

BIO2 GAP-analyse

Checklist — beheersmaatregelen (ISO 27002:2022) en verplichte overheidsmaatregelen (BIO2)

Gebruik deze checklist om per maatregel vast te leggen waar je organisatie staat. Werk 'm door op papier of in een overleg, en verwerk de uitkomsten daarna in de Excel-versie (met automatisch voortgangsdashboard) op bio2kompas.nl.

Volwassenheid (0–5) · beheersmaatregelen

0 Afwezig · 1 Ad hoc · 2 Herhaalbaar · 3 Gedefinieerd ·
4 Beheerst · 5 Geoptimaliseerd

Opzet · Bestaan · Werking · overheidsmaatregelen

Vink per maatregel af of die is **ontworpen** (O),
ingericht (B) en **aantoonbaar werkt** (W).

Deel 1 · Beheersmaatregelen (93) — ISO 27002:2022

Noteer per maatregel je huidige niveau (0–5) en vink af wanneer je aan je streefniveau voldoet.

Organisatorisch (37)

Control	Beheersmaatregel	Niveau	Voldoet
5.1	Beleidsregels voor informatiebeveiliging		
5.2	Rollen en verantwoordelijkheden voor informatiebeveiliging		
5.3	Scheiding van taken		
5.4	Directieverantwoordelijkheden		
5.5	Contact met overheidsinstanties		
5.6	Contact met speciale belangengroepen		
5.7	Dreigingsinformatie (threat intelligence)		
5.8	Informatiebeveiliging in projectmanagement		
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen		
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen		
5.11	Teruggeven van bedrijfsmiddelen		
5.12	Classificatie van informatie		
5.13	Labelen van informatie		
5.14	Informatieoverdracht		
5.15	Toegangsbeveiliging		
5.16	Identiteitsbeheer		
5.17	Authenticatie-informatie		
5.18	Toegangsrechten		
5.19	Informatiebeveiliging in leveranciersrelaties		
5.20	Aandacht voor informatiebeveiliging in leveranciersovereenkomsten		
5.21	Beheer van informatiebeveiliging in de ICT-toeleveringsketen		
5.22	Monitoren, beoordelen en wijzigingsbeheer van leveranciersdiensten		
5.23	Informatiebeveiliging voor het gebruik van clouddiensten		
5.24	Planning en voorbereiding van beheer van informatiebeveiligingsincidenten		
5.25	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen		

Control	Beheersmaatregel	Niveau	Voldoet
5.26	Reageren op informatiebeveiligingsincidenten		
5.27	Lering uit informatiebeveiligingsincidenten		
5.28	Verzamelen van bewijsmateriaal		
5.29	Informatiebeveiliging tijdens verstoring		
5.30	Gereedheid van ICT voor bedrijfscontinuïteit		
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen		
5.32	Intellectuele-eigendomsrechten		
5.33	Beschermen van registraties		
5.34	Privacy en bescherming van persoonsgegevens (PII)		
5.35	Onafhankelijke beoordeling van informatiebeveiliging		
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging		
5.37	Gedocumenteerde bedieningsprocedures		

Mensen (8)

Control	Beheersmaatregel	Niveau	Voldoet
6.1	Screening		
6.2	Arbeidsvoorwaarden		
6.3	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging		
6.4	Disciplinaire procedure		
6.5	Verantwoordelijkheden bij beëindiging of wijziging van dienstverband		
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten		
6.7	Werken op afstand		
6.8	Rapportage van informatiebeveiligingsgebeurtenissen		

Fysiek (14)

Control	Beheersmaatregel	Niveau	Voldoet
7.1	Fysieke beveiligingszones		
7.2	Fysieke toegang		
7.3	Beveiligen van kantoren, ruimten en faciliteiten		
7.4	Fysieke beveiligingsbewaking		
7.5	Beschermen tegen fysieke en omgevingsdreigingen		
7.6	Werken in beveiligde zones		
7.7	Clear desk en clear screen		
7.8	Plaatsing en bescherming van apparatuur		
7.9	Beveiliging van bedrijfsmiddelen buiten het terrein		
7.10	Opslagmedia		
7.11	Nutsvoorzieningen		
7.12	Beveiliging van bekabeling		
7.13	Onderhoud van apparatuur		

Control	Beheersmaatregel	Niveau	Voldoet
7.14	Veilig verwijderen of hergebruiken van apparatuur		

Technologisch (34)

Control	Beheersmaatregel	Niveau	Voldoet
8.1	Eindpuntapparaten van gebruikers		
8.2	Speciale toegangsrechten		
8.3	Beperking van toegang tot informatie		
8.4	Toegang tot broncode		
8.5	Beveiligde authenticatie		
8.6	Capaciteitsbeheer		
8.7	Bescherming tegen malware		
8.8	Beheer van technische kwetsbaarheden		
8.9	Configuratiebeheer		
8.10	Verwijderen van informatie		
8.11	Maskeren van gegevens		
8.12	Voorkomen van datalekken		
8.13	Back-up van informatie		
8.14	Redundantie van informatieverwerkende faciliteiten		
8.15	Logging		
8.16	Monitoringactiviteiten		
8.17	Kloksynchronisatie		
8.18	Gebruik van speciale systeemhulpmiddelen		
8.19	Installatie van software op operationele systemen		
8.20	Netwerkbeveiliging		
8.21	Beveiliging van netwerkdiensten		
8.22	Scheiding van netwerken		
8.23	Webfiltering		
8.24	Gebruik van cryptografie		
8.25	Veilige ontwikkellevenscyclus		
8.26	Beveiligingseisen voor applicaties		
8.27	Veilige systeemarchitectuur en engineeringprincipes		
8.28	Veilig coderen		
8.29	Beveiligingstesten in ontwikkeling en acceptatie		
8.30	Uitbestede ontwikkeling		
8.31	Scheiding van ontwikkel-, test- en productieomgevingen		
8.32	Wijzigingsbeheer		
8.33	Testinformatie		
8.34	Bescherming van informatiesystemen tijdens audittests		

Deel 2 · Overheidsmaatregelen (117) — BIO2 v1.3 (verplicht)

Toets per maatregel op Opzet (O), Bestaan (B) en Werking (W). Kernvereisten zijn samengevat.

Organisatorisch (54)

OM-nr	Kernvereiste (samengevat)	O	B	W
5.01.01	Vastgesteld informatiebeveiligingsbeleid (door bestuur), met minimaal strategische uitgangspunten, organisatie van de IB-functie, verantwoordelijkheden (ketens/OT/privacy/BCM), betrouwbaarheidseisen, evaluatiefrequentie en bevordering bewustzijn.			
5.01.02	IB-beleid minimaal jaarlijks en aansluitend op bestuurs-/P&C-cycli; en externe ontwikkelingen beoordelen en bijstellen.			
5.02.01	Bestuur legt rollen/verantwoordelijkheden (IB, privacy, OT, BCM) en hun samenhang vast; aandacht voor incidentafhandeling; lijnmanagers/proceseigenaren verantwoordelijk voor risicobehandeling.			
5.02.02	Er is een CISO aangesteld die onafhankelijk en zelfstandig adviseert en rapporteert aan bestuur/controlerend orgaan.			
5.04.01	Bestuur en werknemers volgen regelmatig scholing over cyberrisico's; bestuurders tonen voldoende kennis en vaardigheden aan.			
5.05.01	Overzicht van functionarissen en hun formele contacten met (overheids)instanties en toezichthouders; minimaal jaarlijks actualiseren.			
5.08.01	Bij nieuwe systemen en significante wijzigingen een expliciete risicoafweging uitvoeren en beveiligingseisen vaststellen.			
5.09.01	Actuele inventaris van bedrijfsmiddelen (incl. OT, cloud, remote en niet-beheerde devices); periodiek op volledigheid/actualiteit controleren.			
5.10.02	Gedragsregels voor gebruik bedrijfsmiddelen voor extern personeel/vrijwilligers contractueel vastgelegd.			
5.10.03	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor gebruik van bedrijfsmiddelen.			
5.12.01	Informatie in alle systemen geclassificeerd via een vastgestelde impactclassificatiemethodiek (onderdeel risicomanagementmethodiek).			
5.14.01	Internetfacing-systemen en e-mail voldoen aan de verplichte beveiligingsstandaarden (Forum Standaardisatie/Cyberbeveiligingsbesluit), gemeten via internet.nl.			
5.14.02	Minimaal publiek vertrouwde OV-certificaten bij (openbaar) webverkeer van gevoelige gegevens; intern OV of PKI; hogere eisen uit risicoanalyse.			
5.14.03	Geavanceerde/gekwalificeerde elektronische handtekeningen voldoen aan de AdES Baseline Profiles (Lijst open standaarden).			
5.14.04	Actuele registratie van alle internetfacing-systemen, webapplicaties, IP-adressen en API's.			
5.14.05	Publiek toegankelijke websites bekendmaken via het Register Internetdomeinen Overheid (RIO); minimaal halfjaarlijks actualiseren.			
5.15.01	Toegang tot een vertrouwde zone alleen vanaf geauthentiseerde apparatuur of programmatuur binnen een veilige schil.			
5.16.01	Sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.			
5.16.02	Geen groepsaccounts, tenzij de proceseigenaar dit motiveert, vastlegt en afstemt met de CISO.			
5.17.01	MFA minimaal voor primair aanloggen, internet-bereikbare voorzieningen en beheeraccounts (wachtwoordloos of ww + 2e factor); mitigatie + CISO waar MFA niet kan; monitoring op misbruik.			
5.17.02	Wachtwoordmanager of vergelijkbare oplossing aan alle medewerkers aanbieden.			
5.17.03	Wachtwoordeisen worden geautomatiseerd afgedwongen.			

OM-nr	Kernvereiste (samengevat)	O	B	W
5.18.01	Aanmaken/wijzigen van accounts met bijzondere rechten wordt gemonitord; ongeautoriseerde wijziging = informatiebeveiligingsincident.			
5.18.02	Alle uitgegeven toegangsrechten minimaal jaarlijks beoordelen (sneller o.b.v. risicoafweging).			
5.19.01	Bij offerteaanvragen zijn IB-eisen (beschikbaarheid/integriteit/vertrouwelijkheid) onderdeel van de inkoop-eisen, o.b.v. risicoafweging.			
5.20.01	Beveiligingseisen uit de offerteaanvraag expliciet opnemen in (inkoop)contracten.			
5.20.02	Algemene voorwaarden van leveranciers waar mogelijk uitsluiten; anders risico's beoordelen en geaccepteerde/geweigerde consequenties expliciteren.			
5.20.03	Contractueel: leverancier toont jaarlijks (opzet/bestaan/werking) via onafhankelijke onderzoeken aan te voldoen, incl. toeleveringsketen.			
5.20.04	Entiteit voert zelfstandig onderzoek/validatie uit; mogelijkheid tot externe audit contractueel geborgd; restrisico's beheersen.			
5.20.05	Leverancier is transparant over kwetsbaarheden en incidenten (waaronder datalekken) in de dienstverlening.			
5.20.06	Vooraf risicoafweging of leveranciersafhankelijkheid beheersbaar is; exit-strategie is vast onderdeel van het contract.			
5.21.02	Leverancier geeft vooraf inzicht in de keten van toeleveranciers en risico's; entiteit beoordeelt acceptatie.			
5.21.03	Beveiligingseisen gelden onverminderd voor de hele toeleveringsketen (tenzij niet relevant, met onderbouwing).			
5.21.04	Leverancier geeft veranderingen in de keten en bijbehorende risico's door gedurende de looptijd.			
5.21.05	Beveiliging van toeleveringsketens is onderdeel van de risicoanalyse (kwetsbaarheden, kwaliteit, praktijken toeleveranciers).			
5.22.01	Proceseigenaar beoordeelt jaarlijks o.b.v. bewijs of de leverancier voldoet; stelt risico's vast; neemt/accepteert mitigatie.			
5.22.02	Actuele registratie van leveranciers en afgesloten contracten.			
5.23.01	Beleid voor inventariseren/classificeren/selecteren/beoordelen/beëindigen van cloud service providers; minimaal driejaarlijks herzien.			
5.24.01	Toegankelijk meldloket voor IB-incidenten voor alle interne en externe medewerkers.			
5.24.02	Meldprocedure met taken en verantwoordelijkheden van het meldloket.			
5.24.03	Proceseigenaar is verantwoordelijk voor het oplossen van IB-incidenten.			
5.24.04	Proceseigenaar rapporteert maandelijks de opvolging van incidenten aan de eindverantwoordelijke voor de bedrijfsvoering.			
5.24.05	De incidentprocedure verwijst naar de procedure voor crisisbeheersing.			
5.24.07	Incidentprocedure borgt: melden bij CSIRT binnen wettelijke termijn, verwerken van CSIRT-meldingen en tijdig informeren van betrokkenen.			
5.24.08	Coordinated Vulnerability Disclosure (CVD)-procedure ingericht en gepubliceerd (NCSC-leidraad of ISO/IEC 29147); CVD-meldingen in de incidentrapportage.			
5.26.02	Incidenten afdoen via het incidentbeheerproces; relevante incidenten gemeld bij aangewezen toezichthouders.			
5.27.01	Incidenten analyseren op achterliggende oorzaken en verbeteringen om herhaling te voorkomen.			
5.27.02	Analyses (oorzaken + verbeteringen) breed delen met relevante partners.			
5.28.01	Bewaartermijn van (vermoedelijke) incidentinformatie minimaal drie jaar (logging, oplossing, advies).			

OM-nr	Kernvereiste (samengevat)	O	B	W
5.30.01	Proceseigenaar test jaarlijks de continuïteitsplannen op werking, volledigheid en actualiteit.			
5.30.02	Kritieke systemen identificeren o.b.v. risicoafweging; overzicht minimaal driejaarlijks actualiseren.			
5.33.01	Bewaartermijnen in selectielijsten vastgelegd (archiefwet/privacy), praktisch ingeregeld en periodiek getoetst.			
5.35.02	Vastgesteld auditplan met jaarlijkse keuzes voor welke systemen welke beveiligingsaudits krijgen.			
5.36.01	Rapportage over IB in de P&C-/PDCA-cyclus onder CISO-coördinatie, resulterend in een jaarlijkse In Control Verklaring (of vergelijkbaar).			

Mensen (7)

OM-nr	Kernvereiste (samengevat)	O	B	W
6.01.01	Vastgesteld screeningsbeleid; VOG o.b.v. risicoafweging bij indiensttreding en functiewijziging.			
6.02.01	Medewerkers (intern/extern) bij aanstelling/functiewissel gewezen op hun IB-verantwoordelijkheden; regelingen eenvoudig toegankelijk.			
6.03.01	Iedereen kent de regels en verplichtingen voor IB, en waar relevant de eisen voor gerubriceerde omgevingen.			
6.03.02	Training I-bewustzijn aantoonbaar succesvol gevolgd binnen drie maanden na indiensttreding.			
6.03.03	Management benadrukt en stimuleert actief het periodiek volgen van IB-opleiding/training.			
6.03.04	Bewustwordingsprogramma's behandelen de gedragsaspecten van veilig mobiel werken.			
6.08.01	Medewerkers (intern/extern) hebben aantoonbaar kennisgenomen van de meldingsprocedure voor incidenten.			

Fysiek (6)

OM-nr	Kernvereiste (samengevat)	O	B	W
7.01.02	Kritieke informatie of informatiesystemen zijn nooit via één beveiligde zone te bereiken.			
7.02.01	Bij concrete beveiligingsrisico's worden waarschuwingen volgens afspraak verzonden aan relevante collega's binnen het beveiligingsdomein.			
7.07.01	Bij gebruik van een chipcardtoken activeert het verwijderen van het token automatisch de toegangsvergrendeling.			
7.10.01	Verwijderinstructie borgt dat bedrijfsgevoelige inhoud op herbruikbare media die de entiteit verlaten onherstelbaar is verwijderd.			
7.10.02	Gecontroleerd (met verslag) dat alle data onherstelbaar is verwijderd; waar mogelijk NBV/AIVD-geadviseerde producten.			
7.10.03	Koeriers/transporteurs voor geclassificeerde informatie voldoen aan vooraf opgestelde betrouwbaarheidseisen.			

Technologisch (50)

OM-nr	Kernvereiste (samengevat)	O	B	W
8.01.01	Mobiele apparatuur 'zero footprint'; anders toegangsbescherming met minimaal versleuteling; 'wissen op afstand' mogelijk.			
8.01.02	Mobiele apparatuur: patchmanagement/hardening, MDM/MAM, ondertekende gebruikersovereenkomst mobiel werken; periodiek getoetst.			
8.02.01	Speciale bevoegdheden minimaal ieder kwartaal beoordeeld op opzet, bestaan en werking.			
8.03.01	Maatregelen die fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.			

OM-nr	Kernvereiste (samengevat)	O	B	W
8.03.02	Need-to-know: gebruikers zien/verwerken alleen informatie die nodig is voor hun taak.			
8.05.01	Vooraf risicoafweging voor netwerktoegang van externe leveranciers (voorwaarden/duur); rechten uit registratie herleidbaar.			
8.07.01	Downloaden beheerst en beperkt o.b.v. risico en need-of-use; antimalware beoordeelt altijd alle downloads.			
8.07.02	Gebruikers zijn voorgelicht over de risico's van surfgedrag en het klikken op onbekende links.			
8.07.03	Antimalware- en herstelsoftware zijn actueel en worden periodiek geüpdatet.			
8.07.04	Malwarescan op alle omgevingen, op alle downloads vóór executie/opslag en op alle ontvangen bestanden vóór gebruik.			
8.08.01	Bij hoge kans én hoge schade: mitigerende maatregelen zo snel mogelijk, uiterlijk binnen een week.			
8.08.02	Wijze van mitigatie bepalen op basis van een expliciete risicoafweging.			
8.08.03	Tussentijdse mitigerende maatregelen als patchen binnen een week niet mogelijk is.			
8.08.04	Systemen waar mogelijk jaarlijks controleren op naleving/kwetsbaarheden (scans/pentests/red-teaming); internetfacing continu.			
8.08.05	Internetfacing-systemen: verplichte (geautomatiseerde) pentest bij elke release/major update; hoog-risicobevindingen blokkeren productie; minimaal jaarlijks getest.			
8.13.01	Back-upbeleid met bewaar-/beschermeisen; speciale aandacht voor bescherming tegen ransomware en integriteit van de back-up.			
8.13.02	Maximaal toegestaan dataverlies (RPO) en maximale hersteltijd (RTO) bepaald o.b.v. risicoafweging.			
8.13.03	Back-up opgeslagen op een gescheiden locatie zodat één incident niet beide raakt.			
8.13.04	Herstelprocedure minimaal jaarlijks (of na een grote wijziging) getest.			
8.15.01	Logregel bevat minimaal: actie, object, resultaat, oorsprong, actor en tijdstempel.			
8.15.02	Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.			
8.15.03	Er is een overzicht van de logbestanden die worden gegenereerd.			
8.15.04	Bewaartermijn van logs/SIEM risicogericht bepaald (rekening houdend met langdurig aanwezig aanvallers).			
8.15.05	Oneigenlijk wijzigen/verwijderen van loggegevens zo snel mogelijk melden als incident.			
8.15.06	Periodieke, onafhankelijke toetsing op het ongewijzigd bestaan van logs gedurende de bewaartermijn.			
8.16.01	Nieuwe dreigingen (uit 8.16.03) binnen juridische kaders verplicht delen met het aangewezen CERT.			
8.16.02	SIEM/SOC heeft eenduidige regels wanneer een incident aan het verantwoordelijke management wordt gerapporteerd.			
8.16.03	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing.			
8.16.04	Actieve netwerkcomponenten voorzien van logging én monitoring van die logging.			
8.18.01	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen, en uitsluitend wanneer strikt noodzakelijk.			
8.18.02	Gebruik van systeemhulpmiddelen wordt gelogd; logging minimaal een half jaar beschikbaar voor onderzoek.			
8.19.01	Het risico van installatie van niet-geautoriseerde software door gebruikers wordt beheerst.			

OM-nr	Kernvereiste (samengevat)	O	B	W
8.20.01	Netwerkkomponenten voldoen minimaal aan het vertrouwelijkheidsniveau van het netwerk waarvan ze deel uitmaken.			
8.20.02	Toegang tot beheerinterfaces van netwerkkomponenten zoveel mogelijk gescheiden van het gebruikersnetwerk.			
8.21.01	Koppelpunten met externe/onvertrouwde zones: maatregelen om beschikbaarheidsaanvallen te signaleren en mitigeren.			
8.21.02	Dataverkeer van/naar de vertrouwde omgeving wordt bewaakt en geanalyseerd op verdacht verkeer met detectievoorzieningen.			
8.21.03	Nieuwe dreigingen (uit 8.21.02) binnen juridische kaders gedeeld binnen de overheid.			
8.21.04	Draadloos verkeer en bedraad verkeer buiten gecontroleerd gebied versleuteld (waar mogelijk NBV/AIVD-geadviseerde middelen).			
8.22.01	Alle gescheiden netwerkgroepen hebben een gedefinieerd beveiligingsniveau.			
8.24.01	Cryptografiebeleid met minimaal: wanneer cryptografie, verantwoordelijkheden implementatie/sleutelbeheer, registratie, normen (Forum Standaardisatie) en beschermingsniveau.			
8.24.02	Cryptografische maatregelen opgenomen in de inventaris; vastgesteld waar ingezet, wie verantwoordelijk en hoe actueel gehouden.			
8.24.04	Sterkte van cryptografie gebaseerd op de actuele adviezen van NCSC en NBV/AIVD.			
8.24.05	Afspraken over reservecertificaten van een alternatieve leverancier indien nodig voor bedrijfscontinuïteit.			
8.27.01	Architectuurprincipes 'security by design/default' vastgesteld, gedocumenteerd, onderhouden en toegepast bij systeemontwikkeling.			
8.29.01	Acceptatietesten met gestructureerde (waar mogelijk geautomatiseerde) testmethodieken; van resultaten verslag gemaakt.			
8.30.01	Interne maatregelen voor systeemontwikkeling onverkort van toepassing op uitbestede ontwikkeling, aangevuld met uitbestedingsmaatregelen.			
8.31.01	In de productieomgeving wordt niet getest, tenzij vooraf goedgekeurd door de proceseigenaar.			
8.31.02	Significante wijzigingen altijd getest vóór productie, tenzij vooraf goedgekeurd door de proceseigenaar.			
8.32.01	Wijzigingsbeheerproces met minimaal: administratie + testresultaten, risicoafweging incl. rollback-plan, en goedkeuringsprocedure.			
8.32.02	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerraamwerk.			

Bron: beheersmaatregelen volgen NEN-EN-ISO/IEC 27002:2022 (nl); overheidsmaatregelen volgen BIO2 v1.3 (9 januari 2026), Deel 2. Kernvereisten zijn samengevat — raadpleeg de officiële BIO2 en de ISO-norm voor de exacte, geldende tekst. Een aantal overheidsmaatregelen valt buiten de reikwijdte van de Cyberbeveiligingswet (verplichtende zelfregulering); controleer dit in de officiële BIO2.

Meer uitleg per control en de Excel-versie met dashboard: bio2kompas.nl/praktijk/gap-analyse