BASELINE INFORMATIEBEVEILIGING OVERHEID 2

BIO 2

24 september 2025, versie 1.2 definitief

BIO | Baseline Informatiebeveiliging Overheid

Rijksoverheid

VNG

ip Interprovinciaal Overleg
van, voor en door provincies

UNIE VAN WATERSCHAPPEN

Copyright-notitie

De Baseline Informatiebeveiliging Overheid 2 (BIO2) is geheel gestructureerd volgens NEN-EN-ISO/IEC 27001, bijlage A en NEN-EN-ISO/IEC 27002. Forum Standaardisatie heeft deze normen opgenomen in de 'pas-toe-of-leg-uit'-lijst met verplichte standaarden voor de publieke sector, volgens het pas-toe-of-leg-uit principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen. De BIO2 beschrijft de invulling van de laatste versie van de NEN-EN-ISO/IEC 27001 en de NEN-EN-ISO/IEC 27002 voor de overheid. De BIO2 vervangt deze twee normen niet. In de BIO2 zijn alleen specifieke overheidsmaatregelen opgenomen. NEN-EN-ISO/IEC 27001 en NEN-EN-ISO/IEC 27002 beschrijven de details voor implementatie (richtlijnen) en eisen voor de procesinrichting (het ISMS uit NEN-EN-ISO/IEC 27001). Het volgen van ISO 27001 is verplicht voor het inrichten van het managementsysteem voor informatiebeveiliging. Daar waar de BIO2 niet expliciet iets voorschrijft, moeten beide ISO-documenten gebruikt worden om te komen tot een goede inrichting voor risicomanagement. De ISO-documenten geven dus de details voor de toepassing, die niet in de BIO2 zijn beschreven en die nodig blijven voor een goede implementatie van de BIO2. Het gebruik van NEN-EN-ISO/IEC-normen 27001 en 27002 in de BIO is auteursrechtelijk beschermd. Het gebruik van teksten uit deze normen in de BIO geschiedt met toestemming van het Nederlands Normalisatie Instituut. Voor meer informatie over de NEN en het gebruik van hun producten zie: www.nen.nl.

Wijzigingsbeheer

Versie	Datum	Wijziging	Door
1.0	05-03-2025	Eerste conceptversie met instemming van het kern-IBO.	BZK
1.1	28-03-2025		CIP
1.1.1	05-08-2025	Enkele aanpassingen, de kolom "draagt bij aan" consistentie, gelijktrekken GitHub-versie/Word-versie en Excel-versie, voor OBDO.	CIP
1.2	24-09-2025	Door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) vastgestelde versie inclusief nieuwe opmaak.	CIP

Dankwoord

Wij danken iedereen die direct of indirect heeft bijgedragen aan de totstandkoming van de BIO2. In willekeurige volgorde danken wij de vertegenwoordigers van de koepels (Vereniging van Nederlandse Gemeenten, Interprovinciaal Overleg en Unie van Waterschappen), Chief Information Security Officers (CISO's) van overheidsorganisaties, de Auditdienst Rijk (ADR), de Rijksinspectie Digitale Infrastructuur (RDI), medewerkers van ministeries, het Nationaal Cyber Security Centrum (NCSC), het Centrum Informatiebeveiliging en Privacybescherming (CIP), de informatiebeveiligingsdienst voor gemeenten (IBD), de leden van de werkgroep BIO, bestuurders en functionarissen van overheden en alle anderen die hebben bijgedragen.

CIP centrum informatiebeveiliging en privacybescherming

INHOUD

Deel 1 BIO2-kader 4

1. Leeswijzer 4

2. Doel van de BIO 4

3. Toepassing BIO 4

4. Verplichtingen BIO 5

5. Het managementsysteem voor informatiebeveiliging 6

6. Reikwijdte managementsysteem 6

7. Samenhang managementsystemen 6

8. Risicomanagement 6

9. Contextbepaling 7

10. Risico-identificatie 7

11. Risicoanalyse 7

12. Risicobehandeling en maatregelenselectie 7

13. Kiezen risicomanagementmethodiek 7

14. Verklaring van toepasselijkheid (VvT) 8

15. Monitoring en continue verbetering 8

16. Samenstelling overheidsmaatregelen 8

17. Continue ontwikkeling 8

18. Transparantie en verantwoording 8

19. Toezicht 9

20. Toepasselijke overige normen, wet- en regelgeving 9

21. Cyberbeveiligingswet (Cbw) 9

22. Governance 10

23. Leveranciers 11

24. Informatiebeveiligingsprincipes 11

25. Operationaliseren maatregelen/balans in de maatregelenset ..11

26. Treffen aanvullende maatregelen 11

27. Impact van risico's 11

28. Relatie BIO en andere onderwerpen 12

Deel 2 BIO–overheidsmaatregelen 13

DEEL 1 BIO2-KADER

De overheid vervult een essentiële rol in de samenleving door bij te dragen aan de democratische rechtsstaat en het bieden van diensten aan burgers en bedrijven. Deze verantwoordelijkheden vereisen een zorgvuldige omgang met informatie en gegevens. Om deel te kunnen nemen aan de samenleving moeten burgers en bedrijven informatie met de overheid delen, soms zelfs verplicht, en zijn zij afhankelijk van de overheid om informatie te ontvangen. De overheid heeft vanuit deze unieke rol de plicht om zorgvuldig om te gaan met deze informatie.

De Cyberbeveiligingswet (Cbw) verplicht organisaties in de sector 'Overheid' de BIO2 als voornaamste invulling van de zorgplicht.

1. Leeswijzer

De Baseline Informatiebeveiliging Overheid 2 (BIO2) is opgebouwd uit drie onderdelen:

- **Deel 1**: BIO2-kader - de context en het belang van informatiebeveiliging voor overheidsorganisaties, evenals de structuur en toepasselijkheid van de BIO.
- **Deel 2**: BIO-overheidsmaatregelen - verplichte maatregelen, gebaseerd op de internationale standaard zoals NEN-EN-ISO/IEC 27001, annex A, aangevuld met specifieke overheidseisen.
- **Deel 3**: Toelichting [in ontwikkeling] - praktische ondersteuning met extra toelichting of voorbeelden om overheidsmaatregelen effectief te implementeren via de website https://www.bio-overheid.nl.

Samen vormen deze onderdelen een compleet kader voor informatiebeveiliging binnen de overheid. Er worden voor de (ISO-)normen in dit document geen jaartallen gebruikt. Daar waar gerefereerd wordt aan een andere norm wordt de meest actuele versie bedoeld.

2. Doel van de BIO

De Baseline Informatiebeveiliging Overheid (BIO) is het verplichte normenkader voor informatiebeveiliging binnen alle overheidsorganisaties. Het biedt richtlijnen, algemene principes en verplichte overheidsmaatregelen voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen de overheid en haar ketens.

Het doel van de BIO is om de informatieveiligheid overheidsbreed op een gemeenschappelijk basisniveau te brengen en daardoor ook de ketenpartners een basis van vertrouwen te geven bij gegevensuitwisseling. De BIO-aanpak vraagt inspanning door ketenorganisaties en eenduidige samenwerking.

Daarnaast biedt de BIO een basis voor overheidsorganisaties om zowel intern als extern transparant te zijn over de wijze waarop informatiebeveiliging is ingericht. Met de BIO hanteert de overheid één gezamenlijke taal en een gezamenlijk doel voor informatiebeveiliging.

De BIO is samengesteld uit de aanpak van NEN-EN-ISO/IEC 27001 (nl) (het managementsysteem), de beheersmaatregelen en implementatierichtlijnen uit NEN-EN-ISO/IEC

27002 (nl) en aanvullende verplichte overheidsmaatregelen.

3. Toepassing BIO

Met de Cbw is de BIO verplicht voor alle organisaties die vallen onder de sector 'Overheid' en geldt voor alle netwerk- en informatiesystemen, zowel digitaal als fysiek, binnen deze organisaties.

De BIO is van toepassing op de informatiebeveiliging van alle typen omgevingen, onder andere operationele technologie (OT) en zorginformatie en brengt deze op het noodzakelijke niveau met behulp van normen en richtlijnen zoals NEN 7510 Informatiebeveiliging in de zorg en Cybersecurity implementatierichtlijn (CSIR).

Deel 1 BIO2-kader en het bijbehorende deel 2 BIO-overheidsmaatregelen hebben een verplichtend karakter en moeten altijd gevolgd worden. Deel 3 Toelichting is een verzameling, uitwerking en verduidelijking op sommige punten van het kader en de overheidsmaatregelen. Deel 3 zal ontsloten worden op de website https://www.bio-overheid.nl.

Een informatiesysteem is "een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie." Het gaat dus expliciet niet alleen om technische (ICT) systemen, maar informatie en organisatie.

4. Verplichtingen BIO

De BIO stelt de volgende verplichtingen aan overheidsorganisaties:

NEN-EN-ISO/IEC 27001 wordt toegepast op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging en het vaststellen van het toepassingsgebied (de reikwijdte) van dit managementsysteem.

Voor het bepalen van de context van de organisatie neemt de organisatie minimaal de beschreven context over uit de BIO bij het inrichten, implementeren, in stand houden en continu verbeteren van het managementsysteem voor informatiebeveiliging.

NEN-EN-ISO/IEC 27002 én de verplichte overheidsmaatregelen uit de BIO moeten worden toegepast op het formuleren van passende beheersmaatregelen.

Hierbij wordt rekening gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico's gelden, gebaseerd op de scope en de onderkende risico's. De beheersmaatregelen uit NEN-ISO/IEC 27002 en de BIO kunnen, waar nodig én gelijkwaardig worden vervangen of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor zorginformatie de **NEN 7510** en voor Operationele Technologie (OT) de **CSIR** en IEC 62443 Industriële cybersecurity.

Organisaties tonen opzet, bestaan en werking van maatregelen aan.

Deze vereiste volgt ook uit de Cbw/Network and Information Security directive 2 (NIS2). De BIO omvat maatregelen op tactisch niveau. Dit betekent dat deze maatregelen door de organisatie eerst geoperationaliseerd moeten worden voordat ze geïmplementeerd kunnen worden. Deze implementatie is risicogericht en voldoet aan best practices en marktstandaarden. Onderdeel van de operationalisatie is ook het kunnen detecteren of de maatregel goed functioneert. Over het hele ontwerp wordt geborgd dat uitval van één maatregel niet leidt tot een directe kwetsbaarheid in het hele systeem. Hoe de maatregelen zijn geoperationaliseerd, wordt via verwijzingen vastgelegd. Hiermee toont een organisatie de 'opzet' van maatregelen aan. Al dan niet met behulp van externe partijen en/of via self-assessments, audits, pentesten, redteam-testen en dergelijke toont een organisatie het 'bestaan' en de 'werking' aan van maatregelen aan.

Er bestaan beheersmaatregelen zonder overheidsmaatregelen.

Als een dergelijke beheersmaatregel van toepassing is, moet gebruik gemaakt worden van de bijbehorende implementatieaanwijzing uit NEN-EN-ISO/IEC 27002. Afwijken of niet toepassen van bovenliggende beheersmaatregel moet worden onderbouwd met een risicoanalyse en de referentie naar deze analyse moet in een bijlage uitzonderingen opgenomen zijn in de Verklaring van Toepasselijkheid (VvT).

Een beheersmaatregel kan een of meerdere overheidsmaatregelen hebben.

Deze overheidsmaatregelen vormen de minimale invulling van de beheersmaatregel. Uit een risicoanalyse moet blijken of deze voldoende zijn om het risico te beheersen en tot een acceptabel niveau verlagen.

5. Het managementsysteem voor informatiebeveiliging

Het managementsysteem voor informatiebeveiliging (Information Security Management Systeem, ook wel ISMS) is een werkwijze om informatiebeveiliging op een gestructureerde manier toe te passen in de organisatie. Zo wordt de organisatie, en een bestuurder in het bijzonder, in staat gesteld om de juiste afwegingen te maken.

Om een veelvoorkomend misverstand te voorkomen: een managementsysteem is géén applicatie. Een applicatie kan wel ondersteunen bij het toepassen van een managementsysteem.

De BIO schrijft voor dat het managementsysteem van een organisatie voldoet aan NEN-EN-ISO/IEC 27001. Bij het bepalen van de reikwijdte van het managementsysteem moet een organisatie minimaal de bedrijfsprocessen en informatiesystemen opnemen die kritisch zijn voor haar dienstverlening, waarbij aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid zou leiden tot onacceptabele impact.

Het managementsysteem voor informatiebeveiliging borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door een risicomanagementproces toe te passen. Dit geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerd.

Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is met de procedures van de organisatie en met de algehele managementstructuur, en dat informatiebeveiliging in aanmerking wordt genomen bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen.

6. Reikwijdte managementsysteem

Bij het bepalen van de reikwijdte van het managementsysteem moet een organisatie minimaal de bedrijfsprocessen en informatiesystemen opnemen die kritisch zijn voor haar dienstverlening. Het is aan de overheidsorganisaties zelf om te bepalen in welke mate de ondersteunende processen zijn opgenomen in het managementsysteem.

Waar overheden gelijkwaardige processen hanteren, is het aanbevolen om, waar beschikbaar, gebruik te maken van het ondersteuningsaanbod van de koepelorganisatie.

7. Samenhang managementsystemen

De BIO sluit aan op de Harmonized Structure (HS), wat een consistente en uniforme structuur biedt voor managementsystemen, waardoor de integratie van verschillende (ISO-)normen voor managementsystemen wordt vereenvoudigd. Hierdoor wordt dubbel werk voorkomen en middelen efficiënter gebruikt. Het biedt uniformiteit bij de implementatie van verschillende managementsystemen en vereenvoudigt de integratie van deze systemen.

8. Risicomanagement

Risicomanagement is een kernonderdeel van NEN-EN-ISO/IEC 27001 en vormt ook de basis van de BIO-aanpak binnen de overheid. De processen zijn ontworpen om risico's systematisch te identificeren, beoordelen, beheersen en continu te monitoren. Het risicomanagementproces verloopt in hoofdlijnen als volgt:

1. Contextbepaling
2. Risico-identificatie

3. Risicoanalyse
4. Risicobehandeling en maatregelenselectie
5. Kiezen risicomanagementmethodiek

9. Contextbepaling

NEN-EN-ISO/IEC 27001 vereist dat een organisatie eerst haar context vaststelt om relevante informatiebeveiligingsrisico's te identificeren. De BIO vereist hierbij dat overheidsorganisaties minimaal de in de BIO beschreven context meenemen, waaronder de sector 'Overheid' en de specifieke informatiebeveiligingseisen. Dit omvat zowel interne als externe factoren die invloed hebben op de beveiliging van informatie(systemen), en de daarmee samenhangende wettelijke verplichtingen uit de Cbw.

10. Risico-identificatie

In deze stap stelt de organisatie vast welke waardevolle informatie(verwerkende) middelen aanwezig zijn, brengt de relevante bedreigingen in kaart die daarop van invloed kunnen zijn, identificeert de kwetsbaarheden en bepaalt wat de potentiële consequenties zijn indien deze bedreigingen zich daadwerkelijk manifesteren. Hierbij worden uiteenlopende dreigingen en mogelijke scenario's systematisch geïnventariseerd. Verschillende hulpmiddelen zoals de NEN-ISO/IEC 27005 of de NIST (CSF en SP 800-30) kunnen gebruikt worden. Voorbeelden hiervan zijn dreigingen die voortkomen uit ketenafhankelijkheden, op OT, of gegevensuitwisseling met zorginstellingen.

11. Risicoanalyse

De geïdentificeerde risico's worden vervolgens geanalyseerd en geclassificeerd op basis van hun waarschijnlijkheid en impact. Gebruik in dit proces de NEN-EN-ISO/IEC 27001-methoden voor het uitvoeren van risicoanalyses, ondersteund door richtlijnen uit de BIO. Het classificeren van risico's draagt bij aan een consistent beeld van de risicoprioriteiten binnen de organisatie en de overheid als geheel.

12. Risicobehandeling en maatregelenselectie

Er worden na de risicoanalyse passende beheersmaatregelen geselecteerd om risico's te mitigeren. NEN-EN-ISO/IEC 27001, bijlage A, biedt een reeks beheersmaatregelen, die nader uitgewerkt zijn in NEN-EN-ISO/IEC 27002. De BIO vult deze aan met verplicht toe te passen overheidsmaatregelen die aansluiten op de context van de overheid. Deze overheidsmaatregelen zijn altijd verplicht en kunnen ongeacht de risico-inschatting van de organisatie niet geaccepteerd worden, tenzij ze niet van toepassing kunnen zijn.

13. Kiezen risicomanagementmethodiek

Een organisatie moet een risicomanagementmethodiek kiezen en toepassen die aansluit bij de NEN-EN-ISO/IEC 27001. Een risicomanagementmethodiek omvat ten minste de volgende onderdelen:

- Een quickscan om te bepalen of het basisniveau toereikend is of dat aanvullende maatregelen noodzakelijk zijn en waarin de classificatie van een proces en een informatiesysteem wordt uitgevoerd.
- Een methode voor een volledige risicoanalyse om te komen tot aanvullende maatregelen.
- Een risicoregister met daarin de tijdelijk geaccepteerde risico's.
- Een proces voor opvolging van risico's om tijdelijk geaccepteerde risico's structureel op te lossen.

14. Verklaring van toepasselijkheid (VvT)

NEN-EN-ISO/IEC 27001 vereist dat organisaties een VvT (statement of applicability) opstellen, waarin zij de geselecteerde beheersmaatregelen vastleggen en toelichten welke maatregelen zijn geïmplementeerd. Voor overheidsorganisaties geldt dat zij hierin ook de BIO-overheidsmaatregelen expliciet opnemen. Eventuele afwijkingen of niet-toepasbare beheersmaatregelen moeten in een bijlage 'Uitzonderingen op de VvT' worden opgenomen.

15. Monitoring en continue verbetering

NEN-EN-ISO/IEC 27001 en de BIO leggen de nadruk op een continu verbeterproces. Een organisatie moet haar risicomanagementsysteem onderhouden en regelmatig te evalueren om de effectiviteit van beheersmaatregelen te waarborgen. Wijzigingen in wetgeving of nieuwe bedreigingen kunnen aanleiding geven tot het bijwerken van de risicoanalyse en beheersmaatregelen. Met interne audits, managementbeoordelingen en gestroomlijnde documentatie binnen het ISMS houdt de organisatie haar risicomanagement actueel.

16. Samenstelling overheidsmaatregelen

De set overheidsmaatregelen vormt een eerste stap naar een goed niveau van informatiebeveiliging voor elke (overheids)organisatie en moet zonder meer worden geïmplementeerd, ongeacht de mate van risico-acceptatie, tenzij een overheidsmaatregel volgens de VvT niet van toepassing kan zijn. Deze set bestaat uit basismaatregelen, ketenmaatregelen en maatregelen specifiek voor overheidsrisico's of een combinatie daarvan. Het doel is een minimumstandaard te waarborgen. Overheidsmaatregelen zijn ingedeeld naar de volgende categorieën of een combinatie daarvan:

- Basishygiëne: aan deze maatregelen dient minimaal voldaan te worden om aan NIS2 te kunnen voldoen.
- Ketenhygiëne: maatregelen die bijdragen aan het mitigeren van risico's in de keten van overheden en waarbij gezamenlijk handelen door de overheid nodig is.
- Overheidsrisico's: mitigeren van universele informatieveiligheidsrisico's die gelden voor de gehele overheid.

17. Continue ontwikkeling

Informatiebeveiliging is een cyclisch proces. De implementatie BIO kan niet afgedaan worden met een eenmalig project. Door het toepassen van een managementsysteem blijft een organisatie continu ontwikkelen en verbeteren.

18. Transparantie en verantwoording

Burgers moeten de overheid kunnen vertrouwen. Dit wordt ook bereikt door transparant te zijn over de inrichting en de staat van informatieveiligheid en daar verantwoording over af te leggen aan burgers, toezichthouders, ketenpartners en stelselverantwoordelijken.

Een ISMS is een belangrijke manier om gestructureerde verantwoording te ondersteunen.

Het is vanuit NEN-EN-ISO/IEC 27001 verplicht om een reikwijdte, ook wel scope, van het ISMS en een zogenaamde VvT te hanteren. Het publiceren van de reikwijdte van het ISMS en de bijbehorende VvT draagt bij aan transparantie over de inrichting van informatiebeveiliging door de overheid. Niet publiceren van deze informatie zou een onnodige drempel opwerpen voor burgers. Het publiceren van de reikwijdte en de VvT is

daarom verplicht voor een overheidsorganisatie. Een voorbeeld van een VvT wordt gepubliceerd op de website van de BIO [in ontwikkeling].

19. Toezicht

De BIO-aanpak is de basis voor het invullen van zorgplicht van de Cbw door overheden. NEN-EN-ISO/IEC 27001 en 27002 vormen de basis van de BIO. Het is aangeraden voor toezichthouders om deze standaarden te hanteren. De elementen uit het ISMS vormen de basis om het managementsysteem te toetsen, inclusief de verplichte overheidsmaatregelen uit de BIO.

De BIO verplicht geen NEN-EN-ISO/IEC 27001-certificering. Certificering draagt wel bij aan het vereenvoudigen van de verantwoording en geeft op basis van een onafhankelijke beoordeling aan dat de organisatie in staat is om informatiebeveiliging procesmatig uit te voeren.

20. Toepasselijke overige normen, wet- en regelgeving

De BIO bevat overheidsmaatregelen die in lijn zijn met andere wet- en regelgeving, maar is daarin zeker niet uitputtend.

De BIO is expliciet niet bedoeld om alle beveiligingseisen van de overheid af te dekken. De verschillende overheidslagen hebben te maken met specifieke dreigingen. Het staat ze vrij om voor hun overheidslagen specifieke aanvullende maatregelen te benoemen en die, afhankelijk van de interne besluitvorming, verplichtend of adviserend door te voeren. Daarnaast is elke overheidsorganisatie zelf verantwoordelijk om vast te stellen welke interne en externe eisen, waaronder ook wet- en regelgeving, van toepassing zijn.

Binnen de overheid gelden meerdere normen voor informatiebeveiliging. Naast de BIO zijn er bijvoorbeeld de Nederlandse normen NEN 7510 Informatiebeveiliging in de zorg voor verwerkers van zorginformatie, NEN-EN-ISO 22301 Managementsystemen voor bedrijfscontinuïteit en crisismanagement en de CSIR voor OT. De basis van die normen is de internationale norm NEN-EN-ISO/IEC 27001 en NEN-EN-ISO/IEC 27002. Managementsystemen en beheersmaatregelen volgens deze normen kunnen worden geïntegreerd in een managementsysteem voor informatiebeveiliging op basis van NEN-EN-ISO/IEC 27001. Daarmee vallen de twee onderdelen samen: risicomanagement en maatregelen die specifiek passen bij de context.

21. Cyberbeveiligingswet (Cbw)

Voor overheden is in de Cbw vastgelegd op welke wijze de zorgplicht voor informatiebeveiliging moet worden ingevuld. Hieronder volgt een samenvatting van de belangrijkste punten die betrekking hebben op het toepassen van de BIO:

Verplichting BIO: de BIO is via de Cbw verplicht voor alle organisaties die vallen onder de sector ‘Overheid’.

Verantwoordelijkheid bestuurder: De bestuurder is verantwoordelijk voor:

- het treffen van passende en evenredige technische, operationele en organisatorische maatregelen om de risico’s te beheren en afgestemd op de voor de organisatie relevante risico’s en deze beheersen;
- het goedkeuren van te nemen maatregelen voor het beheer van cyberbeveiligingsrisico’s;
- het toezien op de kwaliteit van de uitvoering en het beheer van de maatregelen.

Opleiding: bestuurders moeten opgeleid zijn en kennis hebben om te kunnen sturen op informatiebeveiligingsrisico’s. En bestuurders moeten ervoor zorgen dat hun werknemers regelmatig opleiding/training volgen over het onderwerp. Dit betekent dat de opleiding moet voldoen aan [invulling Cbw voor de sector ‘Overheid’].

Meldplicht: de organisatie is verantwoordelijk voor het tijdig melden van incidenten. Overheden moeten binnen de doorlooptijden [invulling Cbw voor de sector 'Overheid'] een melding maken van een meldplichtig incident.

Toezicht en verantwoording: de toezichthouder zal toezicht houden op de invulling van de zorgplicht volgens de Cbw. De RDI is als toezichthouder aangewezen voor de sector 'Overheid'.

22. Governance

De bestuurder van een overheidsorganisatie is verantwoordelijk voor het beheersen van informatiebeveiligingsrisico's. De bestuurder kan dat niet alleen. Om informatiebeveiliging gedegen in te regelen, is een structuur nodig. Het is aan de organisatie om deze structuur aan te brengen volgens NEN-EN-ISO/IEC 27001.

Voor overheden zijn er een aantal rollen die standaard deel uitmaken van informatiebeveiliging van een overheidsorganisatie. Deze rollen komen ook terug in de uitwerking van overheidsmaatregelen.

Bestuurder

De bestuurder is verantwoordelijk voor het treffen van passende en evenredige technische, operationele en organisatorische maatregelen en moet toezien op de naleving daarvan. Kortgezegd de bestuurder is verantwoordelijk voor risicomanagement, dat gericht is op het borgen van digitale weerbaarheid van de organisatie.

Voor de vier overheidslagen is voor de invulling van de sector 'Overheid' binnen de Cbw gedefinieerd welke bestuurders worden bedoeld:

- Gemeenten: [Volgt uit invulling Cbw voor de sector 'Overheid']
- Provincies: [Volgt uit invulling Cbw voor de sector 'Overheid']
- Rijksoverheid: [Volgt uit invulling Cbw voor de sector 'Overheid']
- Waterschappen: [Volgt uit invulling Cbw voor de sector 'Overheid']

De bestuurder laat zich daarbij adviseren door een Chief Information Security Officer (CISO), Chief Information Officer (CIO), functionaris gegevensbescherming (FG) en dergelijke.

Lijnmanagement

Het lijnmanagement:

- is de eigenaar van informatie(systemen) en is daarmee verantwoordelijk voor het identificeren van dreigingen en risico's van deze informatie(systemen);
- is verantwoordelijk voor het toepassen van de verplichte beheersmaatregelen en overheidsmaatregelen uit de BIO voor het informatiesysteem;
- vraagt de CISO om advies, in alle gevallen waar het afwijkt van overheidsmaatregelen, ook waar dat expliciet als bevoegdheid genoemd is.

CISO

De CISO:

- is verantwoordelijk voor de coördinatie van informatiebeveiliging;
- ondersteunt de bestuurder en moet gevraagd en ongevraagd advies kunnen geven aan de bestuurder;
- vertaalt wetgeving en bedrijfsdoelstellingen naar een informatiebeveiligingsbeleid;
- rapporteert aan het bestuur hoe het lijnmanagement het informatiebeveiligingsbeleid implementeert en op welke wijze wordt voldaan aan de BIO, om ervoor zorg te dragen dat de bestuurder geïnformeerde besluiten kan maken over de behandeling van informatiebeveiligingsrisico's;

- is uitdrukkelijk niet verantwoordelijk voor informatiebeveiliging door het lijnmanagement.

Interne toezichthouder

Een bestuurder moet toezien op de toepassing van informatiebeveiliging in de organisatie. Een interne toezichthouder kan helpen bij dit toezicht.

23. Leveranciers

Leveranciers bieden diensten en/of producten aan overheidsorganisaties. Een overheidsorganisatie blijft zelf verantwoordelijk voor het behandelen van risico's die betrekking hebben op de uitbestede of ingekochte dienst of product.

Afhankelijk van het risico behoren daarom verplichtingen van de overheid die volgen uit de BIO of uit andere richtlijnen te worden meegenomen bij het samenstellen van inkoopeisen aan leveranciers.

24. Informatiebeveiligingsprincipes

Overheidsmaatregelen moeten risicogericht worden toegepast en geoperationaliseerd. Daarbij is het praktisch om informatiebeveiligingsprincipes te definiëren en toe te passen zoals security by design & default, toegang op basis van need to know, assume breach, zero trust, dingen gaan fout, defense in depth et cetera.

25. Operationaliseren maatregelen/balans in de maatregelenset

De BIO bevat maatregelen op tactisch niveau, die geoperationaliseerd moeten worden. Hierbij is het belangrijk om in de maatregelenset balans te houden tussen:

- Beschikbaarheids-, integriteits- en vertrouwelijkheidsmaatregelen.
- Organisatorische/proces-, mensen/gedrag en applicatieve/technische maatregelen.
- Identificeren, beschermen, detecteren, reageren en herstellen.

26. Treffen aanvullende maatregelen

Overheden kennen verschillende soorten informatie. Het is aan de organisatie zelf om te bepalen welk typen informatie wordt verwerkt door de organisatie en welke aanvullende beveiligingsmaatregelen getroffen moeten worden. Bij deze afweging moeten in ieder geval - en niet uitsluitend - de volgende typen gegevens worden afgewogen:

- Open data
- (Bijzondere) persoonsgegevens
- Gevoelige of interne informatie
- Gerubriceerde informatie

27. Impact van risico's

De impact van een informatiebeveiligingsincident hangt sterk af van de context. Overheidsorganisaties ondervinden vaak specifieke gevolgen door hun rol in de samenleving en democratie, hun bestuursstijl en hun verhouding tot de burgers. Bij het bepalen van de impact moeten minimaal onderstaande impactsgebieden worden afgewogen:

- Politieke schade aan een bestuurder
- Diplomatieke schade
- Financiële gevolgen
- Directe imagoschade

- Verlies van publiek respect of vertrouwen
- Organisatiebrede negatieve publiciteit
- Significant verlies van motivatie van medewerkers
- Belangrijk verlies van management control

De impactgebieden kunnen ook bijdragen aan begrip bij de uitwisseling van impact met ketenpartners.

28. Relatie BIO en andere onderwerpen

De BIO richt zich op informatiebeveiliging. Onderwerpen zoals privacybescherming, informatievoorziening, beheersprocessen, bedrijfscontinuïteit en dergelijke zijn aanpalend aan informatiebeveiliging. Voor deze onderwerpen zijn vaak aparte standaarden opgezet. Deze onderwerpen worden daarom niet uitgewerkt in de BIO. Daar waar nuttig wordt verwezen naar deze separate standaarden.

DEEL 2 BIO–OVERHEIDSMAATREGELEN

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
5.01.01	Verantwoordelijkheden en samenhang voor informatiebeveiliging, de beveiliging van operationele technologie (OT) en de verantwoordelijkheden met betrekking tot de continuïteit van de taakuitvoering van de organisatie, bedrijfscontinuïteitsmanagement (BCM) zijn beschreven en vastgesteld. De toewijzing van verantwoordelijkheid voor ketens van informatiesystemen aan lijnmanagers. De organisatie heeft een informatiebeveiligingsbeleid opgesteld en vastgesteld door de leiding van de organisatie. Dit beleid bevat ten minste de volgende punten: 1. De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. 2. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. 3. De toewijzing van de verantwoordelijkheden en samenhang van informatiebeveiliging voor ketens van informatiesystemen, de beveiliging van OT, privacybescherming en de verantwoordelijkheden met betrekking tot de continuïteit van de taakuitvoering van organisatie (BCM) aan lijnmanagers. 4. De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. 5. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. 6. De bevordering van het beveiligingsbewustzijn.	Basishygiëne, ketenhygiëne
5.01.02	Het informatiebeveiligingsbeleid wordt minimaal jaarlijks en in aansluiting bij de (bestaande) bestuurs- en Planning & Control (P&C)-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Basishygiëne
5.02.01	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn voor informatiebeveiliging (ook voor OT, BCM en privacybescherming) binnen haar organisatie. Hierbij is specifieke aandacht voor de verantwoordelijkheden en rollen voor het adequaat afhandelen van incidenten. Lijnmanagers en proceseigenaren die verantwoordelijk zijn voor bedrijfsmiddelen zijn ook verantwoordelijk voor de behandeling van risico's die op die bedrijfsmiddelen van toepassing zijn.	Basishygiëne
5.02.02	Er is een CISO aangesteld die bevoegd is om onafhankelijk en zelfstandig te adviseren en te rapporteren aan het	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
	bestuur en of het controlerend orgaan over informatiebeveiliging.	
5.03.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
5.04.01	Bestuur en werknemers moeten regelmatig, scholing volgen om cyberbeveiligingsrisico's te herkennen en te voorkomen en te weten wat men moet doen als er een informatiebeveiligingsincident is. Daarbij tonen bestuurders aan dat zij voldoende kennis en vaardigheden hebben om de gevolgen van informatiebeveiligingsrisico's te beoordelen op de diensten en/of producten die de organisatie levert.	Basishygiëne
5.04.02	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel en vrijwilligers in het contract vastgelegd volgens de huisregels of interne gedragsregels.	Overheidsrisico
5.04.03	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	Overheidsrisico
5.05.01	De organisatie heeft uitgewerkt welke functionarissen met welke (overheids)instanties en toezichthouders formele contacten hebben over informatiebeveiliging. Dit overzicht wordt ten minste jaarlijks geactualiseerd.	Ketenhygiëne
5.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
5.07.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne, ketenhygiëne
5.08.01	Bij nieuwe informatiesystemen en bij significante wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging op basis van de door de organisatie vastgestelde risicomanagementmethodiek worden uitgevoerd, om risico's te identificeren en in voldoende mate te beheersen en ook voor het vaststellen van de beveiligingseisen.	Ketenhygiëne
5.09.01	Er is een inventaris van bedrijfsmiddelen die van belang zijn voor informatieverwerking, met inbegrip van OT. De inventaris omvat alle eigenschappen die nodig zijn voor het beheer en onderhoud. In de inventaris zijn ook opgenomen: bedrijfsmiddelen op afstand, cloud-omgevingen en bedrijfsmiddelen die regelmatig zijn verbonden met de netwerkinfrastructuur maar niet onder controle van de organisatie staan. De volledigheid en actualiteit van de inventaris wordt periodiek gecontroleerd met tussenpozen die passend zijn voor de frequentie waarmee wijzigingen optreden.	Basishygiëne, ketenhygiëne
5.10.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
5.11.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
5.12.01	Informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd. Hierbij wordt gebruik gemaakt van een vastgestelde impactclassificatiemethodiek die onderdeel is van de vastgestelde risicomanagementmethodiek.	Basishygiëne, ketenhygiëne
5.13.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Ketenhygiëne
5.14.01	Internetfacing-informatiesystemen en e-mail-berichtenverkeer moeten blijvend voldoen aan de verplichte standaarden, zie hiervoor de website van het Forum Standaardisatie. Hierop wordt gestuurd met de metingen van internet.nl. Daarbij dienen alle onderdelen te worden ingesteld zodat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst.	Basishygiëne
5.14.02	Maak bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated (OV)-certificaten. Maak bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten kunnen voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving.	Basishygiëne
5.14.03	Geavanceerde en/of gekwalificeerde elektronische handtekeningen moeten voldoen aan de Advanced Electronic Signatures (AdES Baseline Profiles), zoals opgenomen in de Lijst open standaarden van Forum Standaardisatie.	Basishygiëne
5.14.04	Van alle internetfacing-informatiesystemen, webapplicaties, IP-adressen en API's is een actuele registratie.	Basishygiëne
5.14.05	Publiek toegankelijke websites worden bekend gemaakt via Register Internetdomeinen Overheid. Deze informatie wordt ten minste iedere zes maanden geactualiseerd.	Basishygiëne
5.15.01	Toegang tot een vertrouwde zone is toegestaan in twee situaties: 1. vanaf geauthentiseerde apparatuur of; 2. vanuit programmatuur die draait binnen een veilige schil.	Basishygiëne, ketenhygiëne
5.16.01	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Basishygiëne
5.16.02	Het gebruiken van groepsaccounts is niet toegestaan, tenzij de proceseigenaar dit motiveert, vastlegt en afstemt met de CISO.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
5.17.01	Pas multi-factorauthenticatie (MFA) ten minste toe voor het primaire aanloggen op de digitale werkomgeving, bij accounts voor via het internet bereikbare voorzieningen en accounts die beheerrechten hebben en in andere situaties waar uit de risicoanalyse blijkt dat dit een passende oplossing is. Pas MFA toe in deze twee vormen: 1. Wachtwoordloze toegang, zoals een pincode in combinatie met een hardware token of persoonlijk uniek certificaat (passkey). 2. Wachtwoordtoegang in combinatie met minimaal een tweede factor. Indien MFA niet mogelijk is voor deze accounts, neem andere mitigerende maatregelen. Betrek de CISO hierbij en laat ze goedkeuren door de proceseigenaar. Combineer waar mogelijk en veilig, MFA met federatieve authenticatievoorzieningen zoals Single Sign On en een Stepping Stone-oplossing. Voor beheer en monitoring van authenticatiegegevens: – geef authenticatie-informatie uit met formele vastgestelde procedures en pas nadat de identiteit van de gebruiker met voldoende zekerheid is vastgesteld; – definieer Use Cases voor misbruik van authenticatiegegevens, monitor deze en neem passende actie bij het optreden ervan. Deze Use Cases omvatten in ieder geval inlogpogingen van ongebruikelijke plekken en pieken in mislukte inlogpogingen.	Basishygiëne, ketenhygiëne
5.17.02	De organisatie biedt aan alle medewerkers een wachtwoordmanager of vergelijkbare oplossing aan.	Basishygiëne
5.17.03	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Basishygiëne
5.18.01	Het maken en aanpassen van accounts met bijzondere rechten wordt gemonitord. Indien deze wijzigingen ongeautoriseerd zijn, is dit een informatiebeveiligingsincident en wordt als zodanig vastgelegd en afgehandeld.	Basishygiëne
5.18.02	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. Een risicoafweging bepaalt of dit sneller moet.	Basishygiëne
5.19.01	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, zijn informatiebeveiligingseisen (beschikbaarheid, integriteit en vertrouwelijkheid) onderdeel van het hele pakket aan inkoopeisen. De informatiebeveiligingseisen zijn gebaseerd op een expliciete risicoafweging.	Basishygiëne, ketenhygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
5.20.01	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar de verwerking van informatie een rol speelt.	Basishygiëne, ketenhygiëne
5.20.02	Sluit waar mogelijk algemene voorwaarden van leveranciers expliciet uit en neem eventueel aanvullende voorwaarden op. Als uitsluiten niet mogelijk is, beoordeel dan de risico's. Expliciet is gemaakt welke consequenties geaccepteerd worden, welke gemitigeerd moeten zijn en welke voorwaarden niet of nooit geaccepteerd mogen worden bij het aangaan van de overeenkomst.	Basishygiëne, ketenhygiëne
5.20.03	In het inkoopcontract wordt opgenomen dat de leverancier aantoont dat hij aan alle gestelde eisen voldoet in opzet, bestaan en werking, op basis van onderzoeken van onafhankelijke derden. Deze onderzoeken hebben een scope die dekkend is voor de gecontracteerde dienstverlening. Hierbij is expliciet aandacht voor de toeleveringsketen en hoe de leverancier zijn leveranciersmanagement ingeregeld heeft, zie overheidsmaatregel 5.21.01. Dit toont de leverancier jaarlijks opnieuw aan.	Basishygiëne, ketenhygiëne
5.20.04	De overheidsorganisatie voert zelfstandig onderzoek uit, ook ter validatie van de rapportages die de leverancier aanlevert. Om dit mogelijk te maken, wordt expliciet opgenomen dat er een mogelijkheid is voor een externe audit. Indien uit het voorgaande restrisico's volgen, beheerst de overheidsorganisatie deze door het toepassen van zijn vastgestelde risicomanagementmethodiek.	Basishygiëne, ketenhygiëne
5.20.05	Onderdeel van de afspraken is dat de leverancier transparant is over kwetsbaarheden in de dienstverlening en informatiebeveiligingsincidenten waaronder datalekken. Dit stelt de overheidsorganisatie in staat om passend te reageren onder meer door te rapporteren en mitigerende maatregelen te nemen.	Basishygiëne, ketenhygiëne
5.20.06	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	Basishygiëne, ketenhygiëne
5.21.01	In het contract is opgenomen dat de leverancier verantwoordelijk is voor het borgen van de gestelde eisen bij de toeleveranciers.	Basishygiëne, ketenhygiëne
5.21.02	Voorafgaand aan het afsluiten van de overeenkomst geeft de leverancier inzicht in de keten van toeleveranciers en eventuele risico's daarin. De overheidsorganisatie beoordeelt of de risico's acceptabel zijn.	Basishygiëne, ketenhygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
5.21.03	De overheidsorganisatie borgt dat de beveiligingseisen aan de leverancier onverminderd van toepassing zijn op de keten van toeleveranciers, tenzij die eisen niet relevant zijn gezien de aard van de dienstverlening door de toeleverancier. Indien informatiebeveiligingseisen zijn uitgesloten, maakt de leverancier dat inzichtelijk, inclusief een onderbouwing.	Basishygiëne, ketenhygiëne
5.21.04	Gedurende de looptijd geeft de leverancier veranderingen in de keten van toeleveranciers door, inclusief risico's daarin. Dit omvat minimaal kwetsbaarheden en informatiebeveiligingsincidenten die de dienstverlening aan de overheidsorganisatie kunnen raken.	Basishygiëne, ketenhygiëne
5.22.01	Op basis van het door de leverancier aangeleverde bewijsmateriaal, zie overheidsmaatregel 5.20.03, is de proceseigenaar verantwoordelijk voor het jaarlijks beoordelen dat leverancier voldoet aan de gestelde informatiebeveiligingseisen, het vaststellen van eventuele beveiligingsrisico's, het (laten) nemen van mitigerende maatregelen en het accepteren van rest-risico's.	Basishygiëne, ketenhygiëne
5.22.02	Er is een actuele registratie van leveranciers en afgesloten contracten.	Basishygiëne, ketenhygiëne
5.23.01	Stel beleid op dat toeziet op het inventariseren, classificeren, selecteren, beoordelen en managen van Cloud Service Providers (CSP) en het beëindigen van dienstverlening door CSP's. Implementeer het beleid. Herzie dit beleid minimaal eens per drie jaar. Neem in de contracten op welke situaties aanleiding kunnen zijn tot ontbinding van het contract. Wanneer zich belangrijke wijzigingen bij de leverancier optreden, beoordeel de risico's daarvan en neem passende maatregelen.	Basishygiëne, ketenhygiëne
5.24.01	Er is voor alle interne en externe medewerkers een toegankelijk meldloket waar informatiebeveiligingsincidenten kunnen worden gemeld en geregistreerd.	Basishygiëne, ketenhygiëne
5.24.02	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	Basishygiëne
5.24.03	De proceseigenaar is verantwoordelijk voor het oplossen van informatiebeveiligingsincidenten.	Basishygiëne
5.24.04	De proceseigenaar rapporteert maandelijks de opvolging van informatiebeveiligingsincidenten aan de eindverantwoordelijke voor de bedrijfsvoering.	Basishygiëne
5.24.05	In de procedure voor informatiebeveiligingsincidenten is er een koppeling gemaakt met crisisbeheersing.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
5.24.06	De beveiliging van toeleveringsketens is onderdeel van de risicoanalyse voor de organisatie. In de risicoanalyse wordt rekening gehouden met: – specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener; – de algemene kwaliteit van de producten; – de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.	Basishygiëne
5.24.07	De incidentprocedure is er op ingericht om: – binnen de wettelijke termijn informatiebeveiligingsincidenten te melden bij het nationale Cyber Security Incident Responce Team (CSIRT); – meldingen van het nationale CSIRT te ontvangen, te beoordelen en op te nemen in de risicobehandeling; – betrokkenen binnen de wettelijke termijn op de hoogte te stellen van het incident.	Basishygiëne
5.25.01	Informatiebeveiligingsincidenten worden afgedaan via het incidentbeheerproces. Ze worden indien relevant gemeld bij toezichthouders volgens de bepalingen uit de betrokken wet- en regelgeving zoals de Cbw, de Archiefwet en de Algemene verordening gegevensbescherming (AVG).	Basishygiëne, overheidsrisico
5.26.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
5.27.01	Informatiebeveiligingsincidenten worden geanalyseerd om achterliggende oorzaken vast te stellen, verbeteringen te realiseren, om zo toekomstige incidenten te voorkomen.	Basishygiëne
5.27.02	De analyses van informatiebeveiligingsincidenten, inclusief de achterliggende oorzaken en de verbeteringen worden breed gedeeld met relevante partners om herhaling en toekomstige incidenten te voorkomen.	Basishygiëne
5.28.01	De bewaartermijn van een (vermoedelijk) informatiebeveiligingsincident en alle informatie om het incident te analyseren en op te lossen, is minimaal drie jaar. Dit betreft onder meer de informatie benodigd voor de analyse (waaronder logging), de oplossing en het advies.	Basishygiëne
5.29.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne, ketenhygiëne
5.30.01	De proceseigenaar test jaarlijks continuïteitsplannen op werking, volledigheid en actualiteit, om de plannen te verbeteren.	Overheidsrisico
5.30.02	Binnen de inventarisatie van beheersmaatregel 5.12, identificeert de proceseigenaar kritieke systemen op basis van de vastgestelde risicomanagementmethodiek en een expliciete risicoafweging. De proceseigenaar actualiseert dit overzicht ten minste eens per drie jaar.	Overheidsrisico

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
5.31.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne, ketenhygiëne
5.32.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
5.33.01	De proceseigenaar heeft voor alle informatie(systemen) in selectielijsten de bewaartermijn vastgelegd, rekening houdend met de eigen bedrijfsdoelstellingen en wet- en regeling, zoals de archiefwet en privacywetgeving. De proceseigenaar heeft deze termijnen ook praktisch ingeregeld en toetst periodiek de werking hiervan.	Basishygiëne, ketenhygiëne
5.34.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
5.35.01	Er is een werkend ISMS volgens NEN-EN-ISO/IEC ISO 27001.	Basishygiëne
5.35.02	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Basishygiëne
5.36.01	In de P&C-cyclus en als onderdeel van de plan-do-check-act (PDCA)-cyclus wordt gerapporteerd over informatiebeveiliging onder coördinatie van de CISO. Dit resulteert in een jaarlijks af te geven In Control Verklaring (ICV), of een vergelijkbaar instrument, over de gehele informatiebeveiliging van de overheidsorganisatie. De ICV of het vergelijkbare instrument kan ook onderdeel zijn van de formele verantwoording.	Basishygiëne
5.37.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
6.01.01	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan op basis van een risicoafweging een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.	Basishygiëne, overheidsrisico
6.02.01	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden voor informatiebeveiliging. De voor hen geldende regelingen en instructies voor informatiebeveiliging zijn eenvoudig toegankelijk.	Basishygiëne
6.03.01	Alle medewerkers, lijnmanagers en bestuurders hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels van en verplichtingen voor informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.	Basishygiëne
6.03.02	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding aantoonbaar een training I-bewustzijn succesvol gevolgd.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
6.03.03	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging. Het management stimuleert hen actief deze periodiek te volgen.	Basishygiëne
6.04.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
6.05.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
6.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
6.07.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
6.08.01	Alle medewerkers (intern en extern) hebben aantoonbaar kennisgenomen van de meldingsprocedure van informatiebeveiligingsincidenten.	Basishygiëne
7.01.01	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	Basishygiëne
7.01.02	Kritieke informatie of informatiesystemen zijn nooit via één beveiligde zone te bereiken.	Basishygiëne
7.02.01	In geval van concrete beveiligingsrisico's worden waarschuwingen, volgens onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Ketenhygiëne
7.03.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.04.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.05.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.07.01	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingsvergrendeling automatisch geactiveerd.	Basishygiëne
7.08.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.09.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.10.01	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten, de bedrijfsgevoelige inhoud onherstelbaar verwijderd is.	Overheidsrisico

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
7.10.02	Voor het wissen van alle data op het medium, wordt data onherstelbaar verwijderd of onbeschikbaar gemaakt. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is. Hiervan wordt verslag gemaakt. Er wordt bij voorkeur gebruik gemaakt van producten waarvoor de Unit Weerbaarheid van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) een positief inzetadvies afgegeven heeft.	Overheidsrisico
7.10.03	Het gebruik van koeriers of transporteurs voor transport van geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	Overheidsrisico
7.11.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.12.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.13.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
7.14.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
8.01.01	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet standaard op het gebruikersdevice wordt opgeslagen (‘zero footprint’). Als (near) zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen met een toegangsbeveiligingsmechanisme met minimaal versleuteling van de gegevens. Op mobiele apparatuur moet ‘wissen op afstand’ mogelijk zijn.	Basishygiëne
8.01.02	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: – In bewustwordingsprogramma’s komen gedragsaspecten van veilig mobiel werken aan de orde. – Het apparaat maakt deel uit van patchmanagement en hardening. – Er wordt gebruik gemaakt van Mobile Device Management (MDM)- of Mobile Application Management (MAM)-oplossingen. – Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. Periodiek wordt getoetst of de punten in lid 1., 2. en 3. worden nageleefd.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
8.02.01	De toegewezen of gebruikte speciale bevoegdheden worden in opzet, bestaan en werking minimaal ieder kwartaal beoordeeld.	Basishygiëne
8.03.01	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Basishygiëne
8.03.02	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Basishygiëne
8.04.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.05.01	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden en voor hoelang de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Basishygiëne, ketenhygiëne
8.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.07.01	Het downloaden van bestanden is beheerst en beperkt op basis van het risico en need-of-use. De antimalware-software moet altijd alle downloads beoordelen.	Basishygiëne
8.07.02	Gebruikers zijn voorgelicht over de risico's van surfgedrag en het klikken op onbekende links.	Basishygiëne
8.07.03	De gebruikte antimalware-software en bijbehorende herstelsoftware zijn actueel en wordt ondersteund door periodieke updates.	Basishygiëne
8.07.04	De malwarescan wordt uitgevoerd op: – alle omgevingen, bijvoorbeeld op (mail)servers, (desktop)computers en bij de toegangsverlening tot het netwerk van de organisatie; – alle gedownloade content voorafgaand aan executie of opslag; – alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik of opslag in de eigen omgeving.	Basishygiëne
8.08.01	Als de kans op misbruik en de verwachte schade beide hoog zijn (bijvoorbeeld met de NCSC-Inschalingsmatrix beveiligingsadviezen of leveranciersbeveiligingsadviezen), worden passende mitigerende maatregelen zo snel mogelijk, maar uiterlijk binnen een week getroffen.	Basishygiëne
8.08.02	Op basis van een expliciete risicoafweging wordt bepaald op welke wijze mitigerende maatregelen getroffen worden.	Basishygiëne
8.08.03	In de tussentijd of als installatie binnen een week niet mogelijk is, worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
8.08.04	Informatiesystemen worden bij voorkeur jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses, penetratietesten of red-teamingstesten. Internetfacing-informatiesystemen worden bij voorkeur continue getest op zwakheden en kwetsbaarheden.	Basishygiëne
8.08.05	Internetfacing-informatiesystemen hebben een verplichte (bij voorkeur geautomatiseerde) penetratietest bij iedere nieuwe release of major update. Als daar bevindingen met een hoog risico uitkomen die niet op een andere manier gemitigeerd kunnen worden, mag het systeem niet in productie. Alle internetfacing-informatiesystemen worden minimaal jaarlijks getest op zwakheden en kwetsbaarheden.	Basishygiëne
8.08.06	Een Coordinated Vulnerability Disclosure (CVD)-procedure is ingericht en gepubliceerd volgens de NCSC-leidraad of NEN-EN-ISO/IEC 29147:2020 Vulnerability disclosure. Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD)-meldingen is onderdeel van de incidentrapportage.	Basishygiëne
8.09.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.10.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.11.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.12.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.13.01	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Er moet speciale aandacht zijn voor het beschermen van de back-up tegen ransomware-aanvallen en genomen maatregelen om de integriteit van de back-up te behouden.	Basishygiëne, ketenhygiëne
8.13.02	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	Basishygiëne, ketenhygiëne
8.13.03	Het back-upproces voorziet in de opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Basishygiëne, ketenhygiëne
8.13.04	De herstelprocedure wordt minimaal jaarlijks getest of na een grote wijziging, om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Basishygiëne, ketenhygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
8.14.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.15.01	Een logregel bevat minimaal: – Actie: de gebeurtenis of handeling die heeft plaatsgevonden. – Object: waarop de gebeurtenis of handeling effect had (bijvoorbeeld welk bestand, proces of systeem). – Resultaat: het resultaat van de gebeurtenis of handeling. – Oorsprong: het apparaat of de netwerklocatie van waaruit de gebeurtenis of handeling in gang is gezet. – Actor: identificatie van de persoon die of het proces dat de gebeurtenis in gang heeft gezet. – Tijdstempel: datum en tijdstip waarop de gebeurtenis of handeling plaatsvond.	Basishygiëne
8.15.02	Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Basishygiëne
8.15.03	Er is een overzicht van logbestanden die worden gegenereerd.	Basishygiëne
8.15.04	De bewaartermijn van logbestanden en gegevens in het Security Incident en Event Monitoring (SIEM) worden risicogericht bepaald, rekening houdend met het scenario dat aanvallers langdurig binnen zijn.	Basishygiëne
8.15.05	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident via de procedure voor informatiebeveiligingsincidenten volgens beheersmaatregel 5.24.	Basishygiëne
8.15.06	Op basis van een expliciete risicoafweging bepaalt de organisatie de periodieke toetsing op het ongewijzigd bestaan van logbestanden gedurende de bewaartermijn. Toetsing wordt uitgevoerd door een onafhankelijke functionaris (ten opzichte van de uitvoering).	Basishygiëne
8.16.01	Bij ontdekte nieuwe dreigingen (aanvallen) via overheidsmaatregel 8.16.3 worden deze binnen geldende juridische kaders verplicht gedeeld met de daarvoor aangewezen Computer Emergency Response Team (CERT).	Basishygiëne, overheidsrisico
8.16.02	Het SIEM- en/of het SOC-monitoring-proces hebben eenduidige regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijke management.	Basishygiëne
8.16.03	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing, waarmee aanvallen kunnen worden gedetecteerd en afwijkingen adequaat en tijdig worden behandeld.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
8.16.04	Actieve netwerkcomponenten zijn voorzien van logging en monitoring van die logging om afwijkende gebeurtenissen te kunnen waarnemen en daarop te reageren.	Basishygiëne
8.17.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.18.01	Alleen bevoegd personeel heeft op die momenten dat toegang strikt noodzakelijk is toegang tot systeemhulpmiddelen.	Overheidsrisico
8.18.02	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Overheidsrisico
8.19.01	Het risico van installatie door gebruikers van niet geautoriseerde software moet worden beheerst.	Overheidsrisico
8.20.01	Netwerkcomponenten moeten minimaal voldoen aan het vertrouwelijkheidsniveau van het netwerk waarvan ze onderdeel zijn.	Overheidsrisico
8.20.02	Toegang tot beheerinterfaces van netwerkcomponenten moet (zo veel als mogelijk en risicogericht) gescheiden zijn van het gebruikersnetwerk.	Overheidsrisico
8.21.01	In koppelpunten met externe of onvertrouwde zones en vanwege netwerksegmentatie zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en te mitigeren.	Basishygiëne
8.21.02	Het dataverkeer van of naar de vertrouwde omgeving, wordt bewaakt/geanalyseerd op verdacht verkeer met detectievoorzieningen.	Basishygiëne
8.21.03	Bij ontdekte nieuwe dreigingen vanuit overheidsmaatregel 8.21.02 worden deze doorgeleid, rekening houdend met de geldende juridische kaders gedeeld binnen de overheid.	Basishygiëne
8.21.04	Bij transport van gegevens over draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied worden de gegevens versleuteld met uitzondering van metagegevens die noodzakelijk zijn om het transport tot stand te laten komen. De inrichting van de versleuteling is risicogericht en houdt rekening met de noodzakelijke beschermingstermijn en -niveau. Hierbij wordt bij voorkeur gebruik gemaakt van encryptiemiddelen waarvoor de Unit Weerbaarheid van de Algemene Inlichtingen en Veiligheidsdienst (AIVD) een positief inzetadvies heeft afgegeven. Heeft de Unit Weerbaarheid geen geadviseerde encryptiemiddelen, wordt in overleg met de CISO een andere geschikte versleutelingsmethodiek gekozen en ingericht.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
8.22.01	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Basishygiëne
8.23.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.24.01	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: – Wanneer cryptografie ingezet wordt. – Wie verantwoordelijk is voor de implementatie. – Wie verantwoordelijk is voor het sleutelbeheer. – Hoe geregistreerd wordt waar welke cryptografie toegepast wordt. – Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast. – De wijze waarop het beschermingsniveau vastgesteld wordt. – Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Basishygiëne, ketenhygiëne
8.24.02	Cryptografische beheersmaatregelen zijn opgenomen in de inventaris van de bedrijfsmiddelen. Voor alle cryptografische beheersmaatregelen is vastgesteld waar ze worden ingezet, wie er voor verantwoordelijk is en hoe ze actueel worden gehouden.	Basishygiëne, ketenhygiëne
8.24.03	Cryptografische toepassingen voldoen aan passende standaarden van het Forum Standaardisatie.	Basishygiëne, ketenhygiëne
8.24.04	De sterkte van de cryptografie wordt gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van de AIVD.	Basishygiëne, ketenhygiëne
8.24.05	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit de risicoafweging blijkt dat deze noodzakelijk zijn als onderdeel van gereedheid voor bedrijfscontinuïteit (beheersmaatregel 5.30).	Basishygiëne, ketenhygiëne
8.25.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
8.26.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Basishygiëne
8.27.01	Architectuurprincipes zoals ‘security by design’ en ‘security by default’ voor het ontwerpen van beveiliging van informatiesystemen worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten over het ontwikkelen van informatiesystemen.	Basishygiëne
8.28.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.29.01	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	Basishygiëne

Overheids maatregel-nummer	Overheidsmaatregel	Draagt bij aan
	Van de resultaten van de testen wordt verslag gemaakt.	
8.30.01	Interne maatregelen voor systeemontwikkeling zijn onverkort van toepassing op uitbestede ontwikkeling, aangevuld met maatregelen die volgen vanuit uitbestedingen.	Basishygiëne, ketenhygiëne
8.31.01	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.	Basishygiëne
8.31.02	Significante wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.	Basishygiëne
8.32.01	In het wijzigingsbeheerproces is minimaal aandacht besteed aan: – het administreren van wijzigingen, met de resultaten van het testplan; – een risicoafweging van mogelijke gevolgen van de wijzigingen, inclusief een beschreven rollbackplan; – de goedkeuringsprocedure voor wijzigingen.	Basishygiëne
8.32.02	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerraamwerk.	Basishygiëne
8.33.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico
8.34.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO.	Overheidsrisico