

Informatieclassificatie Vlaamse overheid (Vo-ICR)

# Release en deployment beheer

Minimale maatregelen

**Team Informatieveiligheid | Digitaal Vlaanderen**



Dit is een document voor publiek gebruik

AGENTSCHAP  
DIGITAAL VLAANDEREN  
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

---

## INHOUD VAN DIT DOCUMENT

### Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

### Doel van het document

Dit document beschrijft de kwaliteitseisen waaraan minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen release en deployment beheer. Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vlaamse overheid.

### Werkprincipe van het document

Het huidige document bestaat uit 4 delen. Eerst worden de minimale maatregelen besproken, alvorens in het 2<sup>de</sup> deel al de nodige aanvullende informatie ter beschikking wordt gesteld, vervolgens bespreken we de link met andere maatregelen. Het document wordt afgerond met de prestatie indicatoren.

De organisatie van de maatregelen in het kader van informatieclassificatie wordt beschreven in het document [‘Vo informatieclassificatie – Organisatie - Informatieclassificatieraamwerk’](#).

### Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vlaamse overheid en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

### Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft

### Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

[security@vlaanderen.be](mailto:security@vlaanderen.be)

## Classificatie



Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.



Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

## Historiek

	Datum	Auteur	Opmerkingen
<b>v.0.1</b>	13 november 2019	Kristel VAN AKEN	Draft
<b>v.0.2</b>	19 november 2019	Kristel VAN AKEN	Feedback pre-taakgroep
<b>v.0.3</b>	02 december 2019	Kristel VAN AKEN	Feedback taakgroep
<b>v.0.4</b>	16 december 2019	Kristel VAN AKEN	Consistentie check
<b>v.1.0</b>	16 december 2019	Kristel VAN AKEN	Versie gepubliceerd in pdf
<b>v.1.1</b>	20 maart 2020	Kristel VAN AKEN	Links toegevoegd
<b>v.1.2</b>	03 februari 2021	Kristel VAN AKEN	Integriteit toegevoegd
<b>v.1.3</b>	30 september 2021	Kristel VAN AKEN	Beschikbaarheid toegevoegd
<b>v.2.0</b>	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
<b>V.2.1</b>	17 oktober 2023	Nele Lowet	Update KSZ

## Bronnen en verwijzingen

De inhoud van dit document werd samengesteld op basis van volgende documenten:

### Documentverwijzingen:

- > [Vo Informatieclassificatie – Organisatie Informatieveiligheid \(PDF\)](#)
- > [Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk \(PDF\)](#)
- > Vo Informatieclassificatie – Minimale maatregelen – (PDF):
  - > [Vo Informatieclassificatie - Minimale maatregelen - asset en configuratiebeheer](#)
  - > [Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer](#)
- > [Vo Informatieclassificatie – Overzicht baseline maatregelen \(XLS\)](#)

De laatste versies van deze documenten zijn te raadplegen op [vlaanderen.be](https://vlaanderen.be).

## Inhoudsopgave

<b>Inhoud van dit document .....</b>	<b>2</b>
Situering van het document .....	2
Doel van het document .....	2
Werkprincipe van het document .....	2
Verspreiding van het document .....	2
Vrijwaring.....	2
Eigenaar .....	2
Classificatie .....	3
Historiek.....	3
Bronnen en verwijzingen .....	3
Documentverwijzingen: .....	3
<b>Inleiding .....</b>	<b>5</b>
Het proces release en deployment beheer .....	5
<b>1. Minimale maatregelen .....</b>	<b>6</b>
1.1 Minimale algemene maatregelen .....	6
1.2 Minimale specifieke (GDPR) maatregelen.....	9
1.3 Minimale specifieke (NISII) maatregelen .....	11
1.4 Minimale specifieke (KSZ) maatregelen .....	11
<b>2. Aanvullende informatie over de maatregel .....</b>	<b>12</b>
2.1 Wat is release en deployment beheer? .....	12
2.2 Succesfactoren voor een goed release en deployment beheer.....	12
2.3 De bouwstenen van release en deployment beheer .....	12
2.3.1 Planning.....	12
2.3.2 Bouw, test en acceptatie.....	14
2.3.3 Uitrol .....	15
2.3.4 Verificatie en afsluiten .....	16
2.3.5 Het proces .....	17
<b>3. Link met andere beheersprocessen .....</b>	<b>18</b>
3.1 Link met wijzigingsbeheer .....	18
3.2 Hoe zijn de processen wijzigingsbeheer, asset en configuratie beheer en release en deployment beheer onderling gerelateerd?.....	19
<b>4. Prestatie-indicatoren (KPI's) .....</b>	<b>20</b>

---

## INLEIDING

### Het proces release en deployment beheer

Release en deployment beheer bestaat uit twee deelprocessen:

- › Het release proces is het proces dat verantwoordelijk is voor planning en controle van de samenstelling van releases, het testen en verdelen van releases en voor het leveren van de nieuwe functionaliteit in de ICT-dienstverlening waarbij de integriteit van de bestaande functionaliteit wordt beschermd.
- › De uitrol of deployment zorgt voor de ter beschikking stellen van een release in productie zodat de nieuwe functionaliteit effectief kan worden toegepast of gebruikt. Dit gaat gepaard met een overdracht van de release naar de beheersorganisatie.

De doelstellingen van release en deployment beheer voor informatiebeveiliging omvatten:

- › Een gecontroleerde opzet, testen, uitrol van release pakketten met minimale impact op de bestaande omgeving;
- › Verzekeren dat nieuwe of gewijzigde ICT-dienstverlening de beloofde functionaliteit levert;
- › Opvolging en beheer van afwijkingen, risico's en andere gegevens gerelateerd aan de beloofde nieuwe of gewijzigde functionaliteit en correctieve actie ondernemen waar nodig;
- › Kennisoverdracht naar gebruikers, de beheersorganisatie en andere belanghebbenden.

# 1. MINIMALE MAATREGELEN



## 1.1 Minimale algemene maatregelen




Het opmaken van release pakketten en de uitrol ervan omvat een aantal activiteiten die, afhankelijk van de klasse waartoe de betrokken informatie behoort, al dan niet verplicht uitgevoerd moeten worden. Deze activiteiten zijn (zie hoofdstuk: [‘De bouwstenen van release en deployment beheer’](#)):

- > Planning van de release;
- > Bouw release pakket;
- > Opstellen documentatie;
- > Test en acceptatie van het release pakket;
- > Ontwikkel-, test- en acceptatie omgeving en test data voorzien;
- > Goedkeuring via het proces wijzigingsbeheer;
- > Uitrol van het release pakket;
- > Overhandiging aan de beheersorganisatie;
- > Postverificatie;
- > *Lessons learned.*

De minimale beschikbaarheid van het proces zelf is eveneens afhankelijk van het type en klasse van de getroffen informatie. We onderscheiden beschikbaarheid tijdens kantooruren (10ux5dagen) en permanente beschikbaarheid (24ux7dagen).




### Vertrouwelijkheid

IC klasse	Minimale maatregelen
 	<p><b>Klasse 1</b> en <b>Klasse 2</b> kennen dezelfde maatregelen:</p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: <ul style="list-style-type: none"> <li>&gt; Voor een major release is een <i>big bang</i>, gefaseerde aanpak of gelimiteerde <i>pull</i> toegestaan;</li> <li>&gt; Voor een minor release of sprint is een <i>big bang</i>, gefaseerde aanpak of <i>pull</i> toegestaan.</li> </ul> </li> <li>&gt; Bouw release pakket;</li> <li>&gt; Opstellen documentatie: over de bouw, installatie, test plannen, procedures, scripts en <i>fall back</i> plan;</li> <li>&gt; Test en acceptatie van het releasepakket vooraleer het uitgerold wordt in productie;</li> <li>&gt; Ontwikkel-, test- en acceptatieomgeving moeten gescheiden zijn van productie omgeving;</li> <li>&gt; Goedkeuring minstens door de toepassingseigenaar (voor meer informatie zie document: <a href="#">‘Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer’</a>);</li> <li>&gt; Uitrol van het release pakket;</li> <li>&gt; Overhandiging aan de beheersorganisatie;</li> <li>&gt; Postverificatie.</li> </ul>



	<p>Alle maatregelen van <b>Klasse 1 / Klasse 2 +</b></p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: <i>big bang</i>, gefaseerde aanpak of gelimiteerde <i>pull</i> toegestaan;</li> <li>&gt; Test en acceptatie van het releasepakket via vooraf bepaald testplan met validatie van de testresultaten voorafgaand aan elke volgende stap in de bouw;</li> <li>&gt; Goedkeuring door de CAB ((Voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>');</li> <li>&gt; Overhandiging aan de beheersorganisatie met formele notificatie aan alle belanghebbenden;</li> <li>&gt; <i>Lessons learned</i>.</li> </ul>
	<p>Alle maatregelen van <b>Klasse 1 + Klasse 2 + Klasse 3 +</b></p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: <i>big bang</i> of gefaseerde aanpak;</li> <li>&gt; Ontwikkel-, test- en acceptatieomgeving moeten voldoen aan dezelfde kwaliteitseisen als de productie omgeving.</li> </ul>
	<p>Alle maatregelen van <b>Klasse 1 + Klasse 2 + Klasse 3 + Klasse 4 +</b></p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: enkel gefaseerde aanpak toegestaan;</li> <li>&gt; Test en acceptatie van het release pakket via vooraf bepaald testplan met 4EYES validatie van de testresultaten voorafgaand aan elke volgende stap in de bouw;</li> <li>&gt; Productiedata mogen niet gebruikt worden als test data;</li> <li>&gt; Goedkeuring door de CAB (inclusief DPO) met scheiding van functies en 4EYES validatie (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>');</li> <li>&gt; Overhandiging aan de beheersorganisatie met formele notificatie aan alle belanghebbenden, inclusief DPO.</li> </ul>

## Integriteit

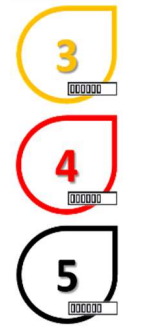
IC klasse	Minimale maatregelen
 	<p><b>Klasse 1 en Klasse 2</b> kennen dezelfde maatregelen:</p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: <ul style="list-style-type: none"> <li>&gt; Voor een major release is een <i>big bang</i>, gefaseerde aanpak of gelimiteerde <i>pull</i> toegestaan;</li> <li>&gt; Voor een minor release of sprint is een <i>big bang</i>, gefaseerde aanpak of <i>pull</i> toegestaan.</li> </ul> </li> <li>&gt; Bouw release pakket;</li> <li>&gt; Opstellen documentatie: over de bouw, installatie, test plannen, procedures, scripts en <i>fall back</i> plan;</li> <li>&gt; Test en acceptatie van het releasepakket vooraleer het uitgerold wordt in productie;</li> <li>&gt; Ontwikkel-, test- en acceptatieomgeving moete gescheiden zijn van productie omgeving;</li> <li>&gt; Goedkeuring minstens door de toepassingseigenaar (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>');</li> </ul>

	<ul style="list-style-type: none"> <li>&gt; Uitrol van het release pakket;</li> <li>&gt; Overhandiging aan de beheersorganisatie.</li> </ul>
	<p>Alle maatregelen van <b>Klasse 1 / Klasse 2 +</b></p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: <i>big bang</i>, gefaseerde aanpak of gelimiteerde <i>pull</i> toegestaan;</li> <li>&gt; Test en acceptatie van het releasepakket via vooraf bepaald testplan met validatie van de testresultaten voorafgaand aan elke volgende stap in de bouw;</li> <li>&gt; Goedkeuring door de CAB (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>');</li> <li>&gt; Overhandiging aan de beheersorganisatie met formele notificatie aan alle belanghebbenden;</li> <li>&gt; <i>Lessons learned</i>.</li> </ul>
	<p>Alle maatregelen van <b>Klasse 1 + Klasse 2 + Klasse 3 +</b></p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: <i>big bang</i> of gefaseerde aanpak;</li> <li>&gt; Ontwikkel-, test- en acceptatieomgeving moeten voldoen aan dezelfde kwaliteitseisen als de productie omgeving.</li> </ul>
	<p>Alle maatregelen van <b>Klasse 1 + Klasse 2 + Klasse 3 + Klasse 4 +</b></p> <ul style="list-style-type: none"> <li>&gt; Planning van de release: enkel gefaseerde aanpak toegestaan;</li> <li>&gt; Test en acceptatie van het releasepakket via vooraf bepaald testplan met 4EYES validatie van de testresultaten voorafgaand aan elke volgende stap in de bouw;</li> <li>&gt; Productiedata mogen niet gebruikt worden als test data;</li> <li>&gt; Goedkeuring door de CAB (inclusief DPO) met scheiding van functies en 4EYES validatie (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>');</li> <li>&gt; Overhandiging aan de beheersorganisatie met formele notificatie aan alle belanghebbenden, inclusief DPO.</li> </ul>

## Beschikbaarheid

IC klasse	Minimale maatregelen
 	<p><b>Klasse 1</b> en <b>Klasse 2</b> kennen dezelfde maatregelen:</p> <ul style="list-style-type: none"> <li>&gt; Beschikbaarheid van het proces release en deployment beheer is minimaal kantooruren (5d x 10u)</li> </ul>

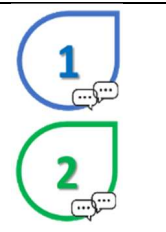





	<p>Klasse 3 en Klasse 4 en Klasse 5 kennen dezelfde maatregelen:</p> <p>Alle maatregelen van Klasse 1 / Klasse 2 +</p> <ul style="list-style-type: none"> <li>› 24x7 beschikbaarheid van het proces release en deployment beheer</li> </ul>
---	---






## 1.2 Minimale specifieke (GDPR) maatregelen

De minimale algemene maatregelen moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing (zie hoofdstuk '[minimale algemene maatregelen](#)').

### Vertrouwelijkheid

IC klasse	Minimale maatregelen
	<p>Er zijn geen GDPR specifieke maatregelen voor Klasse 1 en Klasse 2.</p>
	<p>Maatregelen voor Klasse 3:</p> <ul style="list-style-type: none"> <li>› Planning van de release: <i>big bang</i> of gefaseerde aanpak;</li> <li>› Geanonimiseerde testdata (persoonsgegevens) ofwel moeten ontwikkel-, test- en acceptatieomgeving voldoen aan dezelfde kwaliteitseisen als de productie omgeving;</li> <li>› Goedkeuring door de CAB inclusief DPO (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>');</li> <li>› Overhandiging aan de beheersorganisatie met formele notificatie aan alle belanghebbenden, inclusief DPO.</li> </ul>
	<p>Klasse 4 en Klasse 5 kennen dezelfde maatregelen:</p> <p>Alle maatregelen van Klasse 1 / Klasse 2 / Klasse 3 +</p> <ul style="list-style-type: none"> <li>› Test en acceptatie van het releasepakket via vooraf bepaald testplan met 4EYES validatie van de testresultaten voorafgaand aan elke volgende stap in de bouw;</li> <li>› Goedkeuring door de CAB inclusief DPO met scheiding van functies en 4EYES validatie (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>')</li> </ul>
	<p>Er zijn geen GDPR maatregelen voor Klasse 5.</p>

## Integriteit

IC klasse	Minimale maatregelen
 	Er zijn geen GDPR specifieke maatregelen voor <b>klasse 1</b> en <b>Klasse 2</b> .
	<p>Maatregelen voor <b>Klasse 3</b>:</p> <ul style="list-style-type: none"> <li>› Planning van de release: <i>big bang</i> of gefaseerde aanpak;</li> <li>› Geanonimiseerde testdata (persoonsgegevens) ofwel moeten ontwikkel, test- en acceptatie omgeving voldoen aan dezelfde kwaliteitseisen als de productieomgeving;</li> <li>› Goedkeuring door de CAB inclusief DPO (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>');</li> <li>› Overhandiging aan de beheersorganisatie met formele notificatie aan alle belanghebbenden, inclusief DPO.</li> </ul>
	<p>Maatregelen voor <b>Klasse 4</b>:</p> <p>Alle maatregelen van <b>Klasse 1</b> / <b>Klasse 2</b> / <b>Klasse 3</b> +</p> <ul style="list-style-type: none"> <li>› Test en acceptatie van het releasepakket via vooraf bepaald testplan met 4EYES validatie van de testresultaten voorafgaand aan elke volgende stap in de bouw;</li> <li>› Goedkeuring door de CAB inclusief DPO met scheiding van functies en 4EYES validatie (voor meer informatie zie document: '<a href="#">Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer</a>')</li> </ul>
	Er zijn geen GDPR maatregelen voor klasse 5.

## Beschikbaarheid

Er zijn geen GDPR specifieke maatregelen gedefinieerd in het kader van beschikbaarheid.

### 1.3 Minimale specifieke (NISII) maatregelen

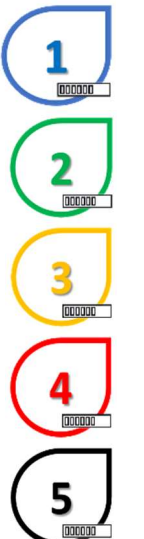
In afwachting van de goedkeuringen omtrent NISII is er in dit document alvast de nodige ruimte voorzien voor toekomstige minimale specifieke NISII maatregelen.

### 1.4 Minimale specifieke (KSZ) maatregelen

De Minimale Normen van de Kruispuntbank Sociale Zekerheid zijn van kracht op de verwerking van sociale gegevens van persoonlijke aard. De minimale normen informatieveiligheid en privacy moeten echter ook worden toegepast wanneer instellingen gemachtigd zijn om onder bepaalde voorwaarden toegang te hebben tot het Rijksregister en om het identificatienummer van het Rijksregister te gebruiken.

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van Release en Deployment beheer toegepast worden:

#### Beschikbaarheid, Integriteit & Vertrouwelijkheid

IC klasse	Minimale maatregelen
	<p>Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen:</p> <ul style="list-style-type: none"> <li>› Elke organisatie moet zich ervan verzekeren dat er geen testen of ontwikkelingen plaatsvinden in de productieomgeving. In bepaalde uitzonderlijke gevallen kan voor testdoeleinden afgeweken worden van deze regel op voorwaarde dat gepaste maatregelen getroffen worden (Ref. KSZ 5.9.1).</li> <li>› Elke organisatie moet: <ul style="list-style-type: none"> <li>▪ over procedures beschikken voor het in productie stellen van nieuwe toepassingen en het aanpassen van bestaande toepassingen</li> <li>▪ voorkomen dat een enkele persoon alleen de controle zou verwerven over dit proces (Ref. KSZ. 5.9.2).</li> </ul> </li> </ul>

---

## 2. AANVULLENDE INFORMATIE OVER DE MAATREGEL

### 2.1 Wat is release en deployment beheer?

Release en deployment beheer is een preventieve maatregel en omvat de procedures, systemen en functies nodig om release pakketten samen te stellen, te bouwen, testen en uit te rollen in een productie omgeving.

Release en deployment beheer omvat volgende activiteiten (zie hoofdstuk: [‘De bouwstenen van release en deployment beheer’](#)):

- › Planning fase,
- › Bouw, test en acceptatie fase,
- › Uitrol,
- › Verificatie en afsluiten.

### 2.2 Succesfactoren voor een goed release en deployment beheer

Een organisatie moet de kritische succesfactoren definiëren die passend zijn voor haar omgeving en elke kritische succesfactor moet opgevolgd worden door één of meerdere kritische prestatie-indicatoren (zie hoofdstuk: [‘Prestatie-indicatoren \(KPI’s\)’](#)). Succesfactoren voor release en deployment beheer omvatten:

- › Optimalisatie van de kost en minimalisatie van het risico dat elke wijziging van een bestaande omgeving met zich meebrengt,
- › Een consistente implementatie aanpak,
- › Goede samenwerking met andere beheersprocessen zoals wijzigingsbeheer, incidentbeheer, probleembeheer en asset- en configuratiebeheer
- › Traceerbaarheid en auditeerbaarheid van de implementatie.

### 2.3 De bouwstenen van release en deployment beheer

#### 2.3.1 Planning

Een goed doordacht en onderbouwd releaseplan is een belangrijk onderdeel van elke succesvolle release, waarbij de nodige aandacht moet worden geschonken aan wat in de release is inbegrepen en hoe deze wordt uitgerold in productie.

Een releaseplan omvat volgende elementen:

- › Welke wijzigingen in de release zijn opgenomen,
- › Wie geïmpacteerd wordt door de release,
- › Welke risico’s verbonden zijn aan de release,
- › De doelgroep van de release,
- › Een duidelijke lijn van goedkeuringen die weergeven welke belanghebbenden welke wijzigingsvraag moeten goedkeuren in elke stap van de release,
- › Aanduiding van het team verantwoordelijk voor de release en de uitrol,
- › Planning van de uitrol en uitrol strategie.

Vaak worden ook bouw- en testplannen in deze fase opgesteld waarbij aandacht wordt geschonken aan functionele en niet-functionele behoeften, designspecificaties, testprocedures, planning voor

bouw en test, acceptatiecriteria in elke stap van de bouw en test en eventuele planning van een piloot opstelling.

De planning moet tevens rekening houden met de wijze waarop de uitrol in productie zal worden uitgevoerd. Hier zijn verschillende opties mogelijk:

- › **Big bang optie:** de nieuwe of gewijzigde functionaliteit wordt uitgerold naar alle betrokken gebruikers tegelijk in één enkele operatie;
- › **Gefaseerde aanpak:** de nieuwe of gewijzigde functionaliteit wordt eerst uitgerold naar een beperkte groep gebruikers, vervolgens wordt de operatie herhaald volgens planning naar andere groepen van gebruikers, net zo vaak als nodig is om de doelgroep volledig te bereiken.
- › **Pull optie:** met deze optie wordt de release ter beschikking gesteld aan de gebruikers maar zij bepalen zelf of en wanneer ze de release op hun apparatuur installeren.

Indien geopteerd wordt voor een *pull* optie, wordt vaak aangeraden om deze optie slechts een beperkte tijd beschikbaar te houden, gevolgd door een geforceerde of *push* uitrol (volgens *big bang* of gefaseerde aanpak) aangezien er altijd wel gebruikers zullen zijn die geen gebruik maken van de *pull* optie. Deze optie noemen we de **gelimiteerde pull**.

De keuze van de uitroloptie heeft zowel gevolgen voor de benodigde middelen voor release en deployment als op de zakelijke omgeving. Om de juiste keuze te maken is een goede kennis van de zakelijke omgeving en de profielen in de doelgroep noodzakelijk.

### Automatische of manuele releases

De mechanismen voor een geslaagde release en uitrol moeten geïdentificeerd worden tijdens de planning en getest tijdens bouw en test fase. Automatisatie kan helpen om herhaalbaarheid en consistentie te garanderen, maar de tijd nodig om een geautomatiseerde uitrol te faciliteren is niet altijd voorhanden. Indien een manuele uitrol de enige optie is, is het belangrijk om alle stappen te monitoren en de impact van vele herhaalde manuele activiteiten te meten aangezien deze waarschijnlijk niet repetitief en/of inefficiënt zijn. Teveel manuele acties kunnen het proces vertragen en kostbare middelen opgebruiken met gevolgen voor het beloofde serviceniveau.

Er zijn vele tools op de markt die kunnen helpen bij (een beperkte) automatisatie:

- › Inventarisatie en ontdekkingstools,
- › Software voor ontdekking en verificaties van bestaande implementaties kunnen helpen om de vooraf bepaalde vereisten voor installatie na te gaan,
- › Automatisatie van het bouwproces,
- › Automatisatie van het onderhoud van gegevens in de CMDB na een release,
- › Installatie procedures.

### 2.3.2 Bouw, test en acceptatie

Zodra een release plan is opgesteld en goedgekeurd, moeten de nodige componenten (hardware, software, documentatie en alle andere) gebouwd, samengesteld en getest worden. Na succesvolle testen volgt dan nog een formele acceptatie door alle belanghebbenden (eindgebruikers, beheersorganisatie, DPO, ...).

Het is raadzaam reeds bij aanvang van deze fase de nodige documentatie aan te leggen om de accuraatheid en efficiëntie van de bouw te verzekeren. Alle activiteiten van het bouwproces moeten gedocumenteerd worden zodat – indien nodig – opnieuw kan aangevat worden. Vaak wordt hierbij gebruik gemaakt van strikte procedures en sjablonen.

Elke stap in het bouwproces vereist eigen test procedures en -plannen en acceptatiemomenten.

Bouw, test en acceptatie omvatten volgende activiteiten:

- › Ontwikkelen van bouwplannen vertrekkende vanuit ontwerp, ontwerp specificaties, functionele en niet-functionele behoeften en andere omgevingsfactoren die een rol spelen bij de ontwikkeling van de release;
- › Vaststellen van de logistiek nodig om de omgeving voor te bereiden;
- › Inplannen van bouw, test en acceptatie activiteiten;
- › Toewijzen van middelen, identificatie van rollen en verantwoordelijkheden nodig om de activiteiten uit te voeren;
- › Bouw-, test- en acceptatie omgevingen voorbereiden;
- › Testgegevens en test databases voorbereiden;
- › Beheer van de nodige licenties.

#### Piloot opstellingen

Piloot opstellingen zijn nuttig om een nieuwe of gewijzigde functionaliteit uit te testen op een beperkte doelgroep vooraleer wordt besloten tot in productie name van de nieuwe of gewijzigde functionaliteit. Hierbij moet de nodige aandacht geschonken worden aan de scope van de piloot opstelling: welke functionaliteit is opgenomen, welke doelgroep wordt erbij betrokken, welke departementen worden aangesproken, enz.

De piloot opstelling moet daarnaast voorzien in de nodige verzameling van testresultaten en feedback, waaronder:

- › Opmerkingen en tevredenheidsscores van eindgebruikers en andere belanghebbenden,
- › Feedback van de beheersorganisatie,
- › Statistische informatie over het gebruik, de resultaten en efficiëntie van de piloot opstelling.

#### Bouw, test en acceptatie van de release

Tijdens bouw, test en acceptatie van de release moet de nodige aandacht geschonken worden aan volgende aspecten:

- › *Security by design* en *by default*,
- › Gebruik van de bouw-, test- en acceptatie omgeving,
- › Documentatie van het bouwproces zodat de bouw kan worden overgedaan indien nodig,
- › Test resultaten documenteren,
- › Acceptatiecriteria en acceptatie momenten vastleggen,
- › Nagaan dat voldaan is aan alle functionele en informatieveiligheidsvereisten,

- › Verificatie van de activiteiten en nagaan of alle vooronderstellingen die gemaakt werden voorafgaand aan de bouw werden ingevuld.

### Logistiek en levering van componenten

Tijdens de bouwfase moet rekening worden gehouden met de logistiek en levering van de nodige componenten (hardware, software, licenties, enz.). Dit houdt onder andere volgende in:

- › Hoe en wanneer de nodige componenten worden geleverd;
- › Welke doorlooptijden worden voorzien en wat de impact is van eventuele vertragingen;
- › Opvolging van de verschillende leveringen.

### Release pakketten

Release pakketten moeten op een gestandaardiseerde en gecontroleerde wijze opgebouwd worden volgens de specificaties van het ontwerp. Vaak is dit een iteratief proces: naarmate de in productie name vordert, kan het zijn dat de bouw van een release pakket herstart moet worden.

Tijdens de bouw van een release pakket houdt men best rekening met volgende factoren:

- › Een gecontroleerde samenstelling en integratie van de componenten in het release pakket;
- › Opmaak van release documentatie (bouw, installatie, test en acceptatie plannen, procedures en scripts);
- › Opvolgen en verifiëren van de kwaliteit van de bouw;
- › De geautomatiseerde en/of manuele procedures nodig om het pakket te verdelen, uit te rollen en te installeren en – waar nodig – bestaande componenten te verwijderen;
- › *Fall back* procedures ingeval van problemen of falen van de uitrol;
- › Opvolging van de benodigde licenties;
- › Installatie en verificatie van het release pakket;
- › Notificatie en communicatie naar de betrokken partijen (gebruikers, beheerorganisatie en andere belanghebbenden).

### 2.3.3 Uitrol

Zodra de diverse testen op het release pakket succesvol zijn afgerond, kan het uitgerold worden in de productie omgeving. Maar eerst moeten de wijzigingen voorgesteld in het release pakket goedgekeurd worden door het proces wijzigingsbeheer. Vanaf dit punt worden bijkomende wijzigingen aan de release beheerd door het proces wijzigingsbeheer, bv. oplossen van fouten of bugs (voor meer informatie zie document: '[Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer](#)')

De uitrol naar de productie omgeving moet met de nodige omzichtigheid benaderd worden:

- › Is de doelomgeving klaar voor uitrol?
- › Zijn potentiële risico's van de uitrol in kaart gebracht en gemitigeerd?
- › Is er rekening gehouden met eventuele onderbrekingen in de operationele werking en de gevolgen ervan?
- › Is de volgorde waarin de componenten uitgerold worden goed gedefinieerd?

Zodra de uitrol is beëindigd, moet nagegaan worden of de nieuwe of gewijzigde ICT-dienstverlening correct werkt voor alle belanghebbenden – interventies of zelfs een *fall back* moeten worden voorzien indien dit niet zo is.

De uitrol eindigt met de overhandiging aan de beheerorganisatie, dit gebeurt vaak in twee fasen:

- › Formele notificatie dat de ICT-dienst of functionaliteit in kwestie beschikbaar is in de productie omgeving;
- › Formele notificatie dat de ICT-dienst of functionaliteit in kwestie volledig operationeel is en SLA's volledig in werking zijn.

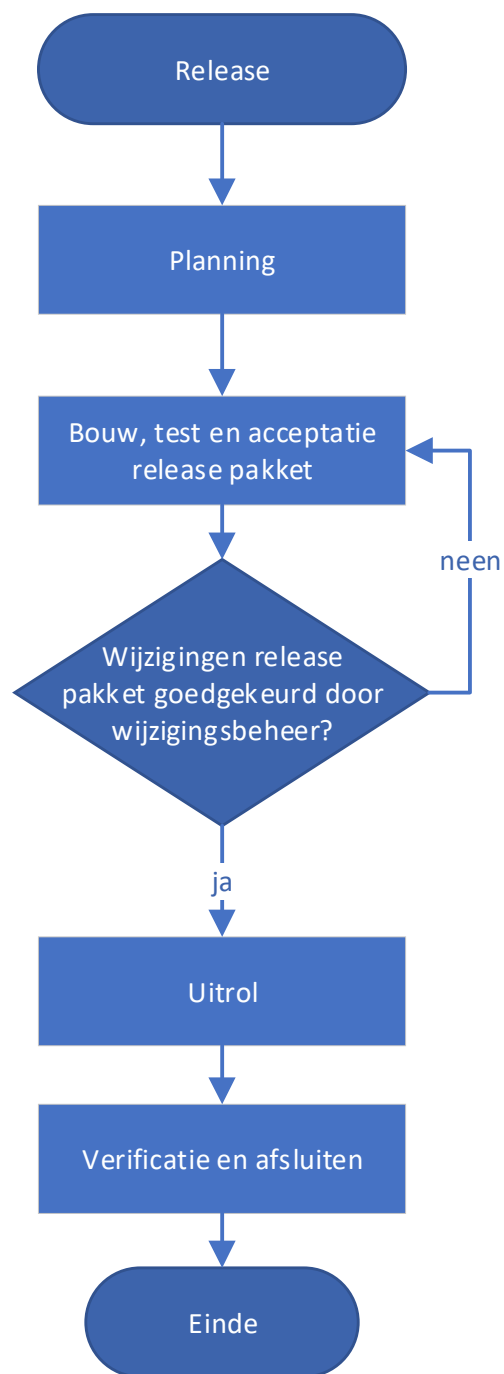
#### 2.3.4 Verificatie en afsluiten

Om een uitrol af te sluiten wordt ze eerst nog geverifieerd en worden lessen getrokken uit de release/uitrol. Bijkomend worden volgende activiteiten uitgevoerd:

- › Verificatie dat aan alle functionele, technische en informatieveiligheidsvereisten zijn voldaan;
- › Controle dat alle acties, noodzakelijke herstellingen (*fixes*) en wijzigingen zijn doorgevoerd;
- › Feedback van gebruikers, beheersorganisatie en andere belanghebbenden;
- › Terugkoppeling naar het proces wijzigingsbeheer;
- › Kwaliteitscontrole op de uitrol;
- › Nagaan of er geen capaciteits-, performantie- of andere problemen zijn opgedoken na de uitrol;
- › Verificatie dat eventuele problemen, gekende fouten en tijdelijke oplossingen gedocumenteerd zijn en goedgekeurd door alle betrokken partijen;
- › Opvolgingen van incidenten en problemen veroorzaakt door de uitrol;
- › Formele overhandiging naar de beheersorganisatie, inclusief de nodige documentatie;
- › Een post-implementatie review door het proces wijzigingsbeheer waar vereist.



### 2.3.5 Het proces



### 3. LINK MET ANDERE BEHEERSPROCESSEN

#### 3.1 Link met wijzigingsbeheer

Er zijn heel wat gelijkenissen tussen wijzigingsbeheer en release/deployment beheer:

- › Beide hebben te maken met wijzigingen in de productieomgeving;
- › Beide doen dit op een gecontroleerde wijze;
- › Beide doen dit met het oog op minimalisatie of minstens beheer van de bijhorende risico's.

Maar waar de intenties van beide processen gelijkaardig zijn, zijn er toch ook verschillen:

- › Wijzigingsbeheer buigt zich over kleinere, individuele wijzigingen uitgevoerd binnen een gepland – relatief kort – tijdsbestek. Hierbij gaat het over installatie, modificatie of verwijdering van componenten op een gecontroleerde en goedgekeurde wijze.
- › Release en deployment beheer zorgt voor implementatie van grotere en/of samengestelde groepen van wijzigingen binnen een gepland – relatief lang – tijdsbestek (de release windows) met het oog op een zo min mogelijke verstoring van de dagdagelijkse werking van de omgeving. Release en deployment beheer bundelt aldus vaak verschillende wijzigingen in één uitrol. Het doet hierbij beroep op het proces wijzigingsbeheer bvb voor de goedkeuring van de wijzigingen in een release pakket.

Volgende tabel zet de voornaamste verschillen op een rij:

<b>Wijzigingsbeheer</b>	<b>Release en deployment beheer</b>
Analyseert de wijzigingen in het release en deployment plan en keurt ze goed.	Bouwt, test, accepteert en rolt wijzigingen uit als één geheel (release pakket).
Pre- en post uitrol activiteiten.	Uitrol activiteiten.
(Relatief) korte termijn planningskalender	Lange-termijn release windows
Niet alle wijzigingen zijn opgenomen in een release.	Alle releases betreffen één of meerdere wijzigingen.
Goedkeuringsproces.	Implementatieproces (pakketten van goedgekeurde wijzigingen).
Post implementatie reviews.	Versie controle.

## 3.2 Hoe zijn de processen wijzigingsbeheer, asset en configuratie beheer en release en deployment beheer onderling gerelateerd?

Wijzigingsbeheer zorgt voor een systeem van autorisatie en opvolging zodat enkel goedgekeurde wijzigingen worden uitgevoerd.

Asset en configuratie beheer zorgt voor een up-to-date database met de nodige informatie over wijzigingen, software en hardware configuratie-items, release pakketten en alle andere relevant informatie over de betrokken configuratie-items.

Release en deployment management zorgt voor de voorbereiding en samenvoegen van wijzigingen in een release pakket dat dan kan worden uitgerold in productie.

**Wijzigingsbeheer** (voor meer informatie zie document: [‘Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer’](#)):

- › Heeft asset en configuratie beheer nodig om de gevolgen van een wijziging op alle betrokken configuratie-items te evalueren;
- › Heeft release en deployment management nodig om de nodige wijzigingen samen te voegen tot een release pakket voor een succesvolle implementatie met minimale verstoring van de productie omgeving.

**Asset en configuratie beheer** (voor meer informatie zie document: [‘Vo Informatieclassificatie – Minimale maatregelen – asset en configuratiebeheer’](#)):

- › Heeft wijzigingsbeheer nodig om ervoor te zorgen dat enkel goedgekeurde wijzigingen worden uitgevoerd;
- › Heeft release en deployment management nodig voor de nodige informatie over de release pakketten zodat de CMS bijgewerkt kan worden na uitrol van een release pakket in productie.

**Release en deployment management:**

- › Heeft wijzigingsbeheer nodig om de nodige wijzigingen goed te keuren en op te volgen doorheen het release proces;
- › Heeft asset en configuratie beheer nodig om de gevolgen voor de betrokken configuratie-items te evalueren en om de release pakketten te kunnen samenstellen.

---

## 4. PRESTATIE-INDICATOREN (KPI'S)

Prestatie-indicatoren die door de dienstenorganisatie kunnen worden gemeten, zijn onder andere:

- › Verbetering van de prestatie van een gewijzigde dienstverlening;
- › Verlaging van het aantal incidenten na implementatie;
- › Verhoging van de tevredenheid van gebruikers en andere belanghebbenden;
- › Vermindering van de kosten gerelateerd aan incidenten en problemen;
- › Vermindering van de afwijkingen geconstateerd tijdens audits van de omgeving.

Het vastleggen van de juiste prestatie-indicatoren is een moeilijke klus die de nodige aandacht vraagt: een teveel aan KPI's zal de organisatie (te) veel werk bezorgen, maar te weinig of onjuiste KPI's schetsen geen goed beeld van de kwaliteit van het proces.