# Factsheet Configuratiemanagement

**Configuratiemanagement zorgt voor een actueel inzicht in alle hardware en software en onderlinge verbindingen binnen de organisatie en is een belangrijk aspect voor het verhogen van de digitale weerbaarheid van de organisatie (VDW Module 1). Om kwaadwillenden en onbevoegden buiten de deur te houden moet allereerst bekend zijn welke hardware en software zich bevinden binnen het gemeentenetwerk of onder beheer van de gemeente vallen, zoals cloudoplossingen. Het is immers belangrijk dat zicht is op wat beschermd dient te worden. Apparatuur en configuraties zijn niet altijd eenvoudig in kaart te krijgen en te houden. Maar het werpt zeker zijn vruchten af. Dit is waarom:**

Configuratiemanagement is een randvoorwaarde om goed beheer uit te kunnen voeren. Zoals het gericht beheren van de omgeving en het opsporen van onbekende en ongeautoriseerde apparaten binnen het netwerk. Inzicht in hardware en software is de basis voor de ICT-foto die de gemeente aan de IBD levert, waardoor de IBD gericht advies kan leveren over kwetsbaarheden in de gemeentelijke hard- en software. Het biedt ondersteuning aan de andere processen van VDW Module 1; change management, incident management en patchmanagement om zo de basisbeveiliging te verhogen.

### Wat is het risico als configuratiemanagement niet op orde is?

Als het inzicht ontbreekt in de hardware en software in de organisatie kan ‘shadow-IT’ ontstaan, d.w.z. apparatuur en programmatuur die zonder expliciete organisatorische goedkeuring worden gebruikt, waardoor onbekende personen, apparaten of kwetsbaarheden schade kunnen aanrichten binnen het netwerk en de gemeente-organisatie.

## Aan de slag!

### Waar begin ik?

- Zorg dat er een actueel inzicht is in alle configuratie-items (CI) binnen de organisatie of onder beheer van de organisatie.
- Laat contractueel vastleggen, ook waar dat aan leveranciers is uitbesteed, dat de hardware en software geregistreerd dient te worden.
- Dan de hardware en software in eigen beheer; wat is hier al van vastgelegd?
- Alles wat vanaf nu wordt vastgelegd is een stap in de goede richting en zorgt voor meer overzicht in het configuratiemanagement. Na een eerste begin is er altijd nog de mogelijkheid om het configuratiemoment op een later moment verder te professionaliseren.

### Hoe begin ik?

- Maak iemand verantwoordelijk voor het in kaart brengen van de apparatuur en configuraties binnen het beheer. Wijs ook het proces van het configuratiemanagement toe aan een persoon of functierol. Zo wordt het overzicht geen momentopname.
- Breng in kaart wat er al is. Hoe meer er al bekend is, hoe meer tijd het scheelt. Let er hierbij wel op dat eerdere registraties inmiddels verouderd kunnen zijn.
- Aan de slag: bepaal welke gegevens van apparaten en software binnen de organisatie vastgelegd en beheerd dient te worden. Maak het je makkelijk. Leg alleen dat vast wat je nodig denkt te hebben om configuraties te beheren in de Configuratie Management DataBase (CMDB) waarin alle Configuratie Items (CI) zijn vastgelegd en worden bijgehouden. Dit zijn alle relevante soft- en hardware en de onderlinge relaties. Zie hiervoor ook de basisopzet voor een CMDB van de IBD. Maar veel gemeenten gebruiken hiervoor ook ITIL-tooling voor het structureel bijhouden van een CMDB.
- Pak dan door; Bepaal binnen welke scope en welke termijn hardware en software geregistreerd dient te worden. Dit kan ook een langere periode van een paar maanden zijn. Zolang er maar een duidelijke einddatum is vastgesteld. Dan moet het overzicht compleet zijn.
- Zorg voor een volledig en relevant overzicht in de CMDB. Dat kan door een scan op het netwerk uit te voeren, maar ook door per afdeling in kaart te brengen welke CI’s er in gebruik zijn.
- Zorg er daarbij voor dat elk CI binnen het netwerk uniek geïdentificeerd kan worden.
- Ook is het belangrijk dat elk configuratie-item (CI) is toegewezen aan een unieke eigenaar.

### Hoe pak ik het structureel op?

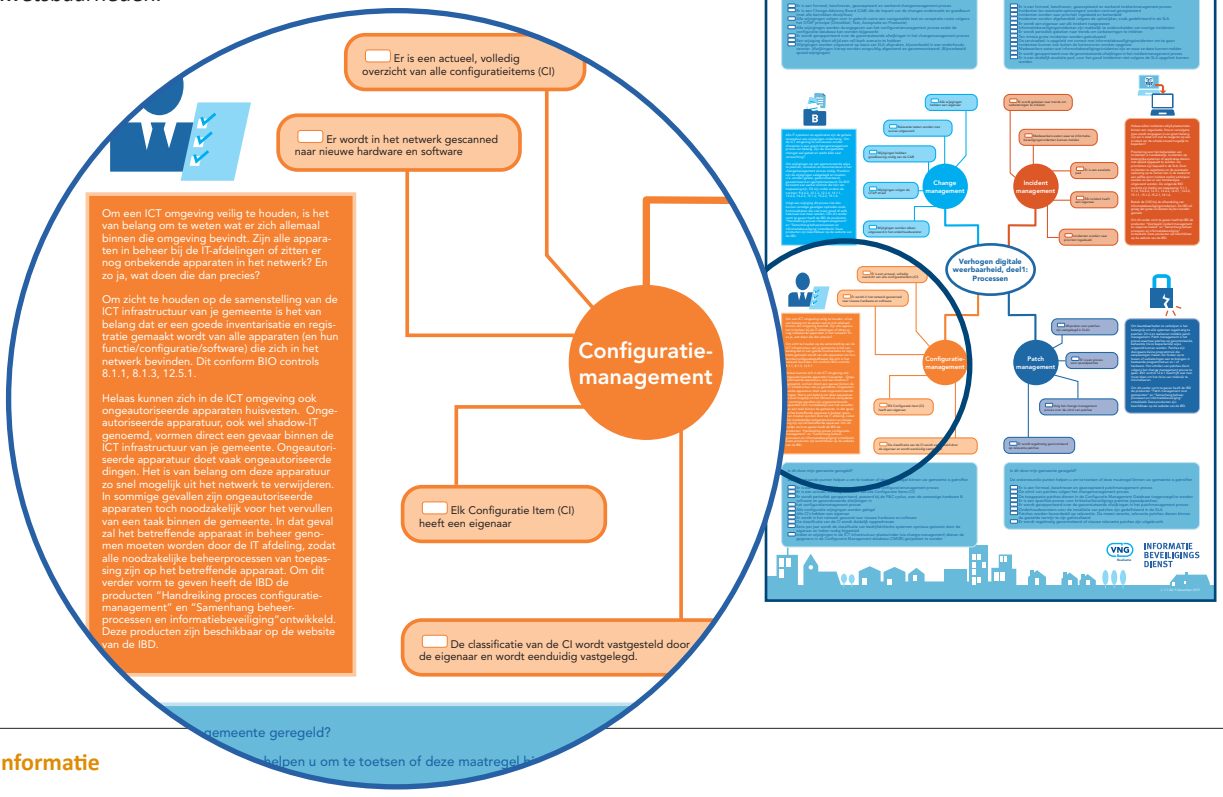
- Zorg ervoor dat configuratiemanagement is vastgelegd in duidelijke afspraken en procedures. Dit hoeft niet veel tekst te zijn. Als in ieder geval duidelijk is bepaald wie waarvoor verantwoordelijk is.
- Leg ook afspraken en procedures vast voor het toevoegen of uitfaseren van hardware of software uit de organisatie. Zo blijft het configuratiemanagement ook bij wijzigingen actueel.
- Check minimaal jaarlijks of het gemaakte overzicht nog klopt. Dit kan ook door steeds een onderdeel van het geheel na te lopen. Bijvoorbeeld iedere 2 maanden voor 1/5$^{e}$ van het geheel of na een wijziging in de infrastructuur. Dan zijn de werkzaamheden te overzien en wordt toch jaarlijks alles gecontroleerd.

## De basis op orde en klaar voor de volgende stap?

- Voer jaarlijks een technische scan uit van het netwerk om na te gaan of het configuratiemanagement volledig is en geen potentieel kwetsbare apparaten of software over het hoofd worden gezien.
- Gebruik van een zogenaamde *'applicatie whitelist'* zorgt ervoor dat alleen die applicaties gebruikt kunnen worden die op de lijst staan. Dit is veel veiliger dan het blokkeren van bepaalde applicaties. Maar let op! Dit levert ook een hoop extra beheerwerkzaamheden op.

## Tips uit de praktijk

- Weinig tijd? Begin dan met 'kroonjuwelen', ofwel de belangrijkste hardware en software. Dit zijn de applicaties en processen die essentieel zijn om te kunnen blijven werken en waar informatie zeker niet zomaar gewijzigd moet kunnen worden of uitlekken.
- Zorg ervoor dat ieder configuratie item (CI) een eigenaar heeft. Zo is het makkelijk te achterhalen bij wie je moet zijn als bepaalde software kwetsbaar is of een controle nodig is.
- Eenduidige registratie is essentieel. Maak dus duidelijke afspraken en een naamgevingsbeleid voor hoe een apparaat wordt benoemd en welke gegevens op welke manier worden vastgelegd.
- Enkele vuistregels voor waarom bepaalde hardware of software moet worden vastgelegd;
  - *Hoogte van de aanschafprijs is substantieel.*
  - *Hoogte van de onderhoudskosten is substantieel.*
  - *Noodzaak tot registratie in relatie met de gebruiker.*
  - *Er is sprake van een logische eenheid voor beheer / mogelijke kwetsbaarheden.*




## Waar vind ik meer?

**Verhogen Digitale Weerbaarheid Module 1**
https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/

**Handreiking configuratiemanagement BIO**
https://www.informatiebeveiligingsdienst.nl/product/handreiking-proces-configuratiebeheer-v1-0/

**Handreiking afvoer ICT-middelen**
https://www.informatiebeveiligingsdienst.nl/product/afvoer-ict-middelen/

**ITIL**
https://nl.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

Kijk voor meer ook op de productenpagina van de IBD;
https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

## Hulp nodig?

Neem contact op met de IBD. Wij denken mee!
Deel vooral ook je successen! Ook andere gemeenten kunnen leren van wat werkt.

### Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatiebeveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).