UNIVERSITEIT VAN AMSTERDAM | Hogeschool van Amsterdam

# Basisset Operationele Maatregelen

## Inhoud

# 1 Inleiding

De 'Basisset Operationele Maatregelen' zijn een set aan securitymaatregelen waaruit de van toepassing zijnde maatregelen kunnen worden geselecteerd naar aanleiding van een BIV-Classificatie uit een IB&P Analyse.

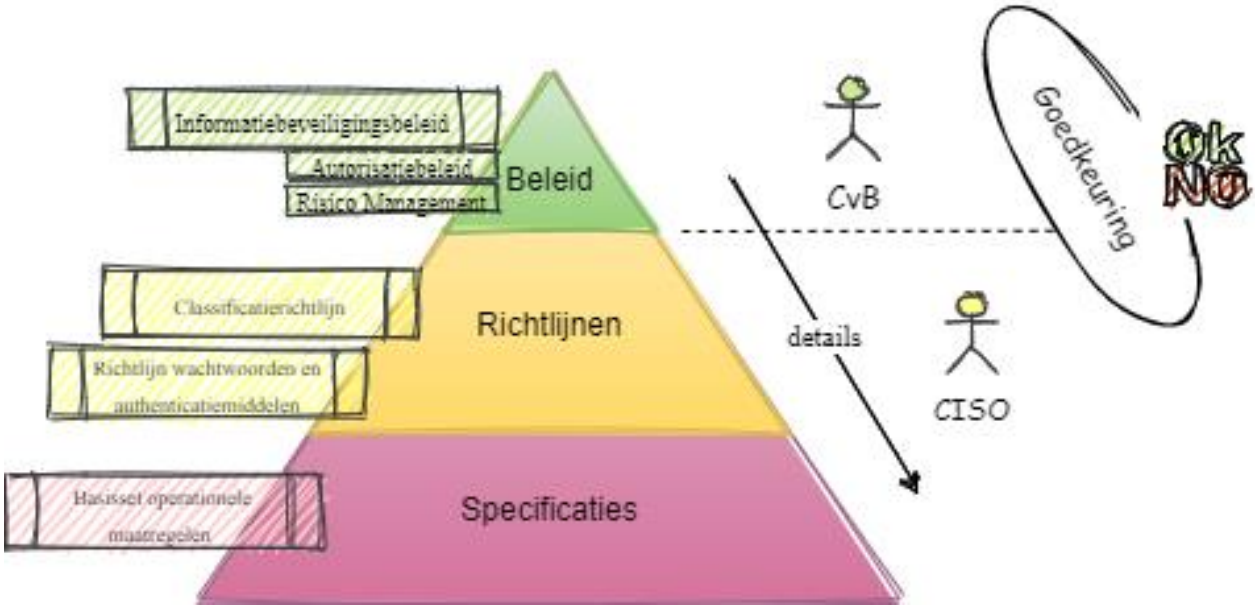
Deze handleiding beschrijft het gebruik van de Basisset Operationele Maatregelen, een lijst met maatregelen die is gebaseerd op de CIS 7.1 en ISO27002 controls.

## 1.1 Doelgroep

De doelgroep is deelnemers aan een IB&P sessie die toepasselijke informatiebeveiligingsmaatregelen willen selecteren om daarbij geïdentificeerde risico's te kunnen mitigeren of minimaliseren. Te denken valt aan systeemeigenaars, (facultair) information security officers, privacy officers, informatiemanagers en securityspecialisten.

## 1.2 Positionering van de maatregelen

De volgende figuur geeft de positionering weer van de Basisset Operationele Maatregelen:




Het informatiebeveiligingsbeleid beschrijft de strategische keuzes van de organisatie m.b.t. informatiebeveiliging. Het beleid wordt verder uitgewerkt in richtlijnen, eventueel per domein, en richtlijnen worden weer uitgewerkt in maatregelen.

De maatregelen zijn de meest uitgewerkte operationele omschrijvingen van informatiebeveiligings-maatregelen. Deze kunnen ook een verwijzing zijn naar een interne of externe technische specificatie.

# 2 Korte handleiding

Deze korte handleiding heeft tot doel de gebruiker van de Basisset Operationele Maatregelen op weg te helpen in het gebruik ervan. In Bijlage A staat een voorbeeld van een stukje van de Basisset Operationele Maatregelen getoond.

## 2.1 Kolom-uitleg

Hieronder zijn alle kolommen toegelicht.

### 2.1.1 Nr

De nummering van maatregelen is statisch en uniek. Dat wil zeggen dat er geen nieuwe maatregel komt met eenzelfde nummer.

### 2.1.2 Titel

Een indicatieve naam voor de maatregel.

### 2.1.3 Omschrijving

Omschrijving van een maatregel die aangeeft wat de maatregel inhoudt.

### 2.1.4 Asset Type

Een maatregel kan van toepassing zijn op één of meerdere Asset types. Het Asset type geeft aan voor welk bedrijfsmiddel de maatregel van toepassing is. Filtering op deze kolom is van waarde, ingeval alleen maatregelen voor een bepaald type asset worden gezocht. Het is aan te bevelen gebruik te maken van filtermethode 1, zie 2.2 Filtering op pagina 6, aangezien er meerdere asset types in één cel kunnen staan. Een aantal asset types worden hier verder uitgelegd:

- Applicatie
  Een computerprogramma dat bedoeld is voor eindgebruikers. Dit in tegenstelling tot een servertaak of andere taken die door een besturingssysteem op de achtergrond worden uitgevoerd.
- Cloud: IaaS, PaaS, SaaS
  Verschillende vormen van Cloud dienstverlening, van het hosten van een eigen virtuele server (IaaS) tot en met het afnemen van de complete dienst (SaaS).
- End user device
  Alle door een eindgebruiker te bedienen ICT-apparatuur, zoals computers, printers, smartphones, projectors en camera's
- Fysieke omgeving
  Een ruimte met betrekking op fysieke aspecten in de omgeving van een persoon
- Gebruiker
  Betreft een maatregel die een directe uitwerking heeft op een gebruiker en/of de gebruikerservaring.

- Informatie
  Gegevens die op zichzelf of in samenhang van waarde zijn voor de organisatie.
- Netwerk
  Het geheel aan communicatie-infrastructuur voor ICT-middelen.
- Proces
  Een geheel van samenhangende of elkaar beïnvloedende activiteiten.
- Removable Media
  Een vorm van computeropslag die is ontworpen om in een systeem te worden ingebracht en daaruit te worden verwijderd.
- Systeem
  De hardware en daaraan gelieerde systeem specifieke software waaronder personal computers, servers en netwerkapparatuur.

### 2.1.5 Security Functie

De Security Functie geeft aan welk onderdeel van de “gelaagde beveiliging” deze maatregel helpt ondersteunen. Er zijn een 5-tal functies van een maatregel, te weten 1) Identify, 2) Protect, 3) Detect, 4) Respond en 5) Recover. De functies geven aan welke bijdrage de maatregel biedt binnen de informatiebeveiliging. Het gebruik van deze kolom dient:

- het snel kunnen filteren op maatregelen met een bepaald doel;
- ter ondersteuning bij het vinden van de invulling van de maatregel.

### 2.1.6 Toepassingsgebied

In de kolom Toepassingsgebied kun je de context waarbinnen je de maatregelen wenst te gebruiken selecteren. Het is aan te bevelen gebruik te maken van de filtermethode 1, zie 2.2 Filtering op pagina 6, aangezien er meerdere toepassingsgebieden in één cel kunnen staan. De toepassingsgebieden zijn:

- IB&P
  Relevant als je op basis van een IB&P wilt weten welke maatregelen getroffen dienen te worden. Door deze filtering toe te passen wordt een groot deel van de generieke zaken achterwegen gelaten.
- Generiek
  Betreft fundamentele maatregelen die in de breedte ingevoerd moeten worden.

### 2.1.7 BIV-element

Het BIV-element geeft aan waar de maatregel een ondersteuning is op het gebied van Beschikbaarheid, Integriteit en/of Vertrouwelijkheid, als ook op welk niveau [Laag, Midden, Hoog]. In het gebruik geven we per element elk niveau aan dat van toepassing is. Door alle van toepassing zijnde niveaus op te nemen:

1. worden de juiste maatregelen getoond bij het gebruik van IB&P Match, zie beschrijving van de gelijknamige kolom;
2. wordt voorkomen dat bij een filtering op een hoger niveau, de onderliggende voorwaardelijke maatregelen uit beeld verdwijnen.

### 2.1.8 IB&P Match

De IB&P Match biedt de mogelijkheid maatregelen te filteren op basis van de BIV-classificatie die voort is gekomen uit de IB&P analyse. Door die uitkomst in te vullen in cel N2, is de onderliggende kolom te filteren op ‘IB&P Match’.

### 2.1.9 Richtlijn referentie

De kolom Richtlijn referentie geeft aan welke control uit een normering of framework deze maatregel uitwerkt.

### 2.1.10 Thematiek

Thematiek is een kolom bedoeld om de mogelijkheid te bieden te filteren op basis van thematiek.

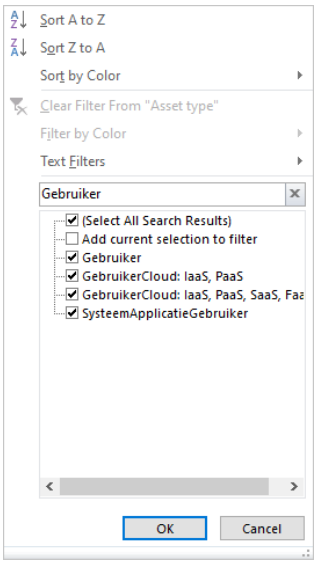
### 2.1.11 Documentatie

Een verdere verwijzing naar documentatie (indien beschikbaar).

## 2.2 Filtering

De insteek van de matrix is om er zo efficiënt mogelijk in te kunnen filteren. Onderstaand enkele tips om de juiste informatie uit de BOM lijst te kunnen halen. Iedere kolom voorziet in de volgende mogelijkheid om te filteren:

1. Op alle door Excel ondersteunde manieren. Om op een bepaald Asset type of bepaalde richtlijn te filteren is het raadzaam gebruik te maken van de filtering zoals hierboven afgebeeld en een tekst in te geven. Eventueel valt de filtering uit te breiden door deze stap te herhalen en te kiezen voor *Huidige selectie aan filter toevoegen*[1]. Zie afbeelding rechts.
2. Op de gewenste BIV-score door de BIV score uit de IB&P in te voeren in het donkerblauwe deel bovenin de sheet. In de illustratie, zie Bijlage A, staat daar nu "LLL" ingevuld. De gegevens in de BIV-element kolommen worden gebruikt voor de matching in de kolom *IB&P Match*.




De kolommen B, I en V onder 'BIV-element', zie Bijlage A, zijn voorzien van alle niveaus waarop de maatregel van toepassing is. De toepasbare niveaus zijn: Laag, Midden en Hoog. Dit resulteert erin dat een maatregel die:

- vanaf het niveau "Vertrouwelijk – Laag" van toepassing is, dat kolom V met LMH ingevuld wordt;
- van toepassing is op "Vertrouwelijk – Laag & Middel", maar niet op Hoog, dat kolom V met LM gevuld wordt;
- vanaf Midden van toepassing is, aangeduid wordt met MH;
- alleen voor Midden van toepassing is, de kolom gevuld wordt met slechts een M.

[1] Add current selection to filter in het Engels

# Bijlage A Voorbeeld Basisset Operationele Maatregelen

Onderstaande voorbeeld is gefilterd op het toepassingsgebied ‘Cloud:*’, waarbij er gematcht wordt op de IB&P classificatie ‘LLL’. In deze illustratie is de kolom ‘IB&P Match’ niet gefilterd zodat het onderscheid tussen wel en niet *matching* maatregelen geïllustreerd wordt.

| *Basisset Operationele Maatregelen voor Informatiebeveiliging v0.9.0* | | | | | | BIV element | | | LLL | <- IB&P BIV classificatie | Gefilterd resultaat: 91 maatregelen | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nr. | Titel | Omschrijving | Asset type | Security Functie | Toepassingsgebied | B | I | V | IB&P Match | Richtlijn referentie | Thematiek | Documentatie |
| 1 | Gebruikers toegangsbeveiliging: Speciale toegangsrechten | Speciale toegangsrechten als admin accounts behoren te worden toegekend aan een gebruikersidentificatie die verschilt van identiteiten die voor reguliere bedrijfsactiviteiten worden gebruikt. Reguliere bedrijfsactiviteiten behoren niet met een speciale gebruikersidentificatie te worden verricht. Het toekennen van deze rechten gaat middels een goedkeuring van de eigenaar, obv een geadministreerde onderbouwing en obv het "least privilege" principe. | Gebruiker<br>Systeem<br>Applicatie<br>Cloud: IaaS, PaaS, SaaS, FaaS | Protect | IB&P<br>Inkoop | LMH | LMH | LMH | IB&P Match | CIS 4.3<br>ISO27002 A.9.2.3<br>ISO27002 A.9.2.4 | Controlled Use of Administrative Privileges<br>Access control | |
| 2 | Aanpassen standaard wachtwoorden | Hardware en software die is voorzien van een standaard gebruiker en/of wachtwoord dienen voorafgaand aan, of tenminste direct bij, aansluiting op enig netwerk te worden voorzien van een aangepast en voor dat asset uniek wachtwoord, dat voldoet aan het geldende wachtwoordbeleid. | Systeem<br>Applicatie<br>Cloud: IaaS, PaaS, SaaS, FaaS | Protect | IB&P | H | LMH | LMH | IB&P Match | CIS 4.2<br>CIS 4.4<br>ISO27002 A.9.4.3 | Controlled Use of Administrative Privileges | Link naar wachtwoordbeleid |
| 3 | Domeinscheiding in wachtwoorden | Er dient onderscheid gemaakt te worden tussen verschillende niveau's binnen het landschap waar het gaat om (admin-)wachtwoorden, waarbij tenminste het niveau van werkplek-, netwerk accesslayer, netwerk core, server- en domeinbeheerder onderscheiden wordt. | Systeem<br>Applicatie<br>Cloud: IaaS | Protect | Generiek | LMH | LMH | LMH | IB&P Match | ISO27002 A.9.1.2<br>CIS 14.1 | Access control<br>Controlled Use of Administrative Privileges<br>Controlled Access Based on the Need to Know | |
| 4 | Twee Factor Authenticatie (2FA) | Gebruikeraccounts die toegang hebben tot vertrouwelijke informatie dienen voorzien te zijn van 2FA. | Gebruiker<br>Systeem<br>Applicatie<br>Informatie<br>Cloud: IaaS, PaaS, SaaS, FaaS | Protect | IB&P | | MH | MH | | CIS 4.5<br>CIS 11.5<br>CIS 16.3<br>ISO27002 A.9.4.2 | Controlled Use of Administrative Privileges<br>Secure Configurations<br>Account Monitoring and Control | |
| 5 | Systemen moeten beveiligd zijn tegen het uitvoeren van niet gesignde scripts en macro's | Behoudens op geïsoleerde ontwikkelmachines moet op alle apparaten zijn afgedwongen dat alleen vertrouwde scripts en executables kunnen worden uitgevoerd en met minimale rechten. | Systeem<br>Applicatie<br>Cloud: IaaS, PaaS, SaaS | Protect | IB&P | LMH | LMH | LMH | IB&P Match | CIS 4.7 | Controlled Use of Administrative Privileges | |
| 6 | Monitoring mutatie van beheerdersaccounts | Het aanmaken van nieuwe admin-accounts, mutaties in groepen waarlangs beheersrechten verkregen kunnen worden en de mutaties van wachtwoorden op niet persoonlijke admin-accounts en domain-admins dienen zonder vertraging te resulteren in een te akkoorderen melding.<br>Waar mogelijk dient de mutatie pas effectief te worden na een technisch akkoord vanuit een daarvoor bestemd account. | Systeem<br>Applicatie<br>Cloud: IaaS, PaaS, SaaS, FaaS | Protect | IB&P<br>Generiek | MH | MH | MH | | CIS 4.8<br>CIS 6.7 | Controlled Use of Administrative Privileges | |
| 7 | Monitoring privilege gebruik admins | Het gebruik van beheerrechten dient gelogd te worden op een manier dat deze niet aan te passen of wissen is. Het gebruik van rechten op ongebruikelijke tijdstippen, vanaf ongebruikelijke IP adressen en niet succesvol gebruik van rechten en het gebuik van local/build-in admin accounts moet zonder vertraging resulteren in een te akkoorderen melding. | Systeem<br>Applicatie<br>Cloud: IaaS, PaaS, SaaS, FaaS | Detect | IB&P<br>Generiek | MH | MH | MH | | ISO27002 A.12.4.3<br>CIS 4.9<br>CIS 6.7 | Controlled Use of Administrative Privileges | |
| 8 | Periodieke hereiking admin-accounts | Tenminste 1 maal per half jaar (L & M) of tenminste een maal per kwartaal (H) dient aan de hand van een automatisch uit de systemen gedestilleerde lijst beoordeeld te worden of er hiaten zitten in de admin-accounts en hun groepslidmaatschappen, het laatste gebruik van local admin-accounts en de datum van de laatste wachtwoord wijziging.<br>Accounts die niet herleidbaar zijn naar een proces(/service) of persoon dienen te worden disabled, niet gewijzigde wachtwoorden na gebruik dient nader onderzocht te worden. | Systeem<br>Applicatie<br>Cloud: IaaS, PaaS, SaaS, FaaS | Detect | IB&P<br>Generiek | | LMH | | IB&P Match | CIS 4.1<br>CIS 16.8<br>ISO27002 A.9.2.5 | Controlled Use of Administrative Privileges<br>Account Monitoring and Control<br>Access control | Link naar autorisatiebeleid |
| 9 | Regulering toegang tot managementinterfaces | Systemen die voorzien zijn van specifieke (netwerk)poorten voor beheer, dienen waar relevant met die poorten op een specifiek voor dat doel ingerichte netwerkbeheerzone aangesloten te worden. De netwerkbeheerzone is alleen toegankelijk via een jumphost. | Systeem<br>Netwerk<br>Cloud: IaaS, PaaS, SaaS, FaaS | Protect | IB&P<br>Generiek | | LMH | | IB&P Match | CIS 14.1<br>ISO27002 A.13.1.3 | Controlled Access Based on the Need to Know | |
| 10 | Local en build-in admin wachtwoord procedure | Het gebruik van build-in/local wachtwoorden moet middels een proces beheerst worden, waarbij | Systeem | Protect | IB&P | | LMH | LMH | IB&P Match | ISO27002 A.9.2.3 | Access Control | |