Intern toezichtplan 2025

- Verbijzonderde Interne Controle (VIC)
- Gegevensbescherming (FG)
- Informatiebeveiliging (CISO)

14 november 2024

Gemeente Meppel

Inhoudsopgave

Documentbeheer

Beheer informatie	
Document of registratie	Toezicht plan 2025
Bewaartermijn	Geen wettelijke grondslag
Classificatie	Intern vertrouwelijk

Versiebeheer			
Versie	Datum	Auteur	Opmerkingen
0.1	31-07-2024	CISO/VIC R. Tollenaar	Eerste idee
0.2	09-09-2024	VIC G. Aukema	Detaillering VIC
0.3	07-10-2024	CC, CISO, FG, VIC, CZ	Nadere detaillering
0.4	09-10-2024	CISO/VIC R. Tollenaar	Een aantal aanpassingen doorgevoerd
0.5	21-10-2024	CISO/VIC R. Tollenaar	Hoofdstuk 4 inhoudelijk verbeterd
0.6	23-10-2024	Solisten gezamenlijk	Finetunen, voorstellen TM verwerkt
0.7	08-11-2024	CISO/VIC R. Tollenaar	Laatste verbeterpunten vanuit TM
0.8	14-11-2024	CISO/VIC R. Tollenaar	Laatste verbeterpunten vanuit Directie

Distributielijst		
Versie	Datum	Verspreid aan
0.1	31-07-2024	Alle solisten
0.2-5	--	Alle solisten via Teams (continue proces)
0.6	23-10-2023	Alle solisten + TM
0.7	13-11-2024	Directie
0.8	-	Leden van het Managementoverleg Meppel
0.8	03-12-2024	College, ter vaststelling

Eigenaar			
Versie	Datum	Eigenaar	Herziening Ja/Nee
concepten	Divers	Team B&O	Nee

Intern toezichtplan 2025

1. Algemeen

1.1 Inleiding

Dit is het gemeenschappelijke toezichtplan voor 2025 van de:

- Verbijzonderde Interne Controle (VIC)
- Functionaris Gegevensbescherming (FG)
- Chief Information Security Officer (CISO)

1.2 Managementsamenvatting

Voor 2025 is er een gezamenlijk intern toezichtplan opgesteld voor de onderwerpen Verbijzonderde Interne Controle (VIC), Gegevensbescherming (FG) en informatiebeveiliging (CISO). De plannen zijn in 2025 samengevoegd omdat veel uitgangspunten voor de controles gelijk zijn, maar ook om het besluitvormingsproces te vereenvoudigen. Door deze geïntegreerde aanpak wordt de efficiëntie verhoogd en de samenhang tussen de verschillende toezichtactiviteiten versterkt Dit gezamenlijke plan biedt een overzicht van alle toezichtactiviteiten en maakt inzichtelijk waar we op toezien, waarom en wanneer. De focus van de toezichtactiviteiten voor 2025: de rechtmatigheidsverantwoording en compliancy op wet- en regelgeving blijven de belangrijkste uitgangspunten.

1.3 Leeswijzer

In het eerste hoofdstuk worden de gemeenschappelijke uitgangspunten en doelstellingen beschreven die gelden voor alle drie de toezichtgebieden. Dit hoofdstuk legt de basis voor de specifieke controles en verantwoordelijkheden die in de daaropvolgende hoofdstukken worden besproken.

Hoofdstuk twee richt zich op de Verbijzonderde Interne Controle en beschrijft de methoden en processen voor financiële en operationele controles.

Hoofdstuk drie behandelt het toezicht op de bescherming van persoonsgegevens.

Hoofdstuk vier behandelt het toezicht op informatiebeveiliging.

1.4 Doelstelling

De doelstelling van dit toezichtplan is het:

- Op transparante wijze uitvoeren van intern toezicht door de FG, CISO en VIC.
- Efficiënt uitvoeren van intern toezicht en de rapportage hierover door samenwerking van de FG, CISO en VIC.

1.5 Scope

Dit toezichtplan richt zich op het waarborgen van de naleving van regelgeving. Dit omvat de volgende gebieden:

- Regelgeving en Compliance: Toezicht op de naleving van wet- en regelgeving, bijvoorbeeld de AVG.
- Informatiebeveiliging: Beoordeling en verbetering van de beveiligingsmaatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen.
- Interne Controle: Evaluatie van de effectiviteit van processen en interne beheersmaatregelen om (fraude)risico's te minimaliseren en operationele efficiëntie te bevorderen.

1.6 Invloedrijke documenten en programma's

Bij het opstellen van dit toezichtplan zijn diverse documenten en programma's van invloed geweest. De Visie op Control van de gemeente Meppel vormt de basis, waarbij de principes van het Three Lines of Defense model centraal staan. Daarnaast zijn de volgende stukken meegenomen:

- Normenkader voor 2025, geoperationaliseerd in toetsingskaders per proces
- Coalitieakkoord 2022-2025
- Programmabegroting voor 2025
- Organisatievisie Koers en de evaluatie daarvan

1.7 Ontwikkelingen

Naast het wettelijke kader worden ook algemene ontwikkelingen meegenomen in het toezicht. Deze ontwikkelingen kunnen leiden tot aanvullend toezicht of aanpassingen in het normen/toetsingskader. Ontwikkelingen kunnen een leiden tot een verhoogd of verlaagd risico.

Voor 2025 zijn de volgende relevante (maatschappelijke) ontwikkelingen geïdentificeerd:

- Verbreding en verdieping van de rechtmatigheidsverantwoording
- Steeds bredere digitalisering en toename van cyberdreigingen
- Meer toezichtverplichtingen op informatiebeveiliging en gegevensbescherming
- Aanhoudende risico's van interne fraude en onrechtmatigheden

- Continue veranderingen in wet- en regelgeving
- Toekomstige invloed van kunstmatige intelligentie
- Verloop van personeel
- Aantal gemeentelijke taken en initiatieven (tot samenwerking) neemt toe

1.8 Risico's

Op basis van de genoemde ontwikkelingen kunnen de volgende algemene (verhoogde of verlaagde) risico's worden onderkend:

- Wet- en Regelgeving: Continue veranderingen in wet- en regelgeving kunnen leiden tot nalevingsrisico's als de organisatie zich niet snel genoeg aanpast aan nieuwe eisen.
- Rechtmatigheidsverantwoording: Het risico dat de organisatie niet volledig voldoet aan de vereisten voor rechtmatigheidsverantwoording. Met name op het moment dat tussentijds regelgeving hieromtrent veranderd. Dit kan leiden tot juridische en financiële consequenties.
- Cyberdreigingen: De toenemende digitalisering brengt een hoger risico op cyberaanvallen en datalekken met zich mee, wat de vertrouwelijkheid, integriteit en beschikbaarheid van informatie kan aantasten.
- Informatiebeveiliging en Gegevensbescherming: Verhoogde toezichtverplichtingen kunnen leiden tot nalevingsrisico's als de organisatie niet tijdig en adequaat reageert op nieuwe regelgeving.
- Interne Fraude en Onrechtmatigheden: Aanhoudende risico's van interne fraude en onrechtmatigheden kunnen de integriteit en reputatie van de organisatie schaden en financiële verliezen veroorzaken.
- Kunstmatige Intelligentie: Het gebruik van kunstmatige intelligentie kan ethische en operationele risico's met zich meebrengen, zoals discriminatie in algoritmen en daarmee in besluitvorming.
- Personeelsverloop: verloop van personeel kunnen leiden tot kennisverlies en operationele inefficiënties.
- Samenwerkingen: Het aantal samenwerkingen en varianten neemt toe. De gemeentelijke verantwoordelijkheden moeten hierbij goed worden afgehecht

1.9 Normenkader

Het normenkader van een gemeente is een lijst met van toepassing zijnde wet- en regelgeving en vormt de basis voor alle controles en audits binnen de organisatie. Dit kader wordt vastgesteld door de gemeenteraad en dient als richtlijn voor het naleven van wet- en regelgeving, beleidsdoelstellingen en interne procedures. Het normenkader omvat een verzameling van normen en criteria waaraan de gemeentelijke processen en activiteiten moeten voldoen. Deze normen zijn essentieel voor het waarborgen van transparantie, rechtmatigheid en doelmatigheid in het gemeentelijk bestuur en handelen.

1.10 Toetsingskader

Een toetsingskader is het toegepaste normenkader voor 1 proces en bestaat uit een set gedetailleerde criteria en methoden die worden gebruikt om per proces te beoordelen of aan de normen en richtlijnen wordt voldaan. Het biedt een systematische manier om de naleving en effectiviteit van de geïmplementeerde normen te evalueren. Door middel van audits, monitoring naar ook beoordelingen en bijbehorende evaluaties helpt het toetsingskader bij het identificeren van verbeterpunten en het waarborgen van de kwaliteit en consistentie van processen en systemen binnen onze organisatie.

1.11 Toezichtproces & rapportage

Binnen de gemeente is in 2021 het document Visie op control in 2021 vastgesteld, met als doel duidelijkheid te verkrijgen over de manier waarop we ín “control” willen zijn, vanuit een basis die op orde is, met als belangrijkste effecten:

- Gemeente en samenwerkingspartners elkaar goed verstaan en daaruit voortgekomen afspraken betrouwbaar worden nagekomen.
- Klachten tot een minimum beperkt blijven en dat deze tenminste ordentelijk worden afgedaan.
- Er sprake is van eenduidige communicatie en informatievoorziening.
- De tevredenheid over de dienstverlening goed is.
- Om risico’s effectief te beheren en in-control te zijn, maken we gebruik van het “Three Lines of Defence” model.

Three lines of defence		
Lines of defence	Verantwoordelijkheid	Omschrijving
1	Eerste lijn	Professional in uitvoering is verantwoordelijk voor de organisatie en realisatie van zijn/ haar eigen doelstellingen. En wordt hierin ondersteund vanuit de 2de lijn.
2	Tweede lijn	Realiseren van doelstellingen en de wijze waarop de middelen worden ingezet, alsmede op de borging dat dit plaatsvindt binnen daartoe geldende regelgeving (doeltreffend, doelmatig en rechtmatig)
3	Derde Lijn	VIC (auditfunctie). Toetst in hoeverre het samenspel tussen de 0de, 1ste en 2de lijn functioneert. Deze functie opereert onafhankelijk en staat buiten de ‘lijn’.

Tabel 1: Three lines of Defence

De derde lijn is in Meppel belegd bij het Team Bestuur en Organisatie. De functionarissen van de verbijzonderde Interne Controle, de FG en CISO zijn verantwoordelijk voor de uitvoering van de toezichtstaken, ieder in het eigen expertisegebied, maar waar mogelijk ook gezamenlijk vanuit een efficiency oogpunt.

Deze derde lijn rapporteert rechtstreeks aan Directie en/of College. Dit zorgt ervoor dat bevindingen en aanbevelingen altijd onafhankelijk en objectief zijn. Met deze aanbevelingen kan de Directie risico's mitigeren of bedrijfsprocessen laten verbeteren

De rapportage methodiek volgt ook de principes van het Three Lines of Defence model.
Dit betekent dat de bevindingen achtereenvolgens gedeeld worden met:

- De professional, medewerker of cluster waar de toezichttaak is uitgevoerd.
  Dit zorgt ervoor dat de medewerkers van het team altijd de kans krijgen om feedback te geven op zowel de bevindingen als op de adviezen
- De teammanager, inclusief verzoek voor fysieke bespreking.
  Hiermee informeren wij de leidinggevende over de bevindingen en kunnen eventuele aanvullende acties van de teammanager vastgelegd worden.
- De directie, maar enkel die vanuit een risicoperspectief significant zijn.
  Vanuit een efficiency optiek, worden alle bevindingen van de VIC, FG en CISO in drie 4-maandelijkse rapportages aangeboden aan de directie.

NB: Zeer significante bevindingen, bijvoorbeeld bij overtreding van wet- en regelgeving, een rechtmatigheidsoptiek of gevolgen voor de politieke leiding zullen altijd zonder vertraging rechtstreeks gemeld worden aan de Directie en/of het College.

2. Verbijzonderde Interne Controle

2.1 Algemeen

De Verbijzonderde Interne Controle stelt de organisatie onder meer in staat om inzicht te verkrijgen in de rechtmatige totstandkoming van baten, lasten en balansmutaties in de jaarrekening. Dit gebeurt door het opzetten, bestaan en de werking van relevante beheersmaatregelen en het beoordelen van risico's voor rechtmatigheid en getrouwheid te onderzoeken.

De VIC is gericht op processen met de grootste financiële en maatschappelijke risico's en is bedoeld om foutgevoelige (financiële) processen te identificeren en de gekoppelde risico's te beperken.

Dit doet de VIC door op de significante processen een audit uit te voeren met de volgende stappen:

- Actualiseren normenkader en toetsingskader;
- Actualiseren procesbeschrijving en evt. extra aandachtspunten;
- Opvragen bronbestanden van de populatie;
- Identificeren afwijkingen en trekken aselecte steekproef;
- Uitvoeren lijncontrole op 1 en uitvoeren dossiercontrole op geselecteerde dossiers;
- Omzetten bevindingen naar percentages en actualiseren aanbevelingen;
- Rapporteren uitkomsten van de procesaudit aan teammanager en
- Rapporteren samenvatting aan directie (incl. centraal aanbevelingenbestand).

2.2 Factoren van invloed

Er zijn een aantal belangrijk factoren van invloed op de planning van de werkzaamheden van de Verbijzonderde Interne Controle, denk hierbij aan:

- Resultaten van eerdere procesaudits,
- Aanbevelingen Rapport van bevindingen bij Jaarverslag 2023,
- Aanbevelingen uit voorbespreking nieuwe accountant 2024,
- Aanbevelingen Managementletter Interim Controle 2024 en
- Vraagstukken vanuit Directie, College of Raad in 2024.

2.3 Bijzondere toezichtpunten voor 2025

- Uitbreiden 2de lijnscontrole Wmo en JW
- Opstellen procesbeschrijving/audit Begrotingswijziging
- Opstellen procesbeschrijving/audit Verbonden partijen
- Gezamenlijke audit op JW en PW (Wmo in 2024 gestart)

2.4 Jaarplanning

In onderstaande tabel wordt de jaarplanning weergegeven van de VIC. De te controleren processen zijn afgestemd met de accountant als de processen met financiële impact (voor de RMV. De controles kunnen worden uitgebreid met processen die de organisatie van belang acht (relevant).

Onderaan zijn nog drie algemene zaken opgenomen, die jaarlijks plaatsvinden.

Dit betreft m.n. het toezicht op:

- De Opzet van de processen, via een procesbeschrijving
- Het daadwerkelijke Bestaan, via een lijncontrole en
- De Werking van processen, via steekproef en dossiercontroles in 4 kwartalen.

									2025	2026		
Opzet, bestaan en werking van:	Apr	Mei	Juni	Juli	Aug	Sep	Okt	Nov	Dec	Jan	Feb	Mrt
Aanbestedingen		OB			W12						W34	
Belastingen / kwijting		OB			W12						W34	
Grondexploitatie, verkoop		OB			W12						W34	
Inkoop		OB			W12						W34	
Omgevingsvergunningen			OB		W12						W34	
Personeel			OB		W12						W34	
Schouwburg			OB		W12						W34	
Subsidie-uit (groot, klein)			OB		W12						W34	
Verhuur			OB		W12						W34	
Begrotingswijziging		OB	W1		W2			W3			W4	
Betalingsverkeer		OB			W12			W34				
SD Jeugdwet		OB	W1		W2			W3			W4	
SD Participatiewet		OB	W1		W2			W3			W4	
SD PGB (JW+Wmo)		OB	W1		W2			W3			W4	
SD Wmo		OB	W1		W2			W3			W4	
Verbonden partijen / GR		OB			W12						W34	

Tabel 2: Werkplanning cluster VIC

3. Gegevensbescherming (FG)

3.1 Algemeen

De functionaris gegevensbescherming (FG) houdt toezicht op privacywetgeving de AVG en Wpg. De uitvoering van de FG-functie is belegd bij het externe adviesbureau L2P. De FG is principieel onafhankelijk, maar coördineert zijn toezicht in overleg met de teammanager B&O, in nauwe samenwerking met de VIC, CISO en PO van de gemeente.

3.2 Factoren van invloed

- AVG Incidenten en Datalekken in 2024
- Berichten vanuit de Autoriteit Persoonsgegevens
- Bestuurlijke of organisatorische AVG-vraagstukken vanuit Directie, College of Raad.

3.3 Bijzondere toezichtpunten voor 2025

In oktober 2024 heeft de Autoriteit Persoonsgegevens trends en ontwikkelingen op privacy gebied in kaart gebracht die spelen bij de overheid.1 Deze trends en ontwikkelingen neemt de FG mee voor het toezicht in 2025. Specifiek gaat het om:

- Zonder grondslag delen van gegevens in het sociaal domein, zorgdomein en het veiligheidsdomein.
- Bestrijding van criminaliteit en het handhaven van de openbare orde.
- Gebruik van foto's voor vaststellen WOZ-waarde.
- Transparantie omtrent de verwerking van persoonsgegevens.

[1] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-signaleert-nog-altijd-privacyrisicos-bij-de-overheid

3.4 Jaarplanning

Hieronder vindt u de planning van de FG voor 2025, waarin de belangrijkste onderwerpen en toelichtingen per kwartaal worden weergegeven:

Planning FG 2025		
Kwartaal	Onderwerp	Toelichting
Q1	Awareness	Gemeente Meppel maakt gebruik van Sir Askalot om medewerkers bewust te maken van de risico's op het vlak van informatiebeveiliging en privacy
Q2	Toegangsautorisatie	Toegang tot gevoelige (persoons)gegevens is enkel toe gestaan indien dit noodzakelijk is. Wanneer dit noodzakelijk is wordt vastgelegd in een autorisatiematrix. De toezichtactie zal specifiek gericht zijn op het nieuwe zaaksysteem.
Q3	E-mailarchivering	In 2022 heeft de VNG een methode vastgesteld voor het bewaren of vernietigen van e-mailboxen: de capstone methode. Deze toezichtactie ziet op de naleving van deze methode.
Q4	Zorg- en veiligheidshuis	Op 1 januari 2025 treedt de Wet gegevensverwerking door samenwerkingsverbanden in werking. Deze wet heeft onder andere invloed op het Zorg- en Veiligheidshuis waar gemeente Meppel deelnemer van is. Deze toezichtactie ziet op de naleving van de gestelde eisen.

Tabel 3: Overzicht toezichtactiviteiten FG

Samenwerking VIC
In 2025 zal het normenkader van de VIC voor de Jeugdwet en Participatiewet aangepast worden zodat enkele normen vanuit de AVG worden onderzocht door de VIC. De FG zal hierbij ondersteunen waar nodig. Qua planning wordt het schema van de VIC gehanteerd.

Samenwerking CISO
In 2025 gaat de FG gezamenlijk onderzoek doen met de CISO op het vlak van awareness (Q1 2025) en de autorisatie van het (nieuwe) zaaksysteem (Q2 2025).

4. Informatiebeveiliging

4.1 Algemeen

In dit hoofdstuk is beschreven op welke wijze er uitvoering wordt gegeven aan toezichtfunctie door de CISO. De focus van het toezicht is in 2025 gericht op:

- Risico & Bedrijfscontinuiteit
- BIO Compliancy & ENSIA
- Veiligheidsbewustzijn

4.2 Specifieke richtlijnen & wetgeving

- Baseline Informatiebeveiliging Overheid (BIO1.04)
- EU Network and Information Security 2(NIS2) (vanaf medio 2025)
- Cyberbeveiligingswet (Cbw) (vanaf medio 2025)
- Baseline Informatiebeveiliging Overheid 2.0 (vanaf medio 2025)

4.3 Toetsingskaders voor 2025

In een steeds digitaler wordende wereld is het waarborgen van informatiebeveiliging van cruciaal belang voor gemeenten. Een gedegen toetsingskader is essentieel om de beveiligingsmaatregelen objectief en effectief te evalueren en te verbeteren. De Chief Information Security Officer (CISO) maakt gebruik van verschillende toetsingskaders om toezicht te houden op de borging van informatiebeveiliging. De belangrijkste kaders die hierbij worden gehanteerd zijn:

- NEN-ISO/IEC 27001: Een wereldwijd erkende standaard die richtlijnen biedt voor het opzetten, implementeren, onderhouden en continu verbeteren van een Information Security Management System (ISMS).
- NEN-ISO/IEC 27002: Richtlijnen voor informatiebeveiligingsmaatregelen, die gedetailleerde controles en best practices bieden voor het implementeren van informatiebeveiliging.
- ITIL: Een gestructureerd raamwerk voor het optimaliseren van IT-processen, waardoor organisaties efficiënter en klantgerichter kunnen opereren.
- ENSIA: Het Eenduidig Normenkader Single Information Audit, dat gemeenten helpt bij het uniform en efficiënt uitvoeren van informatiebeveiligingsaudits.
- Toetsingskader Wet Politie Gegevens (WPG) : Specifieke richtlijnen en eisen voor de beveiliging van politiegegevens, zoals opgesteld door de Nederlandse Orde van Register EDP-Auditors (Norea), gebaseerd op specifieke Nederlandse wetgeving.
- Informatiebeveiligingsbeleid Meppel 2023

4.4 Factoren van invloed

Bij het opstellen van dit plan zijn ook andere informatiebronnen geraadpleegd voor dit plan, deze bronnen zijn:

- Adviesrapport PSA accountants met resultaten Pre-audit ENSIA over 2024
- Managementletter van ETL accountants vwb IT-Controls 2024
- Dashboard Informatiebeveiligingsbewustzijn Recourse (Sir Askalot)

4.5 Bijzondere toezichtpunten voor 2025

- Informatiebeveiligingsbewustzijn: Het is noodzakelijk om ook in 2025 toezicht te blijven houden op informatiebeveiligingsbewustzijn. Omdat het toezicht vanuit de lijnorganisatie nog verbeterd moet worden. Dit voorkomt dat de deelname aan trainingen verwatert en waarborgt een hoog niveau van beveiligingsbewustzijn binnen de organisatie.
- Business Continuity Management: Een van de belangrijkste actiepunten voor 2024 is business continuïty management (noodplannen). We moeten continu toezicht houden op de verbetering hiervan, omdat er binnen de gemeente Meppel geen gestructureerde en samenhangende plannen zijn op dit gebied. Dit is cruciaal om de werking van kritische bedrijfsprocessen te waarborgen en de dienstverlening aan de inwoners van Meppel te garanderen. Hierdoor voorkomen we kwetsbaarheden bij verstoringen en zorgen we ervoor dat essentiële diensten altijd beschikbaar blijven.
- Autorisatiematrixen: Sommige autorisatiematrixen binnen de gemeente Meppel zijn nog niet aangepast op het “need to know” principe, zoals beschreven in het informatiebeveiligingsbeleid. We moeten actief toezicht houden op de verbetering hiervan, zodat alleen medewerkers met een directe noodzaak toegang hebben tot specifieke informatie. Dit versterkt de informatiebeveiliging, minimaliseert het risico op ongeautoriseerde toegang en beschermt gevoelige gegevens, wat essentieel is voor de continuïteit van onze diensten.
- Procesvolwassenheid: De procesvolwassenheid van incidentmanagement binnen de gemeente Meppel vereist voortdurende aandacht en verbetering. We moeten actieftoezicht houden op de ontwikkeling en implementatie van incidentmanagementprocessen. Dit zorgt ervoor dat incidenten effectief worden geïdentificeerd, geregistreerd, geanalyseerd en opgelost. Hierdoor verhogen we de responsiviteit en efficiëntie bij incidenten, minimaliseren we de impact op de dienstverlening en waarborgen we de continuïteit van onze kritische processen.
- NIS2 en Cbw: De NIS2-richtlijn is in Oktober 2024 van kracht geworden en in 2025 zal de Cbw van kracht worden. De voorbereidingen en veranderingen als gevolg hiervan moeten grotendeels in 2025 plaatsvinden. Door deze veranderingen op te nemen in het informatiebeveiligingsplan 2025 kan hierop ook op toegezien kan worden.
- BIO2.0: Hoewel de BIO2-richtlijn pas in 2025 actueel wordt voor de gemeente Meppel, moeten we nu al actief toezicht houden op de voorbereiding en implementatie hiervan: De BIO2-richtlijn is nauw verbonden met de ISO 27001 en ISO 27002 standaarden, die richtlijnen bieden voor het opzetten, implementeren, onderhouden en continu verbeteren van een Information Security Management

System (ISMS). ISO 27001 biedt een raamwerk voor risicobeheer en beveiligingsmaatregelen, terwijl ISO 27002 gedetailleerde controles en best-practices biedt voor het implementeren van informatiebeveiliging. Door deze standaarden te integreren in onze aanpak, versterken we onze informatiebeveiliging en zorgen we voor een gestructureerde en samenhangende implementatie van de BIO2-richtlijn

4.6 Planning van toezichtactiviteiten

Hieronder vindt u de planning voor de belangrijkste onderwerpen en activiteiten op het gebied van informatiebeveiliging voor het komende jaar. De tabel geeft een overzicht van de specifieke acties en de maanden waarin deze gepland staan:

Onderwerpen	Jan	Feb	Mrt	Apr	Mei	Jun	Jul	Aug	Sep	Okt	Nov	Dec
Wetgeving & Richtlijnen									X			
Risicobijstelling	*Dit is feitelijk een continu proces*											
Informatiebeveiligingsbeleid							X					
Informatiebeveiligingsplan							X					
Bewustwording			X			X			X			X
Business Continuïteit												
Penetratietesten				X								
Phising testen		?							?			
(Cyber) oefenen	B&R			Uitwijk			B&R					
Autorisaties Essentiële	SSD		Motion		Key2F	Zaak-	DigiD	Suwinet	Leef-		BRP	
In-, door en uitstroom		VOG								VOG		
Incident management proces		X			X			X			X	
Change management proces	X			X			X			X		
Vulnerability Management			X			X			X			X
Clear Screen. Clear Desk	X											
Toegangsbeleid				Logisch					Fysiek			
ENSIA									Coördinatie			
WPG (interne Audit functie)			X							X		
SLA + Rapportage				X					X			

Tabel 4: Toezichtactiviteiten CISO voor 2025

Deze pagina is bewust leeg (template)