Informatieclassificatie Vlaamse overheid (Vo-ICR)

Asset en configuratie beheer (asset & configuration management)

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

© KOPIEERRECHTEN: VLAAMSE OVERHEID, 2017-2022

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 (Vo) 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 asset en configuratie beheer. Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 4 delen. Eerst worden de minimale maatregelen besproken, alvorens in het 2de 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

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
v.0.1	07 november 2019	Kristel VAN AKEN	Draft
v.0.2	19 november 2019	Kristel VAN AKEN	Feedback pre-taakgroep
v.0.3	29 november 2019	Kristel VAN AKEN	Feedback taakgroep
v.0.4	16 december 2019	Kristel VAN AKEN	Feedback leespanel en consistentie check
v.1.0	16 december 2019	Kristel VAN AKEN	Versie gepubliceerd in pdf
v.1.1	20 maart 2020	Kristel VAN AKEN	Links toegevoegd
v.1.2	21 januari 2021	Kristel VAN AKEN	Integriteit toegevoegd
v.1.3	28 september 2021	Kristel VAN AKEN	Beschikbaarheid toegevoegd
v.2.0	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
V.2.1	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 - incident beheer*
  - *Vo Informatieclassificatie - Minimale maatregelen - probleem beheer*
  - *Vo Informatieclassificatie - Minimale maatregelen - release en deployment beheer*
  - *Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer*
- *Vo Informatieclassificatie – Overzicht baseline maatregelen* (XLS)

De laatste versies van deze documenten zijn te raadplegen op vlaanderen.be.

Inhoudsopgave

INLEIDING

Het verschil tussen een asset en een configuratie-item

Assets kunnen meer zijn dan configuratie-items omdat ook niet-tastbare, niet-configureerbare bedrijfsmiddelen meegerekend worden zoals informatie en kennis. Elk configuratie-item is een asset, maar niet alle assets zijn configuratie-items; de verzameling configuratie-items van een organisatie is dus een subset van haar verzameling assets. In het kader van het VO ICR is vooral de opvolging van de configuratie-items belangrijk omdat deze gebruikt worden in andere beheersprocessen zoals wijzigingsbeheer en incident beheer (voor meer informatie zie documenten: '*Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer*' & '*Vo Informatieclassificatie - Minimale maatregelen - incident beheer'*).

Een andere manier om het onderscheid tussen een configuratie-item en een asset te maken is het volgende: enkel een configuratie-item wordt beheerd door de processen wijzigings- of release en deployment beheer, een asset dat geen configuratie-item is, valt dus buiten scope van het proces wijzigingsbeheer en/of release en deployment beheer.

In het kader van de minimale maatregelen worden enkel configuratie-items in de scope opgenomen. Dit neemt niet weg dat ook assets beheerd moeten worden.

Het proces asset en configuratie beheer

Het proces asset en configuratie beheer draagt er zorg voor dat de gegevens over de ICT-infrastructuur, bedrijfsmiddelen en -diensten betrouwbaar worden vastgelegd en dat actuele en relevante gegevens aan andere ICT-beheerprocessen worden geleverd over de bedrijfsmiddelen, hun onderlinge samenhang (relaties) en de relaties met de ICT-diensten. Met een goed asset en configuratie beheerproces kunnen de overige processen effectiever en efficiënter werken en is duidelijk welke bedrijfsmiddelen deel uitmaakt van de ICT-dienstverlening.

Asset en configuratie beheer is nodig om een volledig en actueel overzicht te hebben en zo de overige ICT-beheerprocessen van de juiste informatie te voorzien. Configuratie-items, hun kenmerken en onderlinge samenhang dienen juist, volledig en tijdig te worden geïdentificeerd en vastgelegd; is dit niet het geval, dan bestaat het risico dat de hiervan afhankelijke ICT-beheerprocessen niet van juiste en volledige informatie worden voorzien over de configuratie-items. Hierdoor kunnen zowel de beschikbaarheid, integriteit, vertrouwelijkheid van informatie als controleerbaarheid van de ICT-diensten worden aangetast. Periodiek dienen de configuratie-items vergeleken te worden met de werkelijkheid en eventuele verschillen dienen bijgewerkt te worden in de *Configuration Management System* (CMS).

Asset en configuratie beheer heeft als hoofddoel om van alle configuratie-items in de organisatie een overzicht te hebben. Dit overzicht is cruciaal voor andere processen zoals incidentbeheer, patchmanagement, wijzigingsbeheer, enz.

De andere doelstellingen van asset en configuratie beheer voor informatiebeveiliging omvatten:

- Het onder controle brengen van een steeds veranderende ICT-infrastructuur, bedrijfsmiddelen en -diensten;
- Voorkomen dat er verschillende (en dus verouderde) versies van hetzelfde configuratie-item in productie komen of zijn door juiste, volledige en tijdige informatieverstrekking aan de andere beheersprocessen;

- Vereenvoudigen van de opvolging van kwetsbaarheden door documenteren van de juiste versies in de CMS;
- Opsporen van niet-geautoriseerde apparatuur in de organisatie door een goede inventaris van toegestane apparatuur.
- Opsporen van niet-geautoriseerde wijzigingen aan de configuratie door de vergelijking met de informatie in de CMS.

Noot: de definitie en opzetten van een CMS valt buiten scope van dit document.

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Het beheren van configuratie-items omvat een aantal activiteiten die, afhankelijk van de klasse waartoe de getroffen informatie behoort, al dan niet verplicht uitgevoerd moeten worden. Deze activiteiten zijn (zie hoofdstuk '*De bouwstenen van asset en configuratie beheer*')

- Registratie;
- Administratie;
- Statusbewaking;
- Verificatie.

Het proces zelf is minimaal beschikbaar tijdens kantooruren (10ux5dagen).

De CMS moet 24x7 beschikbaar zijn.

- De informatie in de CMS krijgt minimaal vertrouwelijkheidsklasse 3 en integriteitsklasse 2 toegewezen.

In volgende paragrafen worden enkele noodzakelijke attributen verduidelijkt.

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 en Klasse 3 kennen dezelfde maatregelen: › Alle ICT-componenten die deel uitmaken van de ICT-architectuur nodig voor de ICT-dienstverlening moeten gedefinieerd worden als configuratie-item in de CMS; › Elke ICT-component die ook een configuratie-item is, moet geregistreerd worden in de CMS; › Elk configuratie-item moet beheerd worden, d.w.z. toegevoegd indien nieuw, de nodige attributen wijzigen waar nodig, uit de CMS verwijderen zodra uitgefaseerd. › Van elk configuratie-item moet de status bijgehouden en up-to-date gehouden worden; › Jaarlijks moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? › Jaarlijks moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.
	Alle maatregelen van Klasse 1 / Klasse 2 / Klasse 3 + › Tweemaal per jaar of na wijziging of release moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? › De resultaten van deze inhoudelijke verificatie worden gerapporteerd aan de betrokken toepassingseigena(a)r(en).

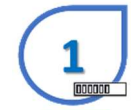
	〉 Jaarlijks of na wijziging van de eigenaar moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.
	Alle maatregelen van Klasse 1 / Klasse 2 / Klasse 3 + Klasse 4 + 〉 Viermaal per jaar of na wijziging of release moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? 〉 De resultaten van deze inhoudelijke verificatie worden gerapporteerd aan de betrokken toepassingseigena(a)r(en) en aan de DPO. 〉 Tweemaal per jaar of na wijziging van de eigenaar moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.

Integriteit

IC klasse	Minimale maatregelen
	〉 Alle ICT-componenten die deel uitmaken van de ICT-architectuur nodig voor de ICT-dienstverlening moeten gedefinieerd worden als configuratie-item in de CMS; 〉 Elke ICT-component die ook een configuratie-item is, moet geregistreerd worden in de CMS; 〉 Elk configuratie-item moet beheerd worden, d.w.z. toegevoegd indien nieuw, de nodige attributen wijzigen waar nodig, uit de CMS verwijderen zodra uitgefaseerd. 〉 Van elk configuratie-item moet de status bijgehouden en up-to-date gehouden worden; 〉 Jaarlijks moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? 〉 Jaarlijks moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.
	Klasse 2 en Klasse 3 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 + 〉 De informatie in de CMS krijgt minimaal integriteitsklasse 2 – toepassen van de minimale maatregelen voor deze klasse.
	Alle maatregelen van Klasse 1 + Klasse 2 / Klasse 3 + 〉 Tweemaal per jaar of na wijziging of release moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? 〉 De resultaten van deze inhoudelijke verificatie worden gerapporteerd aan de betrokken toepassingseigena(a)r(en). 〉 Jaarlijks of na wijziging van de eigenaar moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.

	Alle maatregelen van Klasse 1 + Klasse 2 / Klasse 3 + Klasse 4 + 〉 Viermaal per jaar of na wijziging of release moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? 〉 De resultaten van deze inhoudelijke verificatie worden gerapporteerd aan de betrokken toepassingseigena(a)r(en) en aan de DPO. 〉 Tweemaal per jaar of na wijziging van de eigenaar moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.

Beschikbaarheid

IC klasse	Minimale maatregelen
    	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Beschikbaarheid van het proces asset en configuratiebeheer is minimaal kantooruren (5d x 10u)

1.2 Minimale specifieke (GDPR) maatregelen

De minimale algemene fysieke maatregelen moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing.

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Er zijn geen GDPR maatregelen voor klasse 1 en klasse 2.
	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: 〉 Jaarlijks of na wijziging of release moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? 〉 De resultaten van deze inhoudelijke verificatie worden gerapporteerd aan de betrokken toepassingseigena(a)r(en) en naar de DPO. 〉 Jaarlijks of na wijziging van de eigenaar moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.
	Er zijn geen GDPR maatregelen voor klasse 5.

Integriteit

IC klasse	Minimale maatregelen
	Er zijn geen GDPR maatregelen voor klasse 1 en klasse 2.
	Maatregelen voor Klasse 3: 〉 Jaarlijks of na wijziging of release moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid? 〉 De resultaten van deze inhoudelijke verificatie worden gerapporteerd aan de betrokken toepassingseigena(a)r(en) en naar de DPO. 〉 Jaarlijks of na wijziging van de eigenaar moet geverifieerd worden of de eigenaar van elk configuratie-item nog correct geïdentificeerd is.

	Maatregelen voor Klasse 4: Alle maatregelen van Klasse 1 / Klasse 2 / Klasse 3 + 〉 Tweemaal per jaar of na wijziging of release moeten de attributen van elk configuratie-item inhoudelijk geverifieerd worden: weerspiegelt de waarde van de attributen de geïnstalleerde werkelijkheid.
	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 algemene maatregelen voor asset en configuratiebeheer moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing (zie hoofdstuk '*minimale algemene maatregelen*').

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van asset en configuratiebeheer toegepast worden:

Beschikbaarheid, Integriteit & vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 De eigen mobiele toestellen duidelijk identificeren, veilig configureren (met de nodige anti-malware software en met software die alle data op het toestel vanop afstand kunnen wissen) en de identificatie bijhouden in een centraal register (Ref. KSZ 3.2.1 e). 〉 Elke organisatie moet over een permanent bijgewerkte inventaris beschikken van het informaticamateriaal en de software (Ref. KSZ 5.5.2). 〉 Elke organisatie moet een geactualiseerde cartografie bijhouden van de geïmplementeerde technische stromen via het Extranet van de sociale zekerheid. De veiligheidsconsulent moet hierover geïnformeerd worden (Ref. KSZ 5.10.4).

 	〉 Elke organisatie moet alle middelen inclusief aangekochte of ontwikkelde systemen toevoegen aan het beheerssysteem van de operationele middelen (Ref. KSZ 5.11.12). 〉 In functie van de rol voor een specifieke (groep) verwerking (verwerker of verwerkings-verantwoordelijke), minimaal de volgende activiteiten uitvoeren: * de opname van de verwerking in het centraal register van de verwerkingsverantwoordelijke of van de verwerker. (Ref. KSZ 5.15.2 b).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1 Wat is asset en configuratie beheer

Asset en configuratie beheer is een preventieve maatregel.

De hoofdbekommernis van asset en configuratie beheer is de identificatie, documentatie en administratie van alle configuratie-items nodig om een ICT-dienst te kunnen leveren. Om dit te kunnen doen, omvat het proces volgende activiteiten (zie hoofdstuk: *'De bouwstenen van asset en configuratiebeheer')*

- **Registratie**: Invoeren/registreren van nieuwe configuratie-items,
- **Administratie**: beheer van de CMS,
- **Statusbewaking**: statusbewaking van de configuratie-items,
- **Verificatie**: verificatie van CMS.

2.2 Succesfactoren voor een goed asset en configuratie 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 asset en configuratie beheer omvatten:

- Het bepalen van het juiste niveau van detail,
- De nodige discipline opbrengen voor het onderhoud van de CMS,
- Een zo laag mogelijke foutgevoeligheid van de CMS bereiken.

2.3 De bouwstenen van asset en configuratie beheer

2.3.1 Registratie

Binnen deze stap worden de componenten van de ICT-infrastructuur, bedrijfsmiddelen en -diensten opgenomen in de CMS. Om dit te verwezenlijken moeten alle configuratie-items worden geïdentificeerd en geregistreerd. Deze procedure is van toepassing op de gehele ICT-infrastructuur en is geldig vanaf het moment van levering van goederen, tot het moment dat de configuratie-items in productie kunnen worden genomen en – op het einde van hun levensduur – uitgefaseerd worden.

Activiteiten omvatten het registreren van alle configuratie-items, het bepalen en onderhouden van naamgeving en het vastleggen van hun attributen.

Attributen beschrijven de karakteristieken van een configuratie-item en moeten steeds bijgewerkt worden wanneer een attribuut wijzigt. Volgende attributen moeten minstens in de CMS opgenomen zijn:

- Definitie type configuratie-item,
- Definitie service componenten,
- VO-informatie klasse (hoogste ingeval van meerdere klassen),
- Versienummering,

- Informatie over hun licentie,
- Locatie (service locatie, bvb in geval van cloud of fysieke locatie),
- Relatie met andere configuratie-items,
- Relatie met andere services of organisatie;
- Informatie over de eigenaar (zowel entiteit die verantwoordelijk is als de applicatie eigenaar),
- Status,
- Beschikbare documentatie,
- Audit trail: minstens datum aanmaak/laatste wijziging en wie de laatste wijziging heeft aangemaakt.

Met behulp van deze attributen wordt informatie opgeslagen die relevant is voor het betrokken configuratie-item en die aansluit op de informatiebehoefte van andere processen.

De CMS levert niet alleen correcte en volledige informatie over de configuratie-items, maar dankzij attributen zoals relaties met andere configuratie-items en servicecomponenten, levert de CMS ook input over de architectuur van de ICT-dienstverlening.

2.3.2 Administratie

Administratie zorgt ervoor dat de inhoud van de asset en configuratie beheerdatabase (de CMS) actueel blijft door alleen geautoriseerde en geïdentificeerde configuratie-items toe te laten, te registeren en te bewaken. Bij alle activiteiten waarbij opgenomen kenmerken van – of relaties tussen – configuratie-items wijzigen, dient deze wijziging te worden geregistreerd in de CMS. Een configuratie-item zelf updaten is het resultaat van een ander proces zoals wijzigingsbeheer, patchmanagement, etc.

Tevens zorgt deze stap ervoor dat geen configuratie-item wordt toegevoegd, aangepast, vervangen of verwijderd, zonder dat daarvan passende documentatie aanwezig is, zoals een goedgekeurd wijzigingsverzoek of een aangepaste specificatie.

Er dienen procedures en werkinstructies aanwezig te zijn, voor het afhandelen van nieuwe configuratie-items en wijzigingen aan bestaande configuratie-items.

2.3.3 Statusbewaking van de configuratie-items

Deze stap zorgt voor de registratie van actuele en historische gegevens over de status van een configuratie-item gedurende de gehele levenscyclus. Hiervoor dienen de historische gegevens met betrekking tot de componenten en de daaraan gerelateerde gegevens beschikbaar te blijven. De levenscyclus van een component kan in verschillende stadia worden ingedeeld. Statusbewaking maakt het mogelijk om veranderingen in status te traceren, zoals besteld, ontvangen, op voorraad, in ontwikkeling, wordt getest, is geaccepteerd, in productie, in onderhoud en uitgefaseerd. Door de datum van elke statusverandering te registreren, kan een goed beeld ontstaan van de levenscyclus van een product: de besteltijden, de installatietijden en de hoeveelheid onderhoud en ondersteuning die eraan besteed is en het aantal beveiligingsincidenten dat eraan kan worden gerelateerd.

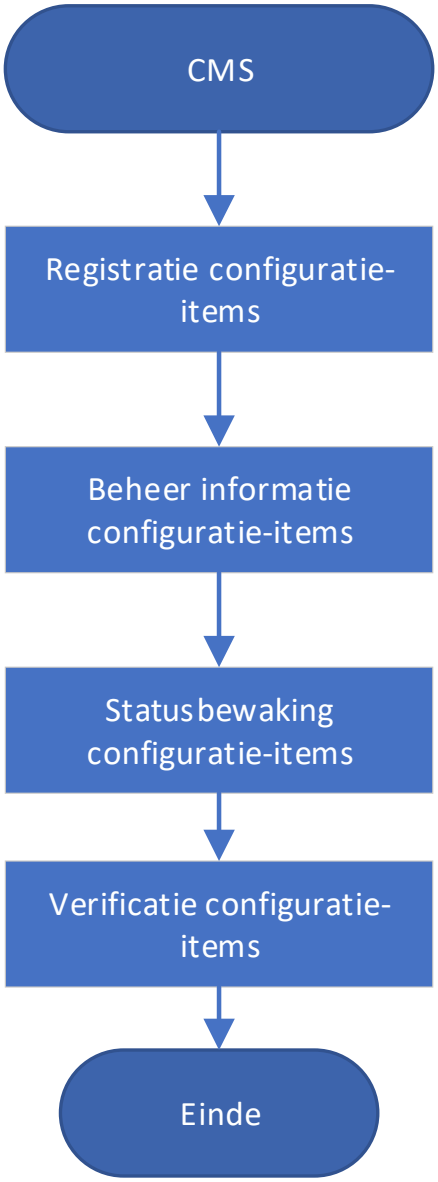
2.3.4 Verificatie

Deze stap zorgt ervoor dat de actuele situatie nog overeenkomt met de gegevens in de CMS. Het kan voorkomen dat de ICT-infrastructuur is gewijzigd zonder dat asset en configuratie beheer daarvan op de hoogte is gebracht. Om de actualiteit van de gegevens in de CMS te garanderen is het noodzakelijk op regelmatige tijdsstippen de gegevens te toetsen aan de werkelijkheid.

De verificatie vindt op niet-geplande en op geplande basis plaats:

- **Op niet-geplande basis**. Tijdens de dagelijkse werkzaamheden kunnen door de expertiseteams afwijkingen worden geconstateerd. Er kan bijvoorbeeld tijdens het oplossen van een incident geconstateerd worden dat de CMS afwijkt van de werkelijkheid.
- **Op geplande basis**. Als uit het aantal opgemerkte en gerapporteerde afwijkingen blijkt dat de betrouwbaarheid en volledigheid van de CMS tekortschiet, kan besloten worden om op een bepaald ogenblik de verificatie te herdoen of een audit uit te voeren op het proces.

2.3.5 Het proces



3. LINK MET ANDERE BEHEERPROCESSEN

Aangezien de CMS de basisinformatie over de te beheren configuratie-items aanlevert, is er een rechtstreekse link met:

3.1 Wijzigingsbeheer

(Voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer'):
Door het attribuut 'relaties' kan de impact van de wijzigingen op alle betrokken configuratie-items op voorhand ingeschat worden. Dit werkt in twee richtingen: wijzigingen aan configuratie-items resulteren ook vaak in een wijziging in de CMS (bvb als een nieuwe versie is geïnstalleerd);

3.2 Beheer van incidenten en problemen

(Voor meer informatie zie documenten: Vo Informatieclassificatie - Minimale maatregelen - incident beheer' & '*Vo Informatieclassificatie - Minimale maatregelen - probleem beheer'*):
Ook hier kan het attribuut 'relaties' gebruikt worden om de gevolgen van een incident in te schatten. De attributen leveren vervolgens informatie die gebruikt kan worden om de oorzaak van een incident op te sporen en de gevolgen in te dijken.

3.3 Release/deployment management

(Voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen - release en deployment beheer'*):
De informatie uit de CMS wordt gebruikt om de impact van nieuwe releases in te schatten en te bekijken welke configuratie-items deel moeten uitmaken van de release. Aan de andere kant moet bij een release de informatie van de betrokken configuratie-items in de CMS toegevoegd dan wel bijgewerkt worden.

3.4 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 relevante 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:

- 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:

- 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:

- Periodiciteit van de evaluatie van de structuur van de CMS.
- Periodiciteit van controle op de juistheid en volledigheid van de CMS.
- Aantal incidenten per impactcategorie, per evaluatieperiode toe te schrijven aan afwijkingen in de CMS.
- Het aantal configuratie-items waarvan de omschrijving is aangepast.
- Het aantal keren dat aangetroffen configuratie-items niet zijn geautoriseerd.
- Het aantal keren dat geregistreerde configuratie-items niet zijn aangetroffen.
- Het aantal keren dat geregistreerde configuratie-items onjuist zijn geregistreerd: afwijking op het niveau van attributen, die zijn ontdekt tijdens audits.
- Het aantal audits dat is uitgevoerd.
- Het aantal rapportages dat is gepubliceerd.
- Het aantal raadplegingen van de CMS.
- De snelheid waarmee verzoeken om registratie zijn afgehandeld.

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.