



centrum informatiebeveiliging
en privacybescherming



Baseline
Informatiebeveiliging
Overheid

BIO2: een hoger IB volwassenheidsniveau voor de hele overheid

Kees Hintzbergen

PvIB 09 december 2025

Wie ben ik

BIO

Werkzaam voor IBD en CIP, vanavond voor CIP

2012 BIG

2016 BIR 2017

2018 BIO

2022 BIO2

Secretaris werkgroep BIO en kern-IBO



Procedure

2x eerder PvlB

- BIO1
- Nut van Baselines

Deze beide onderwerpen ga ik vandaag niet behandelen!

Vragen aan het einde van mijn presentatie

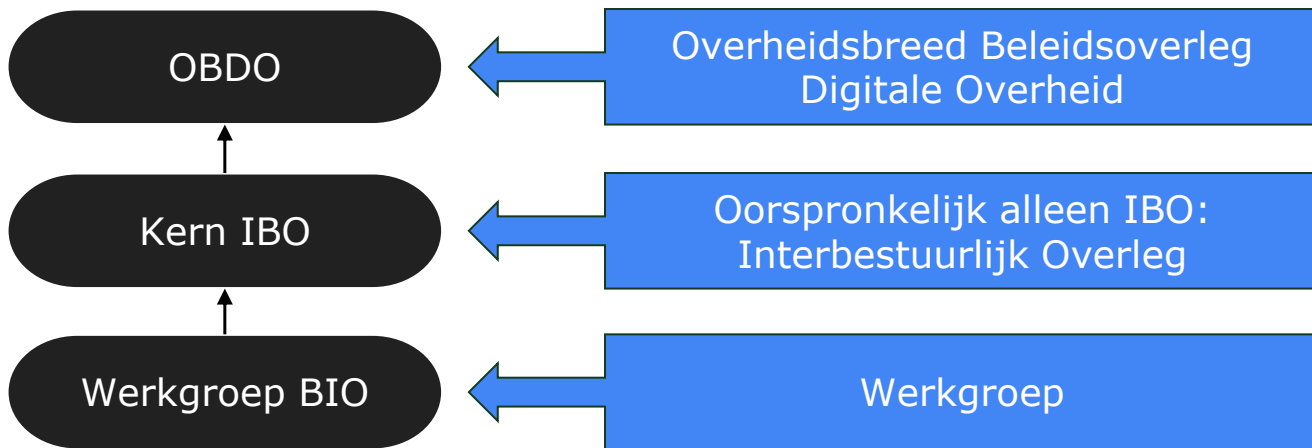
Inhoud

- Waar komen we vandaan
- Wat is de BIO2
- Belangrijkste wijzigingen
- Risicomanagement - ISMS
- Governance - Maatregelen
- Cbw en verplichtende zelfregulering
- Beschikbaarheid en onderhoud
- Ondersteuningsprogramma

Waar komen we vandaan

In de beginjaren: BIR, BIG, BIWA, IBI

- Onderlinge verschillen aanwezig
- Gezamenlijke wens om tot een BIO te komen



Wat is de BIO2?

Overheidsbrede baseline informatiebeveiliging

- Aanpak en “lijstje”
- 100% ISO 27001/27002
- Versterken van de informatieveiligheid door risicogestuurd werken
- Nadruk op governance, leiderschap en ketenveiligheid
- Verankerd de zorgplicht uit de Cbw
- Vraagt expliciet motivatie, risicoafweging en PDCA-bewijs

Belangrijke wijzigingen

De Baseline Informatiebeveiliging Overheid (BIO2) legt essentiële verplichtingen op aan overheidsorganisaties voor een robuust beveiligingsniveau.



Toepassen ISO-normen

- Overheidsorganisaties moeten **NEN-EN-ISO/IEC 27001** toepassen. Dit omvat het vaststellen, implementeren en bijhouden van een ISMS
- ISO/IEC 27002 en BIO-overheidsmaatregelen voor beheersmaatregelen



Aantoonbaarheid

- Organisaties moeten aantoonbaar beveiligingsmaatregelen implementeren in **opzet, bestaan en werking**
- Deze eis vloeit voort uit de Cyberbeveiligingswet (Cbw)
- Aantonen: self-assessments, audits en pentesten, verslaglegging

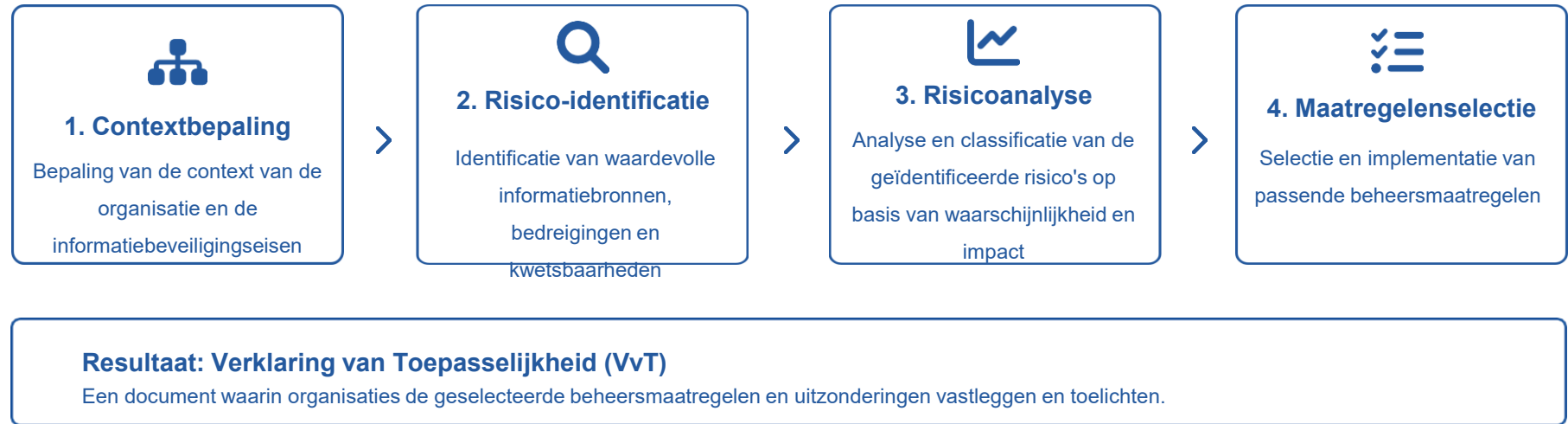


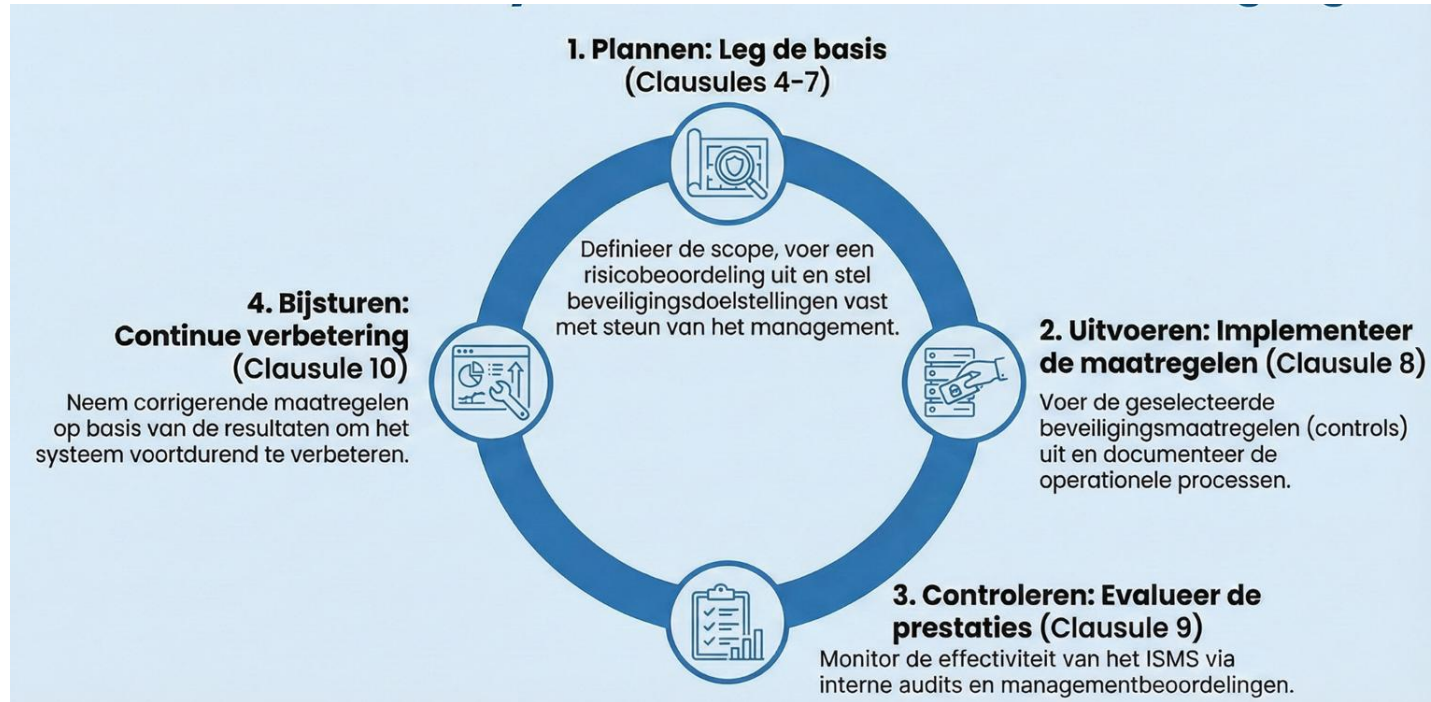
Minimale invulling

- De BIO-opgenomen maatregelen vormen de **minimale invulling**
- Risicoanalyse om te bepalen of de BIO2 voldoende is
- Afwijkingen moeten worden onderbouwd met een risicoanalyse

Risico management

Het risicomanagementproces binnen de BIO





ISO 27001 verplicht toepassen voor managementsysteem

Verklaring van toepasselijkheid (VvT)

Belang voor leveranciers en andere sectoren



- Niet rechtstreeks van toepassing
- Expliciete eisen voor beveiliging in de keten
- De relevantie voor leveranciers komt voort uit de contractuele verplichtingen die overheidsorganisaties moeten opleggen om hun eigen zorgplicht voor informatiebeveiliging te waarborgen
- De leverancier is verantwoordelijk voor het borgen van de gestelde eisen bij zijn toeleveranciers

Governance



- Bestuurder
- Lijn management
- CISO
- Interne toezichthouder
- Leveranciers

Maatregelen

- Beheersmaatregelen uit de ISO standaard risico gedreven toepassen
- Overheidsmaatregelen als minimale verplichte invulling
- Aanvullend maatregelen treffen bij hoger risico
- Gebruik van andere standaarden als de CSIR en NEN7510

Cbw en de BIO2



- BIO2 als zorgplicht
- Onderdeel van de ministeriële regelingen van BZK en IenW
 - BIO2 concept versie 1.3 bijgevoegd bij de internetconsultatie (loopt tot 21 december)
- 3 maatregelen uitgezonderd (grijs gemarkeerd) vanwege scope Cbw: beveiliging netwerk- en informatiesystemen
- Cbw in Q2 2026 in werking
- Toezicht RDI en ILT

Verplichtende zelfregulering



- Tot de Cbw is de BIO2 versie 1.2 verplichtende zelfregulering voor provincies en waterschappen en het Rijk.
- Richtinggevend kader voor de gemeenten.
- De drie uitgezonderde maatregelen blijven verplichtende zelfregulering.
- Ook blijft de BIO2 verplichtende zelfregulering voor overheidsorganisaties die zijn uitgezonderd van de Cbw.

Hoe is de BIO2 beschikbaar?

- BIO2 als PDF versie 1.2 (publicatie september 2025)
- BIO2 in Excel met was-word-lijst
- BIO-SA
- Veelgestelde vragen
- Deel 3

www.bio-overheid.nl

Onderhoud en beheer

- Overheidsbreed
 - Werkgroep BIO
 - Kern-IBO voor de besluitvorming
- GitHub
- Wijzigingsverzoeken
- 2026 grootschalige evaluatie van de BIO2, nieuwe versie 2027

Samen aan de slag!



Maand	Thema	Centrale vragen
September & oktober 2025	Publicatie van de BIO2	Wat is de BIO2? Wat zijn de verplichtingen? Is er ondersteuning?
November 2025	Information Security Management System (ISMS)	Hoe richt je een basis-ISMS in conform ISO 27001?
December 2025	Risicomanagement binnen de Cbw/BIO2	Focus op risicomanagement en hoe verhoudt dit zich tot toezicht/verantwoording?
Januari 2026	Bestuur en organisatie meenemen	Hoe betrek en activeer je als CISO het bestuur?
Februari 2026	Operationele technologie (OT), ook wel OT-security en de Cbw/BIO2	Aan de slag met OT-security. En specifiek voor waterschappen: welke rol speelt de CSIR?
Maart 2026	Leveranciersmanagement en de Cbw/BIO2	Hoe borg je informatiebeveiliging in samenwerking met leveranciers?

Samen aan de slag!

- Bestuurder aan zet
- Update ICO wizard
- Quicksan

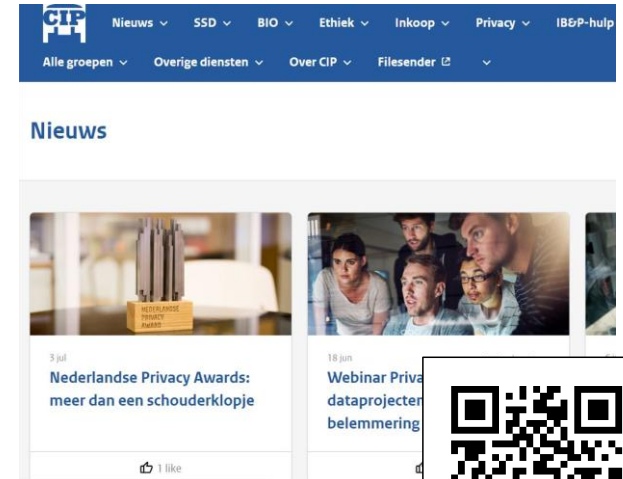
Meer informatie

BIO

BIO-website



CIP-community



Meer informatie



Voor allen, door allen!



© Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-NietCommercieel-GeenAfgeleideWerken 4.0 Internationaal (CC BY-NC-ND 4.0) verleend. Voor meer informatie zie: <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.nl>.