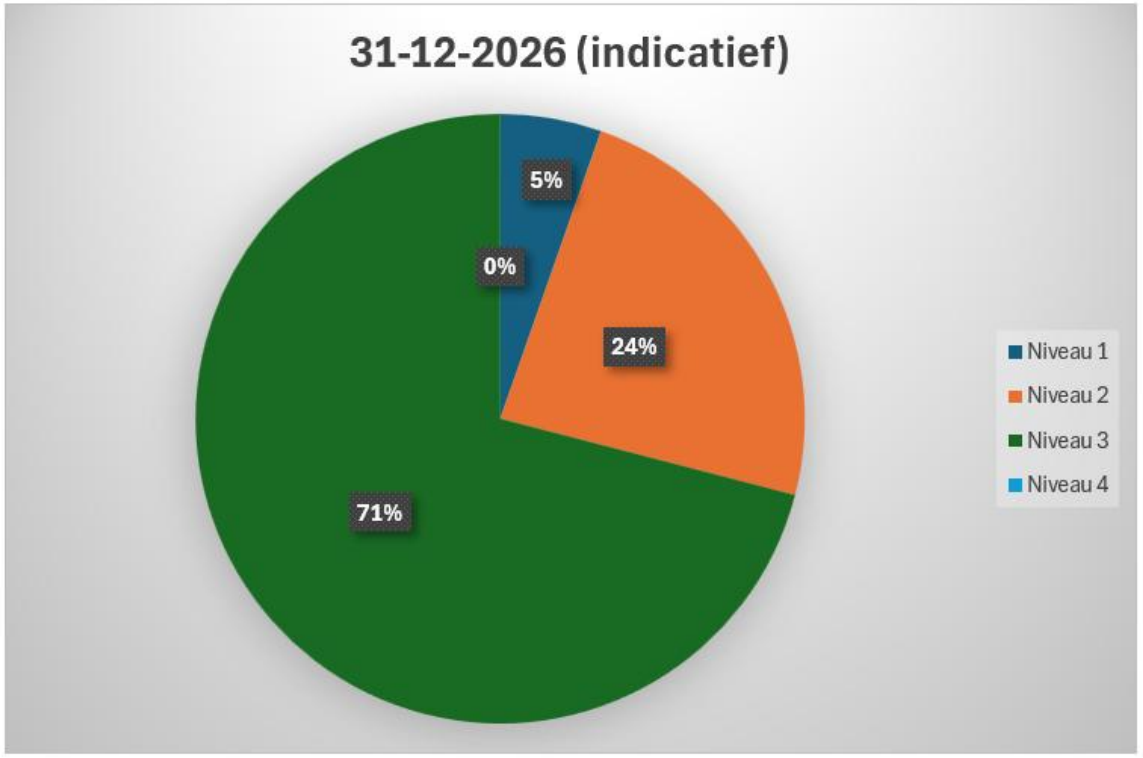


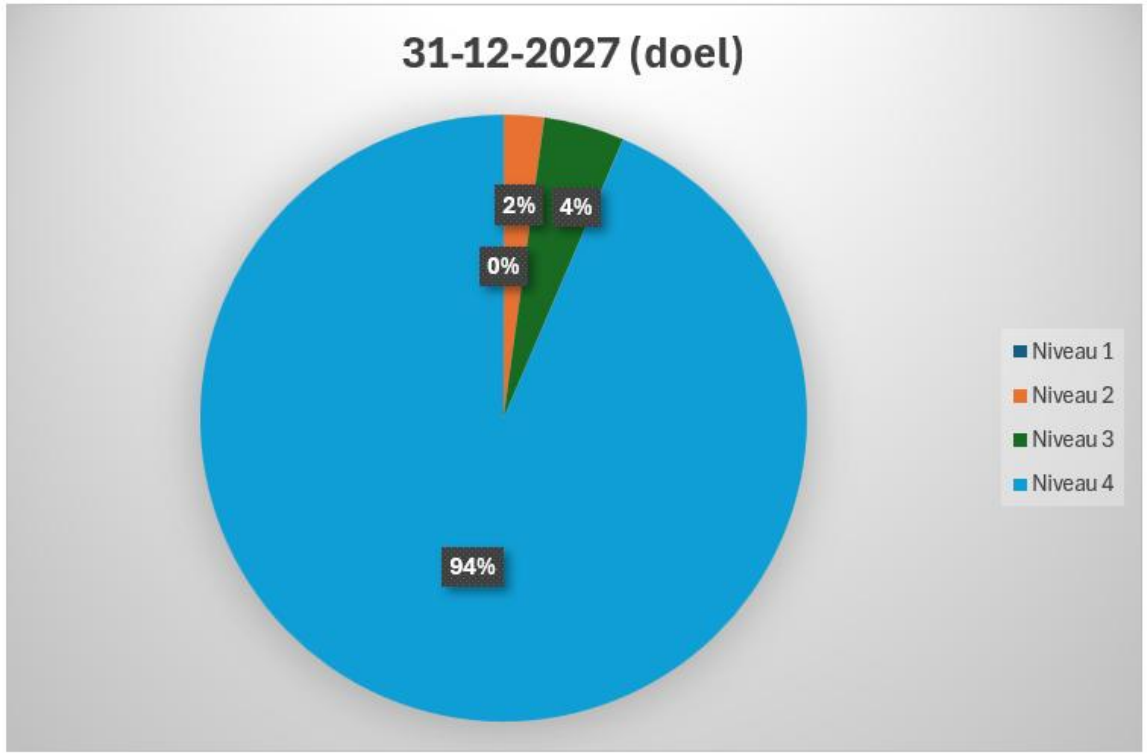
Tijdslijn: huidige situatie





Tijdslijn: 31-12-2027 op niveau 4





Kostenoverzicht: extra middelen noodzakelijk

Uitgangspunt: Informatieveiligheid is regulier werk en daarmee onderdeel overhead

1. Om ambitie te realiseren en niveau te behouden zijn extra middelen noodzakelijk
2. Structureel en incidenteel
3. Kosten zijn opgenomen in kadernota 2026
   - 100k structureel
   - 50k incidenteel voor 2026 en 2027

Gemeente Soest

Toekomstige ontwikkelingen





Trends 2025-2030

De komende jaren zijn er diverse belangrijke trends en risico's op het gebied van informatieveiligheid waar organisaties in Nederland rekening mee moeten houden. Hier zijn de meest opvallende ontwikkelingen voor de periode 2025–2030:

Belangrijke trends en risico's

1. AI
2. Supply Chain Security
3. Aanvallen via leveranciers en partners nemen toe.
4. Menselijke fouten blijven een zwakke schakel.
5. Nieuwe wet- en regelgeving zoals de EU AI Act
6. Ransomware blijft een topbedreiging


NATO
OTAN
The Hague
La Haye
24-25 VI 2025
Summit | Sommet

Gemeente Soest

Afsluiting / Resumé

