

	Systeemdokumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Leeswijzer

Baseline Informatiebeveiliging Overheid (BIO) Interpretatie naar de praktijk Reikwijdte: (intelligente) Verkeer Regel Installaties



K109 Martelaarsgracht

Auteurs:

Eric Bish Sr. Projectleider & Adviseur Systemen
Hans Hoets Sr. Adviseur Verkeer Regel Installaties

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Management samenvatting

De gemeente Amsterdam dient als Overheid organisatie zich te conformeren aan de richtlijnen ten aanzien van Informatiebeveiliging voor de gehele overheid. Het normenkader “Baseline Informatiebeveiliging Overheid (BIO)” beschrijft alle maatregelen en controles die er voor moeten zorgen dat de omgang met informatie (data) in systemen en door eindgebruikers op correcte wijze plaats vindt. De beschikbaarheid, integriteit en vertrouwelijkheid moet geborgd zijn.

Op de website <https://bio-overheid.nl/> is het normenkader beschreven en is publiekelijk beschikbaar voor iedereen. De set van maatregelen en controle punten zijn in de vorm van een tekst document beschikbaar en toegevoegd in de bijlage van dit document. Hoofdstukken 5 t/m 18 van het BIO document bevatten de feitelijke lijst met maatregelen en controlepunten. De lijst is ook in de vorm van een Excelsheet beschikbaar gesteld op de website. Dit Excelsheet is het uitgangspunt voor dit document.

Wanneer de maatregelen en controle punten worden bekeken, dan blijkt daaruit meestal al vrij snel wat de bedoeling is voor iemand die werkzaam is in de automatisering. Het probleem met de gekozen vorm waarin het BIO raamwerk is vastgelegd is dat de maatregelen zijn voortgekomen vanuit een kantoor automatisering perspectief en een te hoog-over abstractie niveau hebben. In deze vorm is de lijst niet geschikt om als concrete systeemeisen voor te leggen aan leveranciers werkzaam in het industriële domein. Het implementeren van de BIO is daardoor in de praktijk een moeizame aangelegenheid gebleken en de interpretatie van de maatregelen is niet eenduidig.

Dit document is opgesteld om mee te geven als een eisenlijst bij een aanbesteding voor levering, beheer en onderhoud van Verkeer Regel Installaties . De BIO is geïnterpreteerd en vertaald in concrete eisen en maatregelen gericht specifiek en uitsluitend op (intelligente) Verkeer Regel Installaties (VRI). De (i)VRI wordt hierbij beschouwd als een “Network endpoint device” aangesloten op een IT besturingsnetwerk en dat geplaatst is in een straatkast. De reikwijdte en de focus van de maatregelen beschreven in dit document zijn daarop gericht.

Alhoewel er zeer grote overeenkomsten zullen bestaan kan dit document niet 1-op-1 toegepast worden voor andere assets die in beheer zijn van Team Licht. Voor andere assets zal de interpretatie voor die nieuwe situatie opnieuw doorlopen moeten worden en zullen asset specifieke eisen gedefinieerd moeten worden.

Een beperkt deel van de maatregelen en controle punten van de BIO is gericht op de beheer organisatie van de opdrachtgever (gemeente Amsterdam) en een aanzienlijk deel op die van de opdrachtnemer ((i)VRI leverancier) onder de aannahme van desktop of server applicaties voor gebruik door medewerkers. Wanneer specifiek en alleen naar een VRI wordt gekeken zijn dit soort maatregelen en controle punten in deze specifiek context niet van toepassing en daarom niet overgenomen in de eisenlijst.

De maatregelen en controlepunten die worden overgeslagen zijn in algemene zin echter wel zeer waardevol. In een andere context en waarbij er een werkrelatie bestaat tussen de opdrachtgever en de

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

opdrachtnemer zal een separate BIO toets tegen de automatiseringsomgevingen van beide partijen uitgevoerd moeten worden, maar dat valt dus buiten de reikwijdte van dit document.

Mogelijk dat bij de implementatie van de maatregelen ook wijzigingen in de organisatie van de opdrachtnemer belegd moeten gaan worden.

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Versie historie

Historie

Versie	Status	Wijzigingen	Auteur	Datum
1.0 Concept	Initiële versie	Initieel document	E. Bish	30 januari 2021
1.1 Concept	Concept	Tekstuele wijzigingen HH	E. Bish	7 februari 2021
1.2 Concept	Concept	Tekstuele wijzigingen project team	E. Bish	8 februari 2021
1.3	Uitgave	Toelichting OTAP	E. Bish	31 augustus 2021

Distributie

Naam	Organisatie	Rol
E. Bish	Verkeer en Openbare Ruimte	Adviseur en Projectleider Systemen
H. Hoets	Verkeer en Openbare Ruimte	Adviseur Verkeer Regel Installaties
E. Breems	Verkeer en Openbare Ruimte	Security Officer
E. Folten	Verkeer en Openbare Ruimte	Assetmanager Verkeer Regel Installaties

	Systeemdokumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Inhoudsopgave

Leeswijzer	1
Management samenvatting	2
Versie historie.....	4
Inleiding en context.....	6
1 Baseline Informatiebeveiliging Overheid (BIO)	7
Hoe zit het in elkaar?	8
Het forum	9
Basis Beveiligingsniveau (BBN)	10
Werken volgens het Plan-Do-Check-Act (PDCA) principe	11
Ontwikkel Test Acceptatie Productie (OTAP)	11
Voor wie van toepassing?.....	12
Indeling in Controls en maatregelen	12
2 Interpretatie van de BIO in de praktijk - Toelichting	13
Probleemstelling.....	13
Oplossingsrichting	13
3 Interpretatie van de BIO in de praktijk – De actie lijst	15
Bijlage1 Baseline Informatiebeveiliging Overheid (BIO)	18

	Systeemdokumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Inleiding en context

De gemeente Amsterdam dient als Overheid organisatie zich te conformeren aan de richtlijnen ten aanzien van Informatiebeveiliging voor de gehele overheid. Het normenkader “Baseline Informatiebeveiliging Overheid (BIO)” beschrijft alle maatregelen en controles die ervoor moeten zorgen dat de omgang met informatie (data) in systemen en door eindgebruikers op correcte wijze plaats vindt. De beschikbaarheid, integriteit en vertrouwelijkheid moet geborgd zijn.

Wanneer de maatregelen en controle punten worden bekeken, dan blijkt daaruit meestal al vrij snel wat de bedoeling is voor iemand die werkzaam is in de automatisering. Het probleem met de gekozen vorm is dat de maatregelen zijn voortgekomen vanuit een kantoorautomatisering perspectief en een te hoog-over abstractie niveau hebben. In deze vorm is de lijst niet geschikt om als concrete systeemeisen voor te leggen aan leveranciers werkzaam in het industriële domein. Het implementeren van de BIO is daardoor in de praktijk een moeizame aangelegenheid gebleken en de interpretatie van de maatregelen is niet eenduidig.

Veel areaal beheerders ervaren de BIO en het thema Informatiebeveiliging als moeilijk toegankelijke materie en als een enorme last om eraan te voldoen. Door middel van dit document willen wij het onderwerp wat gemakkelijker toegankelijk maken en meer op de praktijk richten.

Het document is opgesteld om mee te geven als een eisenlijst bij een aanbesteding voor levering, beheer en onderhoud van Verkeer Regel Installaties. De BIO is geïnterpreteerd en vertaald in concrete eisen en maatregelen gericht specifiek en uitsluitend op (intelligente)Verkeer Regel Installaties ((i)VRI). De (i)VRI wordt hierbij beschouwd als een “Network Endpoint device” aangesloten op een IT besturingsnetwerk en dat geplaatst is in een straatkast. De reikwijdte en de focus van de maatregelen beschreven in dit document zijn precies daarop gericht.

Alhoewel er zeer grote overeenkomsten zullen bestaan kan dit document niet 1-op-1 toegepast worden voor andere assets die in beheer zijn van Team Licht. Voor andere assets zal de interpretatie voor die nieuwe situatie opnieuw doorlopen moeten worden en zullen asset specifieke eisen gedefinieerd moeten worden.

Leeswijzer:

Hoofdstuk 1 is een uitleg van de BIO, geeft aan waar de documenten zijn te vinden en volgens welke principes wordt gewerkt.

Hoofdstuk 2 is de toelichting op de wensen en eisenlijst die is opgesteld om het leveranciers van de gemeente gemakkelijker te maken systemen te ontwikkelen die bij implementatie bij een overheidspartij zoals de gemeente BIO compliant zijn.

Hoofdstuk 3 is de lijst met acties voor de opdrachtgever en de opdrachtnemer.

	Systeemdokumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

1 Baseline Informatiebeveiliging Overheid (BIO)

In dit hoofdstuk wordt in beknopte vorm toegelicht wat de BIO inhoudt en waar alle relevante informatie gevonden kan worden.

Voor een veilige digitale overheid

Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor [Rijk](#), [Gemeenten](#), [Waterschappen](#) en [Provincies](#). Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. Helder, actueel en veilig.

De BIO bestaat uit een verzameling van “controls” en “maatregelen” die als een soort checklist gebruikt worden om te controleren of een systeem robuust genoeg is op het vlak van Informatievoorziening. Het begrip Informatievoorziening is niet eenduidig (hard) gedefinieerd. Wanneer op Internet gezocht wordt naar de definitie kom je verschillende varianten tegen. Onderstaande definitie¹ is één van de meest beschrijvende varianten:

Een geautomatiseerd informatiesysteem is het geheel van apparatuur met daarbij behorende basisprogrammatuur en toepassingsprogrammatuur, gegevensverzamelingen, procedures en personen voor het kennen en/of besturen/ondersteunen van reële systemen ofwel bedrijfsprocessen. De apparatuur, programmatuur etc. zijn te beschouwen als de informatiesysteemcomponenten.

Vijf componenten van het geautomatiseerde informatiesysteem:

- *Apparatuur.*
- *Programmatuur (basis en toepassing).*
- *Gegevensverzamelingen.*
- *Mensen.*
- *Procedures.*

¹ Bron: <http://www.raamstijn.nl/eenblogjeom/index.php/informatiemanagement/5173-informatievoorziening-volgens-maarten-looijen>

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Een applicatie duidt op dat deel van het informatiesysteem dat de toepassingsprogrammatuur en de daarbij behorende gestructureerde gegevensverzamelingen omvat. Dit deel vertegenwoordigt de functionaliteiten van het informatiesysteem.

In de praktijk wordt applicatie ook wel gebruikt om daarmee een informatiesysteem in zijn totaliteit weer te geven. (...) Zonder een goede definitie geeft het gebruik van de term applicatie aanleiding tot misverstanden.

Informatievoorziening is het geheel aan activiteiten dat voor een organisatie moet worden uitgevoerd om iedereen de informatie te verstrekken die nodig is om toegewezen functies te vervullen. In dat verband is informatievoorziening een organisatorisch begrip. Binnen de informatievoorziening bevinden zich informatiesystemen.

Deze beschrijving is in een niet-specifieke vorm opgesteld. In de context van een industriële omgeving voor het besturen van objecten in de openbare ruimte, waarbij ook prestatie- en logging gegevens worden opgehaald, vallen de volgende componenten binnen het aandachtsgebied van Informatiebeveiliging:

- Het object in de openbare ruimte als samenhangend systeem (bijvoorbeeld een (i)Verkeer Regel Installatie, of een toezichtcamera voor het verkeer.)
- De dataverbinding met dat object.
- De besturingsapplicatie van dat object.
- De risico's op verstoring van de correcte werking van dat object.
- De impact van een mogelijke verstoring op het veilig en correct functioneren van het object.
- De kwetsbaarheid van het object ten aanzien van een kwaadwillende.
- De veilige, correcte en gecontroleerde omgang met het object.
- De aard van de data die met het object wordt uitgewisseld. (bijvoorbeeld camera beelden worden als privacy gevoelig gezien en moeten goed beschermd worden.)
- De omgang en bescherming van digitale identiteiten. Identiteitsfraude is in toenemende mate een probleem.
- Het voorkomen van datalekken.
- Het algemeen veiligheidsbewustzijn van de organisatie. Het periodiek herhalen van trainingen om dit bewustzijn vast te houden.
- Het eenduidig vastleggen van eigendomsrechten en intellectueel eigendom van configuratiegegevens, autorisatiegegevens, licenties, systeemsoftware, applicaties e.d.

Hoe zit het in elkaar?

Op de website <https://bio-overheid.nl/> is het normenkader beschreven en is publiekelijk beschikbaar voor iedereen.

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

De set van maatregelen en controle punten zijn in de vorm van een tekst document beschikbaar via https://bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf

Deel1 van het BIO document bestaat uit de hoofdstukken 1 t/m 4 waarin de BIO in detail wordt uitgelegd.

Deel2 van het BIO document bestaat uit de hoofdstukken 5 t/m 18 en bevatten de feitelijke lijst met maatregelen en controlepunten.

De lijst is ook in de vorm van een Excelsheet beschikbaar gesteld op de website via de link:

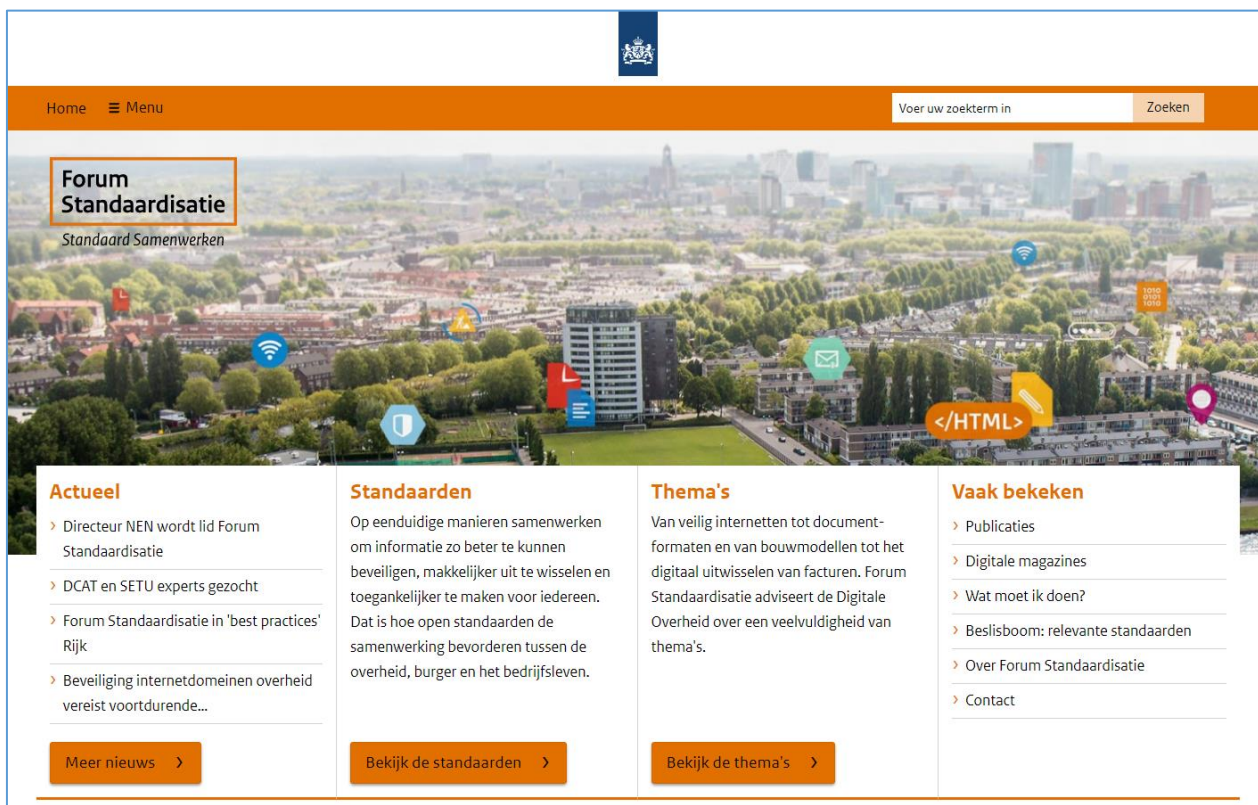
<https://bio-overheid.nl/media/1404/baseline-informatiebeveiliging-overheid-104-spreadsheet.xlsx>

Dit Excelsheet is het uitgangspunt voor dit document.

De BIO is een interpretatie van de generieke ISO27001 en ISO27002 normenkaders. De BIO volgt de indeling van de ISO 27002 zodat bedrijven of leveranciers die een certificering hebben met dit normenkader weinig moeite zullen hebben.

Het forum

Binnen de BIO maatregelen wordt regelmatig verwezen naar het “forum”. Dit betreft een verwijzing naar de website <https://www.forumstandaardisatie.nl/>.



Forum Standaardisatie
Standaard Samenwerken

Home Menu Voer uw zoekterm in Zoeken

Actueel

- > Directeur NEN wordt lid Forum Standaardisatie
- > DCAT en SETU experts gezocht
- > Forum Standaardisatie in 'best practices' Rijk
- > Beveiliging internet domeinen overheid vereist voortdurende...

Meer nieuws >

Standaarden

Op eenduidige manieren samenwerken om informatie zo beter te kunnen beveiligen, makkelijker uit te wisselen en toegankelijker te maken voor iedereen. Dat is hoe open standaarden de samenwerking bevorderen tussen de overheid, burger en het bedrijfsleven.

Bekijk de standaarden >

Thema's

Van veilig internetten tot documentformaten en van bouwmodellen tot het digitaal uitwisselen van facturen. Forum Standaardisatie adviseert de Digitale Overheid over een veelvoudigheid van thema's.

Bekijk de thema's >

Vaak bekeken

- > Publicaties
- > Digitale magazines
- > Wat moet ik doen?
- > Beslisboom: relevante standaarden
- > Over Forum Standaardisatie
- > Contact

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Deze website van de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties bevat onder andere lijsten van verplichte en aanbevolen standaarden².

Een aansprekend voorbeeld van een verplichte standaard is het gebruik van Transport Layer Security (TLS) voor verbindingen tussen systemen die data uitwisselen. Op zo'n verplichting berust het "pas toe of leg uit" principe³.

Het komt erop neer dat wanneer TLS niet toegepast kan worden, dat er dan een gelijkwaardig alternatief gebruikt moet worden of in een extreem geval het risico van niet toepassen bewust geaccepteerd zal moeten worden en voortdurend naar verbeteringen gezocht zal moeten worden.

Een aansprekend voorbeeld van een aanbevolen standaard is het gebruik van de web programmeertaal HTML en het web protocol HTTP(S) voor websites. Deze aanbevolen standaarden zijn dus niet verplicht maar worden aangemoedigd om te gebruiken om de communicatie (interoperabiliteit) tussen systemen te vereenvoudigen.

Basis Beveiligingsniveau (BBN)

Er zijn 3 niveaus van beveiliging benoemd. Elk systeem van de overheid moet minimaal aan niveau 1 voldoen. De eisen voor de hogere niveaus zijn cumulatief. Een systeem op BBN2 niveau moet dus ook aan de eisen voor BBN1 voldoen en daarnaast aan aanvullende eisen voor het BBN2 niveau.

BBN1

- Het systeem moet aan wet en regelgeving voldoen voor zover van toepassing.
- Het systeem moet aan algemene beveiligingsprincipes voldoen (best-practices).

BBN2

- Het systeem voldoet aan de BBN1 eisen.
- Indien het systeem vertrouwelijke informatie verwerkt.
- Indien mogelijke incidenten leiden tot bestuurlijke commotie.
- Indien de veiligheid van andere systemen afhankelijk is van dit systeem.

BBN3

Dit niveau is niet van toepassing op de systemen onder beheer van de Gemeente Amsterdam-Verkeer en Openbare Ruimte – Team Licht. Dit is van toepassing op systemen van bijvoorbeeld defensie en andere gevoelige systemen van de overheid die weerstand moeten bieden tegen statelijke actoren en beroepscriminelen.

² Deze lijsten zijn in bijlage 1 opgenomen.

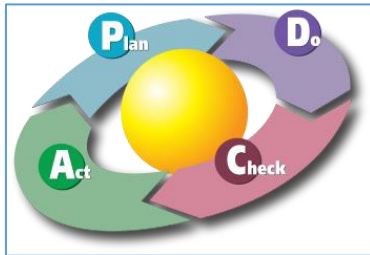
³ Zie voor een uitleg van dit principe: https://nl.wikipedia.org/wiki/Pas_toe_of_leg_uit

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

>> De (intelligente) Verkeer Regel Installaties vallen in de categorie BBN2 hetgeen het standaard niveau is voor data verwerkende systemen binnen de overheid.

Voor BBN2 geldt dat de proceseigenaar het informatiesysteem voor ingebruikname bij voorkeur al in de ontwerp-/ontwikkelfase ter consultatie voorlegt aan de medewerker die de rol van Chief Information Security Officer (CISO) vervult. In de praktijk zal dit betekenen dat wanneer een opdrachtnemer of leverancier een significante wijziging aan de werking of opzet van het systeem wil doorvoeren, en dat deze wijziging van invloed kan zijn op Informatiebeveiliging, deze eerst door de opdrachtgever geaccordeerd zal moeten worden. Zowel opdrachtgever als opdrachtnemer rapporteren over de mogelijke consequenties op het gebied van Informatiebeveiliging.

Werken volgens het Plan-Do-Check-Act (PDCA) principe



Informatiebeveiliging is geen eenmalige actie. Het beveiligen van systemen vereist voortdurend aandacht en aanwezige beveiligingen moeten periodiek op hun effectiviteit beoordeeld worden en zo nodig moeten aanvullende beveiligingen aangebracht worden. Er is sprake van een cyclische beweging volgens het PDCA principe⁴.

De insteek van risicomanagement in het kader van de BIO is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging.

Ontwikkel Test Acceptatie Productie (OTAP)

Omdat de BIO is ontwikkeld binnen kantoor automatiserings omgevingen kunnen er begrippen of principes worden toegepast die niet als algemeen bekend verondersteld mogen worden. Eén belangrijk werkingsprincipe is het gebruik van gescheiden omgevingen volgens de OTAP⁵ indeling gedurende de levenscyclus van een automatiseringsproduct. De Ontwikkel en Test omgevingen zijn aanwezig bij de systeemleverancier. De producten die door de leverancier goed door alle testen zijn gekomen worden overgebracht naar de Acceptatie omgeving van de opdrachtgever om de nieuwe versie of doorgevoerde wijziging te kunnen beoordelen op functionele, technische en beveiligingsaspecten. Zo'n acceptatie omgeving kan in het geval van een (i)VRI bestaan uit een installatie die nog niet op straat is geplaatst en standaard al via een FAT procedure⁶ wordt getest. Na een succesvolle acceptatie kan de (i)VRI in productie genomen worden door deze in de openbare ruimte in gebruik te nemen. Het is nadrukkelijk de bedoeling om verstoringen in de productie situatie te voorkomen. Ongecontroleerde wijzigingen dienen altijd voorkomen te komen om de beschikbaarheid en stabiliteit van de dienstverlening zo groot mogelijk te maken.

⁴ Zie voor een uitleg van dit principe: <https://en.wikipedia.org/wiki/PDCA>

⁵ Zie voor een uitleg van dit principe: <https://nl.wikipedia.org/wiki/OTAP>

⁶ Zie voor een uitleg van dit principe: <https://nl.wikipedia.org/wiki/Acceptatietest>

	Systeemdokumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Voor wie van toepassing?

Externe leveranciers zijn geen onderdeel van de overheid en zijn daarmee zelf niet rechtstreeks gebonden aan de BIO. Ze moeten wel voldoen aan de eisen van de opdrachtgever. De gemeente Amsterdam is opdrachtgever en is wel verplicht gehouden aan de BIO. Voorwaarden ten behoeve van informatiebeveiliging moeten daarom altijd in het contract met de opdrachtnemer zijn vastgelegd.

Indeling in Controls en maatregelen

De hoofdstukken 5 t/m 18 van de BIO omvatten het 2^e deel van het BIO document. Deze hoofdstukken zijn verdeeld over 13 “Controls” (thema’s) die hieronder staan vermeld.

- (05) Informatiebeveiligingsbeleid
- (06) Organiseren van informatiebeveiliging
- (07) Veilig personeel
- (08) Beheer van bedrijfsmiddelen
- (09) Toegangsbeveiliging
- (10) Cryptografie
- (11) Fysieke beveiliging en beveiliging van de omgeving
- (12) Beveiliging bedrijfsvoering
- (13) Communicatiebeveiliging
- (14) Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- (15) Leveranciersrelaties
- (16) Beheer van informatiebeveiligingsincidenten
- (17) Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- (18) Naleving

Voor elke control is een set van maatregelen van toepassing. Er zijn in totaal ruim meer dan 100 maatregelen genoemd. In algemene zin zijn de maatregelen allen gericht op :

- Het toetsen op in gebruik zijn van een goede deugdelijke procedure om Informatiebeveiliging onder controle te houden.
- Het eenduidig beleggen van verantwoordelijkheden.
- Het implementeren van passende technische maatregelen.
- Het implementeren van procedures voor veilige en bewuste omgang met informatiebeveiliging aspecten.

In de uitwerking van de BIO voor de gemeente Amsterdam is in een klein aantal gevallen aan een enkele control een maatregel toegevoegd die moet zorgen voor een meer specifieke uitvraag of detaillering.

 Gemeente Amsterdam VOR-IN Infrastructure Services	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

2 Interpretatie van de BIO in de praktijk - Toelichting

Dit hoofdstuk beschrijft hoe een praktische invulling is gegeven aan het BIO normenkader om de implementatie begrijpelijker en minder ingrijpend te maken.

Probleemstelling

In hoofdstuk 1 is uitgelegd wat de Baseline Informatiebeveiliging Overheid precies is, waar de betreffende documenten zijn te vinden en hoe de indeling is opgezet. De beschrijving van hoofdstuk 1 is een vereenvoudigde voorstelling om een onervaren lezer op het vlak van Informatiebeveiliging op weg te helpen. Het bron bestand op de website van BIO-Overheid.nl bevat alle details, is de actuele versie en is leidend in geval van twijfel of onduidelijkheid.

Wanneer de maatregelen en controle punten worden bekeken, dan blijkt daaruit meestal al vrij snel wat de bedoeling is voor iemand die werkzaam is in de automatisering. Het probleem met de gekozen vorm waarin het BIO raamwerk is vastgelegd is dat de maatregelen zijn voortgekomen vanuit een kantoor automatisering perspectief en een te hoog-over abstractie niveau hebben. In deze vorm is de lijst niet geschikt om als concrete systeemeisen voor te leggen aan leveranciers werkzaam in het industriële domein. Het implementeren van de BIO is daardoor in de praktijk een moeizame aangelegenheid gebleken en de interpretatie van de maatregelen is niet eenduidig.

Veel areaal beheerders en leveranciers ervaren de BIO en het thema Informatiebeveiliging als moeilijk toegankelijke materie en als een enorme last om er aan te voldoen. In veel gevallen is er ook sprake van onvoldoende bewustzijn ten aanzien van Informatiebeveiliging hetgeen aanleiding kan geven tot kwetsbare systemen die achteraf weer gerepareerd of aangepast moeten worden.

Oplossingsrichting

Als overheidsorganisatie willen we dat onze systemen veilig zijn te gebruiken, betrouwbaar werken en geen onnodige risico's opleveren voor bijvoorbeeld privacy of het lekken van data. Dit komt overeen met de doelstellingen van de BIO waarmee gepoogd wordt risico's op falende systemen, lekken van data en schenden van privacy te minimaliseren en onder controle te houden.

De controls en maatregelen van de BIO zijn niet areaal specifiek (te algemeen opgesteld) en opgezet als een achteraf controle.

Het idee achter dit document is het omdraaien van de situatie:

1. Voorafgaand aan aanbestedingen of offerte uitvragen voor systemen aan leveranciers wordt een lijst met eisen opgesteld waaraan iedere inschrijver moet voldoen. Hiermee ontstaat een "level playing field".
2. Wanneer aan alle eisen invulling wordt gegeven met daarbij de doelstellingen van de BIO in het achterhoofd, dus niet om maar zo min mogelijk invulling te geven aan die eisen, dan zou bij een

	Systeemdocumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

officiële audit van het systeem volgens het BIO normenkader tenminste een voldoende rapportcijfer gescoord moeten kunnen worden. Het is nog wel mogelijk dat er aanwijzingen of verbeterpunten worden gegeven.

3. Het BIO normenkader van de overheid blijft altijd leidend. Bij twijfel over de invulling van de maatregelen wordt verwezen naar de officiële BIO documenten.
4. Dit document maakt ook duidelijk welke documenten en informatie aangeleverd moet worden als het gaat om de procedurele aspecten.

Aan de opdrachtnemer wordt gevraagd een Informatiebeveiligingsplan op te leveren waarmee de eisenlijst wordt ingevuld, beschreven en toetsbaar gemaakt. In dit plan zijn ook een beperkt aantal rollen en taken voor de opdrachtgever opgenomen. Het informatiebeveiligingsplan dat wordt opgesteld door de leverancier moet ten behoeve van eenvoudige verificatie de hoofdstukken, thema's en nummering van de BIO Interpretatie voor VRI volgen. Het doel is om te komen tot een wederzijds vastgesteld plan. Het informatiebeveiligingsplan zal volgens het Plan-Do-Check-Act principe actueel gehouden moeten worden.

	Systeemdokumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

3 Interpretatie van de BIO in de praktijk – De actie lijst

Dit hoofdstuk bevat de actie lijst waarin de acties benoemd zijn voor zowel de opdrachtgever (OG) als de opdrachtnemer (ON).

De BIO Controls zijn:

- (05) Informatiebeveiligingsbeleid
- (06) Organiseren van informatiebeveiliging
- (07) Veilig personeel
- (08) Beheer van bedrijfsmiddelen
- (09) Toegangsbeveiliging
- (10) Cryptografie
- (11) Fysieke beveiliging en beveiliging van de omgeving
- (12) Beveiliging bedrijfsvoering
- (13) Communicatiebeveiliging
- (14) Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- (15) Leveranciersrelaties
- (16) Beheer van informatiebeveiligingsincidenten
- (17) Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- (18) Naleving

De acties zijn:

#	Actie	OG	ON
01	Object en reikwijdte benoemen	X	Object: (intelligente) Verkeer Regel Installaties Reikwijdte: Technische installatie, procedures Informatiebeveiliging.
02	Basis Beveiligingsniveau bepalen	X	Niveau: BBN2
03	Eisenlijst opstellen	X	De eisenlijst is in een apart Excel sheet "BIO maatregelen V&OR VRI v.1.xlsx" vastgelegd en goedgekeurd door de Information Security Officer en de assetmanager.
04	Informatiebeveiligingsplan ON		X
			De ON levert een Informatiebeveiligingsplan op: • De 13 Controls van de BIO worden gevolgd zodat verificatie door OG of een externe neutrale partij eenvoudig mogelijk is. • De inhoud van dit Informatiebeveiligingsplan volgt uit de eisenlijst. • Het plan bevat alle punten die gemarkeerd zijn als "document" of "procedure". • De items gemarkeerd als "eis" dienen zeer nadrukkelijk opgevolgd te worden. • Als het gaat om het benoemen van verantwoordelijke personen en belegde rollen

Systeemdokumentatie

Titel : BIO naar de praktijk – reikwijdte: VRI's

Auteur : Eric Bish & Hans Hoets

Datum : 31 augustus 2021

Versie : 1.3

moet deze aangeleverd worden in een aparte bijlage of document zodat onderhoud van het plan en bescherming van de privacy gemakkelijker geborgd kan worden. In het bijzonder moet de rol van Chief Information Security Officer (CISO) ook in dit document belegd zijn. De beschrijving van de CISO rol geeft aan welk mandaat en verantwoordelijkheid deze functionaris heeft. De CISO treedt op als contactpersoon voor OG ten aanzien van Informatiebeveiliging.

- In het geval van het beschrijven van de werkwijze of omgang met informatiebeveiliging dient de uitwerking zeer precies te zijn en weinig ruimte te bieden voor verschillende interpretaties.
- Procedures dienen beschreven te worden en daadwerkelijk geïmplementeerd in het dagelijkse werk binnen de organisatie. Er wordt gevraagd dit aan te tonen of te verklaren.
- In het beveiligingsplan bevinden zich ook rollen en taken voor de OG. Het sleutelplan is hier een voorbeeld van. In het plan wordt duidelijk aangegeven wanneer het een rol of taak van de OG betreft.

05 Informatiebeveiligingsplan OG X

De OG voert controles uit op:

- De inhoud van het beveiligingsplan.
- De aan te leveren verklaringen en gegevens.
- De gerealiseerde technische oplossing.
- Verstrekte autorisaties.
- De effectiviteit van de beschreven procedures.

De OG verstrekt:

- Contact gegevens van de Servicedesk
- Contact gegevens van de assetmanager.
- Toegang via de Telewerkvoorziening volgens de daarvoor aanwezige procedure.
- De procedures rondom uitgifte en beheer van sleutels.
- Indien van toepassing technische hulpmiddelen.
- Systemen in het Datacenter van de OG voor het ontvangen van logging en status informatie.
- Systemen in het Datacenter van de OG voor het besturen en onderhouden van de asset.
- Een technisch koppelvak in de straatkast voor het aansluiten van de asset op het besturingsnetwerk van de OG.

Systeemdokumentatie

Titel : BIO naar de praktijk – reikwijdte: VRI's

Auteur : Eric Bish & Hans Hoets

Datum : 31 augustus 2021

Versie : 1.3

06	Plan-Do-Check-Act	X	X	Zowel OG als ON toetsen periodiek de oplossing op Informatiebeveiliging aspecten, nieuwe versies van het BIO raamwerk en ontwikkelingen die van invloed zijn op Informatiebeveiliging. Het periodiek uitvoeren van audits en penetration & hacking tests maakt deel uit van de PDCA cyclus en zal worden geïnitieerd door de OG.
07	Onderhoudscontract	X		De opdrachtgever neemt afspraken over end-of-life producten, het installeren van updates, upgrades en andere IT specifieke componenten, op als een apart onderdeel binnen het onderhoudscontract.
08	Goedkeuringen en controles	X		De OG zal periodiek het gebruik van licenties, het leveren van documentatie en het opleveren van configuratie bestanden controleren. De OG behoudt zich het recht voor audits op naleving van de afspraken te laten uitvoeren.

	Systeemdokumentatie Titel : BIO naar de praktijk – reikwijdte: VRI's Auteur : Eric Bish & Hans Hoets Datum : 31 augustus 2021 Versie : 1.3
--	---

Bijlage1 Baseline Informatiebeveiliging Overheid (BIO)

Dit zijn de bronbestanden waarop dit document is gebaseerd:



baseline-informatie bio-versie-104zv_de
beveiliging-overheid



f.pdf

De documenten zijn op Internet te vinden:

https://bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf

<https://bio-overheid.nl/media/1404/baseline-informatiebeveiliging-overheid-104-spreadsheet.xlsx>

Het “forum standaardisatie” van de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties waar naar verwezen wordt is hier te vinden:

<https://www.forumstandaardisatie.nl/>

Dit zijn de lijsten met verplicht en aanbevolen standaarden van het forum:



Forum



Forum

Standaardisatie - AaStandaardisatie - Ve