Security jaarplan 2025

Provincie Gelderland

Doel van dit document
Beschrijven welke taken met bijbehorende planning het security team voorziet in 2025, voor duiding van en sturing op de verwachte werkzaamheden om strategisch en gecoördineerd de juiste werkzaamheden uit te kunnen voeren.

Versie	:	1.0
Status	:	Definitief
Datum	:	5 februari 2025
Afdeling	:	I&A / CIO – intern PG security team
Auteur	:	5.1.2e

provincie Gelderland

provincie Gelderland

Inhoudsopgave

1 Algemeen

1.1 Versiegeschiedenis

Auteur	Omschrijving	Datum	Versie
5.1.2e	Initieel document	3 december 2024	0.1
	Verwerking opmerkingen stakeholders distributielijst.	16 december 2024	0.2
	Planning ingevuld/bijgevuld aan de hand van meeting met CH/GS/JJ d.d. 19/12/2024.	19 december 2024	0.9
	Geaccordeerde versie 1.0	5 februari 2025	1.0

1.2 Verspreiding

Naam	Functie	Datum	Versie
5.1.2e	Information Security Officer	3 december 2024	0.1
	Information Security Officer	3 december 2024	0.1
	Chief Information Security Officer	3 december 2024	0.1
	Teamleider I&A regie	3 december 2024	0.1
	Lead architect	3 december 2024	0.1
	Chief Information Security Officer	16 december 2024	0.2
	Information Security Officer	16 december 2024	0.2
	Information Security Officer	16 december 2024	0.2
	Chief Information Security Officer	23 december 2024	0.9
	Information Security Officer	23 december 2024	0.9
	Information Security Officer	23 december 2024	0.9
	Teamleider I&A regie	23 december 2024	0.9
	Information Security Officer	Teams Security Team	1.0
	Information Security Officer	Teams Security Team	1.0
	Chief Information Security Officer	Teams Security Team	1.0
	Teamleider I&A regie	5 februari 2025	1.0
	Teamleider CIO Office	5 februari 2025	1.0

Akkoord document 5.1.2e

RE Security jaarplan accordering.msg

2 Context

2.1 Doel van het security jaarplan

Er is een uitbreiding gaande in de security teaminrichting van de Provincie Gelderland. Waar 5.1.2e 5.1.2e tot 2024 als CISO de peiler informatiebeveiliging en implementatie/ onderhoud van het Information Security Management System (hierna: ISMS) als enige binnen de provincie in zijn portefeuille had, hebben 5.1.2e als vaste PG-medewerkers een ISO-rol gekregen – de bezetting van het interne security team binnen de provincie is hiermee uitgebreid naar bijna 2 FTE.

De uitbreiding van het security team – waarbij 5.1.2e in eerste instantie een solo-rol binnen informatiebeveiliging vervulde – vraagt om extra coördinatie en sturing om doelmatig en planmatig te werken. Dit security jaarplan is de basis om de ijkpunten en bijbehorende verwachte taken te definiëren ter uitvoering in 2025.

2.2 Huidige teamsamenstelling

Het security team van de provincie bestaat nu uit vier personen:

Naam	Functie	Bezetting (FTE)
5.1.2e	Chief Information Security Officer	1.0
	Information Security Officer (en architect)	0.45 (ISO), 0.45 (architect)
	Information Security Officer (en wijzigingscoördinator)	0.5 (ISO), 0.5 (wijzigingscoördinator)
	Information Security Officer (externe inhuur)	0.45 (16 uur per week)

In de wekelijkse overleggen binnen de provincie sluiten ook andere medewerkers aan die door hun vervulde rol belang hebben bij goed ingerichte informatiebeveiliging:

- 5.1.2e Lead Architect);
- 5.1.2e (Platform team engineer);
- 5.1.2e Netwerkinfrastructuur engineer);
- Security Analist OGD – 1x per twee weken).

2.3 Externe inhuurkracht - ISO27001-certificering

5.1.2e wordt sinds 2023 ondersteund door 5.1.2e als externe inhuurkracht. Hij is zelfstandig adviseur en consultant en heeft mede gezorgd voor de ISO27001-ceritficering van de provincie, waarbij het ISMS is bepaald en in opzet, deels in bestaan/werking is geïmplementeerd. Daarnaast draagt hij actief bij aan taken die voor de waarborging van ons ISMS nodig zijn – denk hierbij aan de uitvoering van risicoanalyses, het vullen van de ISMS-tooling die de provincie gebruikt (Strict Control Cockpit (hierna: SCC)) voor verantwoording van de ISO27001-maatregelen en het opzetten van hernieuwde processen als Business Continuity Management (BCM). Hij houdt zich tevens bezig met de toekomstige ontwikkelingen op gebied van wet- en regelgeving en de gevolgen voor de provincie Gelderland – denk aan NIS2 en BIO2. Tot slot is 5.1.2e nauw betrokken bij audits en wordt hij betrokken bij de periodieke security overleggen.

3 Interne ontwikkelingen in 2025

3.1 Optimalisering werking van interne security team

Het security team is in 2024 vanuit 1 solo-rol (CISO) uitgebreid naar drie vaste medewerkers (2 ISO's en 1 CISO). Dat vraagt nauwe afstemming met elkaar om elkaars taken goed te laten aansluiten.

- Vanuit het management is het uitgangspunt is dat de externe inhuurkracht in de loop van 2025 de operationele lead in security taken geleidelijkerwijs zal afbouwen. Inherent

16 uur per week

5.1.2e
12/05/2024 09:53
Resolved
Verwerkt.

5.1.2e
12/16/2024 16:24
Resolved

Feitelijk ben ik zelfstandig adviseur en consultant

5.1.2e
12/05/2024 09:53
Resolved
Verwerkt

5.1.2e
12/16/2024 16:25
Resolved

Wellicht toe te voegen: Ik houd mij ook bezig me
NIS2: Business Continuity Management en
LeveranciersRisco.

5.1.2e
12/05/2024 09:55
Resolved
Tevens ook implementatie en optimalisatie van B
naar Bio2.0 - zo ook voor ISO27001

5.1.2e
12/05/2024 10:00
Resolved
Verwerkt.

5.1.2e
12/16/2024 16:31
Resolved

hieraan neemt de taken voor het security team toe en zal het vaste security team steeds meer de operationele security taken die 5.1.2e uitvoerde moeten oppakken. Onder andere vertaalt dit zich in de volgende uitgangspunten.

- 5.1.2e gaat vanuit zijn operationele lead-rol voor ISMS security activiteiten naar een adviserende rol in 2025. Gezien zijn kennis van de ISO27001-certificering binnen PG, de registratie van bewijslast in SCC en de jaarlijkse interne- en externe audit waar 5.1.2e met name bij betrokken is om deze succesvol af te ronden, moet het interne security team meer bij de operationele handelingen worden betrokken.
- Het bijhouden van de tooling SCC, het ISMS systeem van de provincie, vereist specialistische kennis 5.1.2e is tot op heden verantwoordelijk voor het vullen en bijhouden van de tool. Algemene kennis over de tool is op dit moment wel voorhanden maar nog niet voldoende binnen het interne security team. 5.1.2e moet zorgen voor kennisoverdracht van de tool SCC.

5.1.2e zal tot minimaal maart 2026 blijven (tot aan de heraudit ISO27001) als lid van het Security Team, zoals besproken met het Security Team en 5.1.2e

- Inherent moet het interne securityteam verder professionaliseren. Derhalve is het noodzakelijk om in 2025 de noodzakelijke cursussen/opleidingen te volgen die de nodige kennis bijbrengen voor een efficiëntere samenwerking, zowel binnen als buiten het securityteam.
- Op de Teams site van I&A team Regie maakt het Security-team een nieuw Security-kanaal aan, waarin we actief kunnen samenwerken aan documenten. Tevens wordt er een backlog bijgehouden op basis van de interne ontwikkelingen van 2025 + de hieruit voortvloeiende taken, zoals deze zijn benoemd in het jaarplan. Aan de taken worden owners gekoppeld, zodat duidelijk is wie verantwoordelijk is voor de uitvoering van de specifieke actie.

3.2 MSSP dienstverlening (SOC/SIEM en adviesdiensten)

Op dit moment zijn we bezig met de aanbesteding van de Managed Security Service Provider (hierna: MSSP) dienstverlening. Dit betreft een nieuwe dienstverlener binnen de provincie die zowel SOC/SIEM (detectief) als adviesdiensten (preventief) levert voor de IT-omgeving van de provincie:

- Het security team voorziet derhalve een actieve bijdrage van de MSSP in zowel pro-actieve taken (o.a. impact analyses op vulnerabilities, meedenken over security architectuur, bijdrage aan voldoen (nieuwe) wet en regelgeving) als reactieve taken (o.a. leveren van SOC/SIEM diensten, scannen netwerkverkeer en escaleren wanneer nodig) op gebied van informatiebeveiliging binnen de provincie. Dit heeft direct invloed op de taken en verantwoordelijkheden die het interne security team / externe inhuurkracht van de PG zal hebben.
  - We moeten in kaart brengen waar overlappende taken liggen tussen de interne security team, externe inhuurkracht 5.1.2e en de MSSP dienstverlener, om de samenwerking zo soepel als mogelijk te laten verlopen.
  - De operationele werkstructuren (denk aan o.a. overleggen, rapportages) worden samen met de MSSP dienstverlener opgetuigd.

De dienstverlener zal begin 2025 middels een aanbesteding bekend worden. Naar verwachting is de MSSP dienstverlener operationeel actief voor de provincie in Q2 2025.

3.3 Azure migratie en technische BIO-compliance

Op dit moment is de provincie bezig met een Azure migratie, waarbij onze private cloud– beheerd door OGD – stapsgewijs wordt uitgefaseerd. In 2026 verwacht de provincie onze private cloud vergaand te hebben uitgefaseerd en merendeel van de IT-dienstverlening middels Azure danwel SaaS aan te kunnen bieden.

- Omdat nu de Azure-migratie in volle gang is, is het security team voornemens in 2025 slagen te maken op inzicht in (waar mogelijk geautomatiseerd) Azure-compliance op de technische BIO-maatregelen. De MSSP dienstverlener zal hier nauw bij worden betrokken.

- Naast het verkrijgen van inzicht in compliance op de technische BIO-maatregelen, wordt vanuit het security team ook gestuurd op verbetering in technische Azure-implementatie o.b.v. van de BIO-maatregelen. Wederom ligt hier een adviserende rol vanuit de MSSP dienstverlener.
- Bovenstaande punten vragen nauwere samenwerking en afstemming met (1) het security team, (2) platform team en (3) het architectuurteam van de provincie.

3.4 ISMS professionaliseringsslag

Voor behoud van de ISO27001-certificering is het nauwkeurig bijhouden van een ISMS noodzakelijk. De gewenste manier van registeren van bewijslast t.b.v. het BIO-normenkader is nog in ontwikkeling.

- De opzet van de documentatie bestaat, maar het bestaan en de werking van de richtlijnen vereist aandacht. Dat wil zeggen: de richtlijnen zijn aanwezig, maar de aantoonbare uitwerking op de werkvloer – waaraan bewijslast ten grondslag ligt – ontbreekt vaak nog. Voor de toekomstige hercertificeringen van ISO27001 is veelal de tendens dat organisaties kunnen laten zien dat richtlijnen naar behoren op de werkvloer in de organisatie zijn geïmplementeerd.
    - In 2025 komt in ieder geval de optimalisatie van de implementatie van de volgende beleidstukken aan bod: (1) accountbeleid, (2) wijzigingsbeleid.
- In de praktijk zien we nu een uitdaging om de richtlijnen binnen de operatie te implementeren. De documentatie (richtlijnen) die zijn gebruikt voor de ISO27001-certificering zijn namelijk nog beperkt bekend in de interne I&A-teams.
    - Een concreet verbeterpunt voor het security team is om de ISO27001-richtlijnen en de uitwerking hiervan op de werkvloer dichterbij elkaar te brengen. Dit begint bij het publiceren van deze richtlijnen op een centraal beleidsportaal op de Sharepoint omgeving van de provincie (bijvoorbeeld het I&A beleidsportaal).
    - Er zijn vaak reeds interne beleidstukken aanwezig op het I&A beleidsportaal, die al langer bestaan (ver voordat de provincie ISO27001-gecertificeerd was). Deze beleidstukken behoren te worden samengevoegd met de ISO27001-richtlijnen, alvorens we sturen op implementatie van de richtlijnen op de werkvloer.
- Ter voorbereiding op de nieuwe cyberbeveiligingswet (NIS2) wordt in 2025 ingezet op de vormgeving (opzet) en optimalisatie (bestaan/werking) van leveranciersmanagement met een ICT-component binnen de provincie Gelderland.

Zou je deze willen delen met mij ajb?

5.1.2e
12/05/2024 10:03
Resolved

I&A Beleidsportaal Beveiliging (sharepoint.com)
Zie de document-linkjes rechts van de sharepoint pagina.

5.1.2e
12/16/2024 17:22
Resolved

3.5 Regulier uit te voeren operationele security taken

Op dit moment heeft het security team een Excel-lijst (zie: Takenlijst ISO en CISO 2024_opmISOteam_20240827.xlsx) waarin de operationele (periodieke) taken staan genoemd. Tevens staan deze taken genoemd in SCC.

- De tendens is momenteel dat [redacted] een groot deel van deze taken oppakt. We moeten gezamenlijk kijken hoe deze taken structureel evenredig binnen het security team te laten landen. Zie voor beeldvorming onderstaand knipsel voor de activiteiten in 2024:

Deze staan feitelijk in SCC met laatste informatie
bekijken hoe we dat goed weergeven ok?

5.1.2e
12/05/2024 10:04
Resolved
Verwerkt; beschreven dat de taken ook in SCC st
benoemd.

5.1.2e
12/16/2024 17:09
Resolved

Activiteitenlijst Team Security
Bron: SCC

Jaar	Activiteit	Accountable	Verantwoordelijk (R) vanuit ISO Team (zorgt tevens dat het in SCC komt)
2024	Overleggen	[redacted]	
	IPO Overleg		
	SSS Overleg		
	CIBO		
	IP-ISAC		
	Forum Overleg (1x per 3 maanden) (ISO)		
	Directieoverleg (2x per jaar) (ISO)		
	Security Overleg OGO (1x per 2 weken)		
2024	Audits		
	Accountantscontrole		
	Kwetsbaarheids analyses (externe Gelderland sites)		
	Nexpose Audits		
	DigiD Audit (externe audit)		
	Externe Audit (ISO27001 certificering) begeleiding		
	Interne Audit begeleiding		
	Audits Dienstenleveranciers (opvragen rapporten SOC/NEN/ISO)		
	Voorbereiden Intern Audit Oktober		
2024	ISMS-werkzaamheden (periodieke activiteiten)		
	ISMS PDCA (documentatie vaststellen 2 keer per jaar)		
	Bijhouden jaarlijkse check updates in SCC		
	Behandelplan ISMS		
	[redacted]		
	Maatregelenset 2022, Cloud en rapportage		
	Logische Toegangscontrole Azure en breder (RBAC)		
	Opleiding en Bewustwording		
	Review Richtlijnen ISMS		
	Leveranciersmanagement NIS2		
	Directietraining NIS2		
	Incidenten beheer		
2024	ISMS-werkzaamheden (eenmalige activiteiten)		
	Business Continuity Plan		
	Risicoanalyse Office 365		
	Risicoanalyse Cloud Azure		
	Mini-risicoanalynes Cloud project		
	NIS2 Scoping en coordinatie - GAP Analyse en acties		

4 Globale planning van verwachte taken

Op basis van de verwachte ontwikkelingen in 2025 (zie vorig hoofdstuk) zijn taken geëxtraheerd die het security team tot uitvoer zal brengen in 2025. Deze taken zijn geplot in de globale planning hieronder. De taken worden voorzien van een owner (iemand uit het security team) en tevens in het Security teams-kanaal binnen team Regie als backlog-item geregistreerd.

#	Taak	Owner	Jan	Feb	Maa	Apr	Mei	Jun	Jul	Aug	Sept	Okt	Nov	Dec
	Optimalisering werking van interne security team													
1	Reflectie op/optimalisatie van verantwoordelijkheden en taken - Beschrijving van taken en verantwoordelijkheden (zie hoofdstuk 5) - Bijhouden security mailbox; - Check periodieke rapportages van OGD/Azure.	[redacted]												
2	Kennisoverdracht van tool SCC - Wegwijs worden belangrijkste functies tooling *1x in de 2 weken blok van 2 uur inplannen*													
3	Kennisoverdracht van ISMS werkzaamheden - Processen die door SCC worden gefaciliteerd - Jaarlijkse reflectie op IB-richtlijnen; - Registreren van bewijslast bestaan/werking normen; - Voorbereiding van audits.	5.1.2e												
4	Volgen van cursussen/opleidingen - CISSP/CISM; - OSI-model training. *Tijd gebruiken om te bepalen welke cursussen we willen doen*													
5	Interne kennisoptimalisatie binnen PG - Kennisneming van netwerktopologie; - Kennisneming van Azure inrichting.													
	MSSP dienstverlening (SOC/SIEM en adviesdiensten													
6	Afronding van MSSP aanbesteding													

Toegevoegd n.a.v. feedback FJ/MvM

5.1.2e
12/16/2024 17:16
Resolved

	- Beoordelen en consensus *Eind februari: definitieve gunning*	5.1.2e
7	Bepalen van de taken en verantwoordelijkheden van PG en MSSP - implementatiefase - Hoe stemt MSSP af met de overige Service Providers? - Per uitgevraagde dienst: hoe verloopt het proces van input MSSP/PG tot doel/resultaat? *Half mei: implementatie afgerond*	
8	Opzetten van werkstructuren (overleggen/rapportages en KPI's) - implementatiefase - Input en output van de overleggen beschrijven (gebaseerd op rapportage-eisen PvE)	
9	Operatie MSSP binnen PG – inwerken en verrichten - PG IT landschap aansluiten - FTE vanuit MSSP toegewezen	
	Azure migratie en technische BIO-compliance	
10	BIO maatregelen deployment Azure voor inzicht - Conform BIO cloud theme template	
11	Proces inrichten voor registratie bewijslast SCC voor technische BIO compliance	
12	Proces afstemmen enforcement policies t.b.v. BIO-maatregelen met platform team/workload teams Azure.	
13	Operatie van governance Azure policies	
	ISMS professionaliseringsslag	
14	Werking van vernieuwd (Azure-)accountbeleid optimaliseren *Afstemmen me[redacted] Focus op doorstroom van medewerkers i.c.m. rechten-huishouding in systemen*	
15	Werking van wijzigingsbeleid optimaliseren	

Heel goed! Bedoel je hier ook IAM mee? En processen en owner(s)?

5.1.2e
12/05/2024 10:06
Resolved

Ja, klopt.

5.1.2e
12/16/2024 17:21
Resolved

provincie Gelderland

	Focus op nieuwe leveranciers en samenwerking ertussen														
16	Publicatie en actualiseren van IB-richtlijnen op beleidsportaal														
17	Samenvoegen bestaande richtlijnen met IB-richtlijnen ISO27001 - Zoals deze bestaan op beleidsportaal														
18	Business Continuity Management (BCM) opzetten														
19	Beleid leveranciersmanagement operationaliseren														
	Regulier uit te voeren security taken														
20	Reguliere overleggen														
21	Reguliere rapportagechecks (per mail)														
22	Risicoanalyses *Uiteindelijk wordt Jurgen de owner*														
23	Auditvoorbereidingen (intern/extern) *Uiteindelijk wordt* 5.1.2e *de owner*														
24	SCC registratie - Bewijslast; - Incidenten; - IB-richtlijnen; - Etc.														
25	SCC rapportage - Jaarplan directie / forum - Etc.														

5.1.2e

5 Rollen en bijbehorende taken/verantwoordelijkheden

Onderstaande beschrijvingen van taken en verantwoordelijkheden zijn per september 2024 besproken met het security team en 5.1.2e de teamleider van I&A – Regie. We hebben afgesproken om met deze rolverdeling te starten; deze is nog veranderlijk afhankelijk van de verdere ontwikkeling van het security team.

5.1 CISO 5.1.2e

- Strategische sturing (richten)
  - Verantwoordelijk voor opstellen van (meer)jaarlijkse roadmap met securityactiviteiten voor het komende jaar, o.b.v. risicoanalyse
  - Verantwoordelijk voor opstellen van securitydoelen (visiedocument) met uitgangspunten waaraan PG aan moet voldoen.
- Contacten met bestuur en directie en key-leveranciers (bijvoorbeeld Proxsys t.b.v. NIS2)
- Interprovinciale vertegenwoordiging
- Crisismanagement
- Awarenesstrainingen geven

5.2 ISO – techniek 5.1.2e

- Tactische sturing (inrichten)
- Azure Governance met aandachtsgebied security
  - Technische inrichting van het Azure security dashboard, policies en excepties – o.b.v. beleid en procedures
  - Periodiek rapporteren over de gedefinieerde KPI's aan de hand van statistieken / handmatige controls o.b.v. beleid / procedures en adviseren waar nodig
  - Opstellen en afstemmen verandervoorstellen/verbeteringen Azure/MS365 security
  - (Keuzes tevens afstemmen met het architectuurteam)
- Opstellen plan en uitvoering van (IT-)auditaanbevelingen met betrekking tot security
- Uitvoering van activiteiten zoals beschreven in het security jaarplan (owner van producten)
- Verdere ontwikkeling van het interne ISMS:
  - Doorvoeren van security maatregelen in de operatie van de organisatie
  - Bijhouden van ISMS-tool (SCC)
  - Waarborgen van navolgbaarheid beleid – procedure – acties (vastlegging) – monitoring t.b.v. audit
  - o.b.v. nieuwe ontwikkelingen BIO(2), NIS2, overig – fit-gap analyse
- Verhogen awareness binnen PG
- FB MS365 ondersteunen met security-inrichting en afspraken
  - Afstemmen met FB365 (verandervoorstellen/verbeteringen)
  - Afstemmen met MSSP specifiek voor MS365-security

5.3 ISO – proces 5.1.2e

- Operationele sturing (verrichten)
- Regie MSSP
  - Behandelen van operationele securityvraagstukken.
  - Leveranciersmanagement - monitoren van KPI's MSSP aan de hand van afgesproken securitymaatregelen en adviseren waar nodig (bijhouden van dashboard)
- Uitvoering van activiteiten zoals beschreven in het security jaarplan (owner van producten).
- (Mede)voorbereiden en registreren van risicoanalyses zoals bepaald in SCC
- (Mede)voorbereiden en registreren van audits zoals bepaald in SCC
- (Mede)voorbereiden van BCP (Business Continuïteit Plan) zoals bepaald in SCC
- Overige verbeteringen voorstellen en/of doorvoeren zoals bepaald in SCC

- Verdere ontwikkeling van het interne ISMS.
    - Doorvoeren van security maatregelen in de operatie van de organisatie o.b.v. risicoanalyse
    - Bijhouden van ISMS-tool (SCC)
    - Waarborgen van navolgbaarheid beleid – procedure – acties (vastlegging) – monitoring t.b.v. audit
    - o.b.v. nieuwe ontwikkelingen BIO(2), NIS2, overig – fit-gap analyse
- Verhogen awareness binnen PG