Informatieclassificatie Vlaamse overheid (Vo-ICR)

Wijzigingsbeheer

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

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 (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen wijzigingsbeheer. 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 Vo 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	30 augustus 2019	Kristel VAN AKEN	Draft
v.0.2	18 september 2019	Kristel VAN AKEN	Feedback Johan Smekens, Beau Janssens
v.0.3	10 oktober 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	Versie gepubliceerd in pdf
v.1.2	November 2020	Kristel VAN AKEN	Integriteit toegevoegd
v.1.3	6 augustus 2021	Beau JANSSEN	Wijzigingen aangebracht voor Beschikbaarheid
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 - asset en configuratiebeheer*
  - *Vo Informatieclassificatie - Minimale maatregelen - beheer aanvragen*
  - *Vo Informatieclassificatie - Minimale maatregelen – incidentbeheer*
  - *Vo Informatieclassificatie - Minimale maatregelen – PAM*
  - *Vo Informatieclassificatie - Minimale maatregelen - release en deployment beheer*
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS)

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

Inhoudsopgave

Inleiding

Het proces wijzigingsbeheer

Het proces wijzigingsbeheer beschrijft de afhandeling van door te voeren geplande wijzigingen vanaf het ogenblik dat een wijzigingsaanvraag ingediend wordt tot en met de uitvoering en afsluiting van de wijziging.

De term wijzigingsaanvraag (RFC = *Request for change*) wordt gebruikt zolang het verzoek tot wijziging in aanvraagfase is. Zodra de aanvraag is goedgekeurd en in uitvoering komt, spreekt men over wijziging.

Het wijzigingsproces heeft als doel het zeker stellen dat een gestandaardiseerde werkwijze wordt gehanteerd voor het behandelen van wijzigingen zodat deze conform de afspraken kunnen worden afgehandeld met minimale impact op de kwaliteit van de dienstverlening en op de zakelijke processen. Het proces tracht dit te bereiken door ervoor te zorgen dat:

- Alle wijzigingsaanvragen worden beoordeeld op het doel, risico's en impact op de dienstverlening;
- Wijzigingsaanvragen worden behandeld volgens een gestelde prioriteit zodat de middelen van de organisatie efficiënt worden aangewend;
- Alle wijzigingen tijdig en volledig worden doorgevoerd;
- Enkel gemotiveerde en goedgekeurde wijzigingen worden uitgevoerd;
- Alle wijzigingen worden ingepland, getest en voorzien van een roll-back plan zodat bij falen van de implementatie de vorige, stabiele omgeving wordt hersteld;
- Alle wijzigingen worden gedocumenteerd en de bijhorende configuratie-items worden bijgewerkt.

Wijzigingen kunnen voortkomen uit diverse behoeften, zoals nieuwe functionele en technische eisen, vanwege bedrijfsoverwegingen of een nieuwe dan wel veranderde wet- en regelgeving, en oplossingen voor problemen. Kwetsbaarheden die verholpen worden door een beveiligingsupdate (patch) zijn een ander voorbeeld van een wijziging.

De scope van het proces wijzigingsbeheer beperkt zich tot die wijzigingen die niet aanzien kunnen worden als standaardwijzigingen zoals service aanvragen door gebruikers, namelijk indien zij:

- Invloed hebben op de dienstverlening bvb door degradatie of uitval,
- Tot een verandering leiden van de functionaliteit van een dienst of proces,
- Leiden tot een wijziging aan de configuratie database (CMDB).

Alle andere veranderingen behoren dus niet tot het wijzigingsproces, bvb het wijzigen van een paswoord van een gebruiker of het aanmaken van een account wordt niet aanzien als een wijziging, maar wel als een service aanvraag; dit wordt behandeld door het proces 'beheer van service aanvragen' en is gedocumenteerd in '*Vo Informatieclassificatie – Minimale maatregelen - Beheer van aanvragen*'.

Verschil wijzigingsaanvraag en service aanvraag

Een wijzigingsaanvraag betreft een verzoek tot verandering aan een informatie verwerkende component die ingepland kan worden. Wijzigingsaanvragen worden ingediend door diverse partijen en vanuit verschillende processen (zowel zakelijke als beheersprocessen) en doorlopen alle stappen van het wijzigingsproces (waaronder motivatie en goedkeuring).

Service aanvragen (voor meer informatie zie document: '*Vo Informatieclassificatie – Minimale maatregelen - Beheer van aanvragen*') gaan over vragen van gebruikers over informatie, advies, een standaard wijziging of toegang tot een service. Een standaardwijziging in deze context is een vooraf

gedefinieerde en goedgekeurde wijziging zoals een paswoord reset of toegang tot een bepaalde toepassing of … Deze standaardwijziging hoeft dus niet meer apart goedgekeurd te worden en hoeft de verschillende stappen in het wijzigingsproces niet te volgen.

Wijzigingsbeheer het kader van informatieclassificatie

Informatieclassificatie wordt uitgedrukt in drie kwaliteitskenmerken, men spreekt dan over:

- Vertrouwelijkheid
- Integriteit
- Beschikbaarheid

Merk op dat in een eerste fase van het project informatieclassificatie de focus ligt op vertrouwelijkheid en technische integriteit (functionele integriteit en beschikbaarheid zullen later ingevuld worden); beschikbaarheid wordt inherent meegenomen in de scope van wijzigingsbeheer maar er worden geen maatregelen uitgewerkt (dit wordt opgenomen in het programma bedrijfscontinuïteit).

Wijzigingsbeheer in het kader van informatieclassificatie is dus het beheer van geplande wijzigingen aan de ICT-infrastructuur of aan de ICT-dienstverlening.

1. MINIMALE MAATREGELEN

Het beheren van wijzigingsaanvragen 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 wijzigingsbeheer'*):

- Registratie van de wijzigingsaanvraag;
- Goedkeuring van de wijzigingsaanvraag;
- Impact van de wijziging bepalen;
- Urgentie van de wijziging bepalen;
- Inplannen van de wijziging;
- Uitvoeren van de wijziging;
- Validatie van de wijziging;
- Evaluatie van de wijziging (*lessons learned*);
- Afsluiten van de wijziging.

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

Registratie van de wijzigingsaanvraag

Elke wijzigingsaanvraag wordt geregistreerd. Minimaal wordt hiervoor een logboek aangelegd, dit kan eventueel een manueel onderhouden document zijn.

Het is mogelijk dat er verschillende logboeken voor wijzigingen bestaan, bijvoorbeeld omdat er met verschillende leveranciers en verschillende CAB's wordt gewerkt.

Het logboek staat onder controle van de eigen organisatie maar het beheer ervan kan uitbesteed worden.

Voor meer informatie zie hoofdstuk: '*De wijzigingsaanvraag'*.

Goedkeuring van de wijzigingsaanvraag

De toepassingseigenaar is steeds betrokken bij de goedkeuring van wijzigingsaanvragen die impact hebben op de toepassing maar sommige wijzigingen moeten via de CAB goedgekeurd worden. Voor kleinere organisaties zonder formele CAB worden meerdere partijen bij de goedkeuring betrokken, bvb de veiligheidsconsulent of DPO.

Volgende scenario's zijn mogelijk:

- Goedkeuring door de toepassingseigenaar:
  - Dit is de individuele organisatie die zelf de toepassing beheert, bvb AGO, MOW;
  - De dienstenorganisator die de toepassing beheert en ter beschikking stelt van andere organisaties, bvb HFB/HB+ dienstverlening, AIV voor diensten rond MAGDA, AGO voor Vlimpers, FB voor ORAFIN).
- Goedkeuring door de wijzigingsbeheerder van de dienstenleverancier:
  - Centrale dienstverlener (HB+);
  - Een door de organisatie toegewezen leverancier met een specifiek contract voor maatwerk, bvb Cronos, Realdolmen;

〉 Bij directe dienstafname met een generiek contract en zonder maatwerk, bvb IaaS, SaaS, PaaS, enz.

Welke wijzigingen via de CAB goedgekeurd worden, hangt af van:

〉 De prioriteit (P1 en P2),
〉 De informatieklasse.

Voor meer informatie zie hoofdstuk: '*Goedkeuring van de wijzigingsaanvraag*'.

Bepalen van de prioriteit

De urgentie en de impact worden door de aanvrager gedefinieerd en gevalideerd door de toepassingseigenaar voor het bepalen van de prioriteit.

De hoogte prioriteit P1 wordt enkel toegepast voor wijzigingen ten gevolge van P1 incidenten en noodwijzigingen.

Voor meer informatie zie hoofdstuk: '*Bepalen van de prioriteit van de wijzigingsaanvraag*'.

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Registratie van de wijzigingsaanvraag in een logboek; 〉 De informatie in het logboek krijgt minimaal vertrouwelijkheidsklasse 2 toegewezen; 〉 Impact van de wijziging bepalen; 〉 Urgentie van de wijziging bepalen; 〉 Minstens goedkeuring van de wijzigingsaanvraag door de toepassingseigenaar; 〉 Inplannen van de wijziging; 〉 Uitvoeren van de wijziging; 〉 Validatie van de wijziging voorafgaand aan in productie name is verplicht voor architecturale en functionele wijzigingen; 〉 Evaluatie van de wijziging (*lessons learned*) voor P1 wijzigingen (als gevolg van incidenten of noodwijzigingen); 〉 Afsluiten van de wijziging.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Registratie van de wijzigingsaanvraag in een logboek onder beheer van een wijzigingsbeheerder; 〉 Impact van de wijziging is minstens medium; 〉 Goedkeuring van de wijzigingsaanvraag via CAB; 〉 Validatie van de wijziging voorafgaand aan in productie name is altijd verplicht;

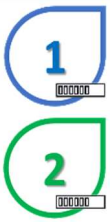
	〉 Evaluatie van de wijziging (*lessons learned*) vanaf P2 wijzigingen.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Impact van de wijziging is altijd hoog; 〉 Validatie van de wijziging voorafgaand aan in productie name en post-validatie; 〉 Altijd evaluatie van de wijziging (*lessons learned*).
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 / Klasse 4 + 〉 Registratie van de wijzigingsaanvraag in een centraal logboek onder beheer van een wijzigingsbeheerder; 〉 De informatie in het logboek krijgt minimaal vertrouwelijkheidsklasse 3 toegewezen; 〉 Goedkeuring van de wijzigingsaanvraag via CAB en DPO met in acht name van scheiding van functies en 4EYES validatie

Integriteit

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Registratie van de wijzigingsaanvraag in een logboek; 〉 De informatie in het logboek krijgt minimaal integriteitsklasse 2 toegewezen; 〉 Impact van de wijziging bepalen; 〉 Urgentie van de wijziging bepalen; 〉 Minstens goedkeuring van de wijzigingsaanvraag door de toepassingseigenaar; 〉 Inplannen van de wijziging; 〉 Uitvoeren van de wijziging; 〉 Validatie van de wijziging voorafgaand aan in productie name is verplicht voor architecturale en functionele wijzigingen; 〉 Evaluatie van de wijziging (*lessons learned*) voor P1 wijzigingen (als gevolg van incidenten of noodwijzigingen); 〉 Afsluiten van de wijziging.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Registratie van de wijzigingsaanvraag in een logboek onder beheer van een wijzigingsbeheerder; 〉 Impact van de wijziging is minstens medium; 〉 Goedkeuring van de wijzigingsaanvraag via CAB; 〉 Validatie van de wijziging voorafgaand aan in productie name is altijd verplicht; 〉 Evaluatie van de wijziging (*lessons learned*) vanaf P2 wijzigingen.

	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Impact van de wijziging is altijd hoog; 〉 De informatie in het logboek krijgt minimaal integriteitsklasse 3 toegewezen; 〉 Validatie van de wijziging voorafgaand aan in productie name en post-validatie; 〉 Altijd evaluatie van de wijziging (*lessons learned*).
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Registratie van de wijzigingsaanvraag in een centraal logboek onder beheer van een wijzigingsbeheerder; 〉 De informatie in het logboek krijgt minimaal integriteitsklasse 4 toegewezen; 〉 Goedkeuring van de wijzigingsaanvraag via CAB en DPO met in acht name van scheiding van functies en 4EYES validatie

Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Beschikbaarheid van het proces wijzigingsbeheer is minimaal kantooruren (5d x 10u)
	Klasse 3, Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Beschikbaarheid van het proces wijzigingsbeheer is minimaal kantooruren (24u x 7d)

1.2 Minimale specifieke (GDPR) maatregelen

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

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1.
 	Klasse 2 en klasse 3 kennen dezelfde maatregelen: 〉 Goedkeuring van de wijzigingsaanvraag via CAB inclusief DPO; 〉 Validatie van de wijziging voorafgaand aan in productie name en post-validatie altijd verplicht. 〉 Altijd evaluatie van de wijziging (*lessons learned*).
	Maatregelen voor Klasse 4: Alle maatregelen van Klasse 2 / Klasse 3 + 〉 Goedkeuring van de wijzigingsaanvraag via CAB en DPO met in acht name van scheiding van functies en 4EYES validatie.
	Er zijn geen GDPR maatregelen voor klasse 5.

Integriteit

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1.
 	Klasse 2 en klasse 3 kennen dezelfde maatregelen: 〉 Goedkeuring van de wijzigingsaanvraag via CAB inclusief DPO; 〉 Validatie van de wijziging voorafgaand aan in productie name en post-validatie altijd verplicht. 〉 Altijd evaluatie van de wijziging (*lessons learned*).
	Maatregelen voor Klasse 4: Alle maatregelen van Klasse 2 / Klasse 3 + 〉 Goedkeuring van de wijzigingsaanvraag via CAB en DPO met in acht name van scheiding van functies en 4EYES validatie.
	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

Er zijn geen KSZ specifieke maatregelen.

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Beheer van wijzigingen als maatregel

2.1.1. Preventie, detectie en reactie

Maatregelen worden genomen als gevolg van een geïdentificeerd risico. Volgende mogelijkheden doen zich voor:

- **Preventie**: vermijden dat iets gebeurt of het verlagen van de waarschijnlijkheid dat het gebeurt;
- **Detectie**: detecteren van de (potentiële) schade zou een bedreiging optreden;
- **Reactie**: beperken van de schade wanneer een bedreiging optreedt of het effect hiervan gedeeltelijk of geheel corrigeren.

Bij preventieve maatregelen wordt de dreiging verkleint tot het niveau dat ze aanvaardbaar is.

Detectie maatregelen zorgen ervoor dat een dreiging en het gevolg ervan tijdig ontdekt wordt.

Reactieve maatregelen richten zich op de gevolgen indien een dreiging zich toch voordoet, door het inperken of herstellen van de schade.

Wijzigingsbeheer is een reactieve maatregel.

2.1.2. De verschillende activiteiten van wijzigingsbeheer

Beheer van wijzigingen omvat (zie hoofdstuk: '*De bouwstenen van wijzigingsbeheer*'):

- Registratie van een wijzigingsaanvraag;
- Goedkeuren van een wijzigingsaanvraag;
- Bepalen van de prioriteit van een wijzigingsaanvraag;
- Inplannen van de wijziging;
- Uitvoeren en validatie van de wijziging;
- Afsluiten van de wijziging.

Het proces wijzigingsbeheer kent 3 grote stappen:

- Ten eerste: de voorbereiding: registreren van de wijzigingsaanvraag tot en met het inplannen;
- Ten tweede: de uitvoering: in deze stap wordt de gevraagde én goedgekeurde wijziging ontwikkeld, getest en in productie gebracht;
- Ten derde: evaluatie en afsluiten: focust op het resultaat van de wijziging.

2.1.3. Link met PAM

Priviliged Access Management (PAM) is het proces voor het beheer van speciale toegangsrechten tot informatie verwerkende systemen of – in ITIL termen – de configuratie-items. Deze speciale toegangsrechten laten veel meer activiteiten op deze systemen toe dan de geijkte gebruikersrechten.

Het is dan ook niet verwonderlijk dat het toekennen en gebruiken van deze rechten aan strenge regels moet voldoen teneinde fouten en misbruik te voorkomen.

Wijzigingen aan een configuratie-item in deze context van wijzigingsbeheer vereist in de meeste gevallen speciale toegangsrechten. Daarom is het belangrijk dat de wijzigingsaanvraag goed gemotiveerd wordt, goedgekeurd door een geautoriseerd persoon en dat enkel de uitvoerder(s) mag/mogen beschikken over deze speciale rechten in het tijdsbestek nodig om de wijziging tot een goed einde te brengen.

Het document '*Vo Informatieclassificatie – Minimale maatregelen – PAM*' beschrijft de interacties tussen beide processen en de vereisten voor speciale rechten voor uitvoering van wijzigingen per informatieklasse.

2.2. Succesfactoren voor een goed wijzigingsbeheer

Om tot een efficiënt en effectief wijzigingsbeheer te komen, zijn volgende parameters belangrijk. Zij kunnen meegenomen worden als prestatie-indicatoren of KPI's (zie hoofdstuk: '*Prestatie-indicatoren (KPI's)*') om het succes of falen van het proces te meten en bij te sturen waar nodig:

- **Kwaliteit van de voorbereiding:** een goede voorbereiding en documentatie versnelt het autorisatie proces en vermindert het aantal iteraties om tot een wijziging te komen.
- **Test en acceptatie van de wijziging:** onvoldoende of ontbreken van testen kan leiden tot een implementatie met negatieve impact op de kwaliteit van de dienstverlening of de stabiliteit van de omgeving waardoor terugdraaien van de wijziging nodig kan zijn.
- **Allocatie van middelen:** bij de beoordeling van de wijzigingsaanvraag is het niet alleen belangrijk om de impact op de dienstverlening in te schatten maar ook de benodigde middelen (personeel, materie experten, tooling, …).
- **Implementatie van wijzigingsbeheer:** een goede inbedding van het proces in de ICT en zakelijke processen is nodig om niet-geautoriseerde wijzigingen te vermijden.

2.3. De bouwstenen van wijzigingsbeheer

2.3.1. De wijzigingsaanvraag

Strikt genomen hoort de aanmaak en het indienen van de wijzigingsaanvraag niet bij het proces wijzigingsbeheer, maar het is wel een noodzakelijke input.

Een wijzigingsaanvraag betreft een functionele wijziging of een technische wijziging (m.i. een wijziging i.h.k.v. beveiliging) of beiden.

Wijzigingen kunnen aangevraagd worden vanuit verschillende kanalen:

- **Andere beheersprocessen** zoals incident beheer, probleembeheer: indienen van een technische wijzigingsaanvraag naar aanleiding van een incident of probleem;
- **Zakelijke processen**: functionele wijzigingsaanvragen;
- **Leveranciers**: nieuwe releases en upgrades waarbij structurele fouten worden gemitigeerd of weggenomen nieuwe functionaliteiten zijn geïmplementeerd (zowel functionele als technische wijzigingen zijn mogelijk). Ook kunnen bepaalde versies niet langer worden ondersteund;
- **Projecten**: een project kan meerdere functionele en/of technische wijzigingen tot gevolg hebben;
- **Wet- en regelgeving**: nieuwe of veranderde wet- en regelgeving kan aanleiding geven tot nieuwe vereisten die vertaald worden in wijzigingsaanvragen.

Merk op dat gebruikers geen wijzigingen aanvragen; gebruikers mogen enkel vooraf goedgekeurde wijzigingen vragen via het proces 'beheer van service aanvragen' (voor meer informatie zie document: '*Vo Informatieclassificatie – Minimale maatregelen – beheer van aanvragen*').

Alle wijzigingsaanvragen moeten worden geregistreerd en uitvoerig gedocumenteerd. Er worden door wijzigingsbeheer eisen gesteld aan de wijze waarop een wijzigingsaanvraag wordt ingediend en welke informatie daarbij minimaal moet worden verstrekt.

De wijzigingsaanvraag moet minstens volgende informatie bevatten:

- Informatie met betrekking tot de indiener van de wijzigingsaanvraag;
- Informatie met betrekking tot de goedkeuring van de wijzigingsaanvraag;
- Datum en tijd waarop de wijzigingsaanvraag is ingediend;
- Een omschrijving van de voorgestelde wijziging:
  - Indien van toepassing de referentie naar het achterliggende incident/probleem;
  - De configuratie-items die betrokken zijn bij deze voorgestelde wijziging;
  - Relaties of afhankelijkheden met andere (deel)processen;
- Een omschrijving wat de motivatie van de voorgestelde wijziging is;
- De resultaten van de voorgestelde wijziging, inclusief de consequenties als de voorgestelde wijziging niet wordt doorgevoerd;
- Een voorstel van de urgentie, inclusief motivatie, van de voorgestelde wijziging;
- De gewenste realisatiedatum, inclusief een motivatie;
- De impact op de zakelijke processen;
- De impact van de voorgestelde wijziging op het beveiligingsniveau;
- De impact van de voorgestelde wijziging op het beschermingsniveau van persoonsgegevens;
- De impact van de voorgestelde wijziging op de ICT-infrastructuur en ICT-dienstverlening.

Soorten wijzigingen

ITIL definieert twee verschillende soorten wijzigingen. Voor het inrichten van een effectief proces voor beheer van wijzigingen is het belangrijk een goed onderscheid tussen deze wijzigingen te maken.

- **Gewone wijziging**: Een gewone wijziging is een wijziging die binnen het vooropgestelde tijdsbesteken binnen de volledige workflow van het proces wijzigingsbeheer kan worden uitgevoerd zonder de zakelijke processen significant te benadelen.
- **Noodwijziging**: De noodwijziging is bedoeld voor wijzigingen, die fouten van een ICT-service herstellen, met in hoge mate een negatieve impact op de zakelijke processen en/of de ondersteunende infrastructuur. Noodwijzigingen wijken af van de normale procedures, omdat voor dit soort wijzigingen de benodigde middelen meteen moeten worden vrijgemaakt. Omdat noodwijzigingen afwijken van de normale workflow in het wijzigingsbeheer, moeten zij zoveel mogelijk vermeden worden, maar zeker na uitvoering goed opgevolgd en gedocumenteerd.

2.3.2. Goedkeuring van de wijzigingsaanvraag

De goedkeuring van de wijzigingsaanvraag geldt in eerste instantie de aanvraag zelf: is alle noodzakelijke informatie aanwezig? Is de aanvraag voldoende gedocumenteerd en gemotiveerd? Indien nodig moet de wijzigingsaanvraag door de aanvrager verder aangevuld worden.

Vervolgens moet de aanvraag geautoriseerd worden. Het goedkeuren van de wijziging gebeurt op 3 vlakken:

- **Financiële goedkeuring**: kosten-batenanalyse en budgettering;
- **Zakelijke goedkeuring**: goedkeuring van de gebruikers betreffende functionaliteitbehoefte en impact.

Strikt genomen horen beide uitgevoerd te zijn vooraleer de wijzigingsvraag in het proces wijzigingsbeheer wordt opgenomen.

- **Technische goedkeuring**: technische impact, veiligheid en haalbaarheid;

Als de wijzigingsaanvraag is geaccepteerd, wordt de informatie voor het verdere verloop van de wijziging vastgelegd in een wijzigingsregistratie. In het verdere verloop van de wijziging wordt hier steeds meer informatie aan toegevoegd, zoals:

- De toegekende prioriteit;
- De toegekende categorie;
- Beoordeling van de impact en benodigde middelen, denk hierbij ook aan de kosten;
- Testresultaten;
- Implementatieplan inclusief een fall back plan;
- Actuele datum en tijd van de wijziging;
- De reden van een eventuele afkeuring van de wijzigingsaanvraag.

De CAB

De *Change Advisory Board* (CAB) is een beslissingsforum waarbij:

- De leden beslissingsbevoegdheid hebben;
- De CAB zodanig samengesteld is dat er een evenwicht bestaat tussen de belangen van de beheersorganisatie (continuïteit en stabiliteit) en de zakelijke omgeving (nieuwe functionaliteit);
- De leden van de CAB gezamenlijk over voldoende beheer-, exploitatie- en materiekennis beschikken om verantwoorde besluiten over de wijzigingen te kunnen nemen.
- De verantwoordelijke voor bijvoorbeeld informatiebeveiliging en bedrijfscontinuïteitsbeheer via de wijzigingsbeheerder hun standpunten over wijzigingen in de CAB kunnen inbrengen, of zijn zelf (al dan niet op ad hoc basis) lid van de CAB.

Niet alle organisaties richten een formele CAB in: kleinere organisaties waar de beslissingslijnen kort zijn en er minder partijen betrokken zijn, hebben vaak geen baat bij een CAB maar in grotere organisaties met veel wijzigingen kan een CAB een toegevoegde waarde hebben.

Voor een grote wijziging vindt de eindbeslissing vaak plaats op basis van raadpleging van de CAB. In de CAB zitten verschillende partijen, in sommige gevallen neemt een vertegenwoordiger voor de informatiebeveiliging (bvb CISO) of beveiliging van persoonsgegevens (bvb DPO) plaats. Het is echter niet de bedoeling deze voor iedere wijziging in te schakelen. Beveiliging dient immers zoveel mogelijk een geïntegreerd onderdeel te zijn van de normale taken. De wijzigingsbeheerder moet in staat zijn te beoordelen of hij, of de CAB, de input van de vertegenwoordiger voor informatiebeveiliging/ beveiliging persoonsgegevens nodig heeft.

Wanneer het gaat over noodwijzigingen is het mogelijk dat de volledige CAB niet kan deelnemen. Een nood-CAB moet dan oordelen. In geval van noodwijzigingen met onvoldoende autorisatie moet dit steeds gedocumenteerd én achteraf geverifieerd worden.

Goedkeuring van wijzigingsaanvragen

Een wijzigingsaanvraag moet steeds goedgekeurd worden, maar de mate van goedkeuring (wie erbij betrokken moet zijn) hangt af van de wijziging en van de betrokken informatie verwerkende componenten.

Voor de Vlaamse Overheid onderscheiden we 2 soorten goedkeuring:

- **Goedkeuring door de toepassingseigenaar**: deze bepaalt zelf wie er binnen de eigen organisatie goedkeuringsbevoegdheid heeft en hoeveel autorisaties nodig zijn om een wijzigingsaanvraag te kunnen indienen. Deze autorisaties gebeuren dus voor het indienen van de wijzigingsaanvraag. Het gaat hier vooral om de goedkeuring van de functionele wijzigingen, maar het is mogelijk dat ook de technische wijzigingen opduiken.
- **Goedkeuring door de wijzigingsbeheerder (dienstenleverancier)**: afhankelijk van de wijziging en de betrokken informatie verwerkende systemen is één of zijn meerdere autorisaties nodig.

2.3.3. Bepalen van de prioriteit van de wijzigingsaanvraag

Voor wijzigingen geldt dat deze systematisch worden geëvalueerd op impact en dat deze worden geautoriseerd met inachtneming van de impactanalyse. Als de wijzigingsaanvraag is geaccepteerd, wordt de prioriteit en de categorie daarvan aangegeven.

De prioriteit wordt bepaald door de urgentie en de impact:

- **Urgentie**: geeft aan hoe lang het duurt tot het niet uitvoeren van de wijziging een significante impact heeft op de zakelijke processen, dit wordt aangegeven door de aanvrager op de wijzigingsaanvraag.
- **Impact**: de mate waarin een wijziging effect heeft op de zakelijke processen.

Voor de bepaling van urgentie en impact worden dezelfde categorieën als voor incidenten en problemen gehanteerd met een aangepaste definitie voor wijzigingen.

Urgentie

De urgentie wordt als volgt bepaald:

Urgentie	**Omschrijving**
Hoog	• De aanvrager motiveert dat de wijziging dringend moet worden uitgevoerd.
Medium	• De aanvrager motiveert een verhoogde dringendheid van behandeling en aanvaardt dat de wijziging niet dringend zal worden doorgevoerd.
Laag	• Standaard beschouwen we de urgentie als ‘laag’ en kan dit niveau enkel opgetrokken worden mits motivatie. • Gebrek aan motivatie beschouwen we automatisch als een ‘lage’ urgentie.

Impact

Impact	**Omschrijving**

Hoog	• Niet of te laat uitvoeren van de wijziging heeft potentieel ernstige of bedreigende schade of impact op de organisatie en/of; • Wettelijke of regelgevende verplichtingen op korte termijn en/of; • Belangrijke kostenbesparing na invoering van de wijziging en/of; • Beschikbaarheid van kritische zakelijke processen met impact op een groot aantal personen/gebruikers en/of; • Het betreft een wijziging met potentieel ernstige schade voor individuen.
Medium	• Niet of te laat uitvoeren heeft belangrijke schade of impact op de organisatie en/of; • Wettelijke of regelgevende verplichting en/of; • Kostenbesparing na invoering van de wijziging en/of; • Niet-kritische processen maar er is een significante groep personen/gebruikers betrokken en/of; • Het betreft een wijziging met potentieel matige immateriële schade voor individuen.
Laag	• Alle wijzigingen waarbij de impact niet voldoet aan bovenstaande bepalingen.

Prioriteit

De prioriteit wordt bepaald door impact en urgentie:

		Impact		
		Hoog	Medium	Laag
Urgentie	Hoog	**Hoogdringend** (P1)	**Matig dringend** (P2)	**Weinig dringend** (P3)
	Medium	**Matig dringend** (P2)	**Weinig dringend** (P3)	**Niet dringend** (P4)
	Laag	**Weinig dringend** (P3)	**Niet dringend** (P4)	**Niet dringend** (P4)

Waarbij de wijziging moet worden uitgevoerd binnen volgend tijdsbestek (de aangegeven tijden zijn het verschil tussen tijdsstip van aanvraag en van uitvoering):

P1 = hoogdringend	Niet van toepassing: enkel mogelijk voor incidenten en noodwijzigingen.
P2 = matig dringend	Uitvoering binnen 1 week (kalenderdagen)
P3 = weinig dringend	Uitvoering binnen 1 maand (30 kalenderdagen)
P4 = niet dringend	Uitvoering binnen 3 maanden (90 kalenderdagen)

De hoogste prioriteit voor wijzigingen is alleen van toepassing voor P1 incidenten en noodwijzigingen.

2.3.4. Planning van de wijziging

Zodra de wijziging is goedgekeurd kan zij ingepland worden. Afhankelijk van de prioriteit van de wijziging, de identificatie en toewijzing van de taken aan de noodzakelijke uitvoerders en de complexiteit van de wijziging, wordt de wijziging op de planning gezet.

De planning van de wijziging wordt door wijzigingsbeheer opgezet in een wijzigingskalender of wijzigingsplan. Het wijzigingsplan bevat details van alle goedgekeurde wijzigingen en hun planning. Leden van de CAB adviseren over de planning van een wijziging, want er moet rekening worden gehouden met de beschikbaarheid van het personeel, de middelen, de te maken kosten en de zakelijke omgeving.

De CAB kan, in overleg met de betrokken partijen, vaste periode instellen voor het doorvoeren van wijzigingen op momenten dat de dienstverlening daar geen, of zo min mogelijk, last van heeft. Geschikte momenten kunnen bijvoorbeeld worden gevonden in de weekenden of buiten de normale werktijden (kantooruren). Ook kunnen periodes worden vastgesteld waarin juist weinig of geen wijzigen worden gepland, zoals binnen de kantooruren of rond de jaarwisseling.

2.3.5. Uitvoering van de wijziging

Een wijziging moet uitgewerkt worden, getest en kan dan pas in productie genomen worden. Het is mogelijk dat een ontwikkelingstraject moet worden opgestart. Alle stappen – van ontwikkeling over test/acceptatie tot in productie stelling – zijn onderling gescheiden en kennen verschillende GO/NO GO momenten. De verschillende stappen moeten dus expliciet vrijgegeven worden om te vermijden dat ontwerpfouten in productie terecht komen.

Goedgekeurde wijzigingen worden doorgegeven aan de betrokken specialisten voor de ontwikkeling en samenstelling van de wijzigingen.

Bij het inschatten van de benodigde middelen van de wijziging moet men rekening houden met de volgende aspecten:

- Capaciteit en performantie van de betrokken dienst(en);
- Betrouwbaarheid, veerkracht en herstelbaarheid;
- Fall back-plannen;
- Beveiliging;
- De impact van de wijziging op andere diensten;
- De gewenste doorlooptijd van de wijziging;
- De benodigde middelen en de kosten, niet alleen voor de uitvoering van de wijziging maar ook voor support en onderhoud van de benodigde specialisten;
- Eventuele conflicten met andere wijzigingen.

Op noodwijzigingen, die niet volledig volgens de reguliere procedure kunnen worden afgehandeld, is een bijzondere procedure van toepassing die vereist dat overgeslagen controlestappen achteraf worden doorlopen.

Voordat wijzigingen kunnen worden doorgevoerd, moeten de wijzigingen eerst worden getest. Ter ondersteuning van wijzigingen dient afdoende aandacht te worden besteed aan communicatie.

Ontwikkeling

Niet alle wijzigingen hebben een expliciete ontwikkelfase. Zo worden eenvoudige wijzigingen (bijvoorbeeld het wijzigen van een parameter) ingepland en uitgevoerd.

Het ontwikkelen kan inhouden dat er een nieuwe softwareversie komt, met nieuwe documentatie, handleidingen, installatieprocedures, inclusief een *fall back* plan en aanpassingen op de hardware. De wijzigingsbeheerder vervult hierbij een coördinerende rol.

Als onderdeel van de oplevering van een wijziging moet ook een *fall back*-procedure worden geschreven, om de situatie terug te kunnen draaien als de wijziging niet het gewenste resultaat oplevert. Hierin dient te worden beschreven onder welke voorwaarden tot een *fall back* wordt overgegaan en wie daartoe kan besluiten. Wijzigingsbeheer mag de wijziging niet goedkeuren als er geen *fall back*-procedure is.

Als de wijziging impact heeft op de gebruikersomgeving, dan zal er ook een communicatieplan moeten worden geschreven. Verder wordt in de ontwikkelfase een implementatieplan opgesteld en bekende fouten van te implementeren wijzigingen worden geregistreerd.

Validatie

Zowel de wijziging als de *fall back*-procedure en de invoermethode van de wijziging dienen grondig te worden getest. Afwijkingen van dit principe worden vooraf formeel goedgekeurd, eventueel achteraf in het geval van noodwijzigingen. De evaluatie op doeltreffendheid van wijzigingen is functioneel gescheiden van de uitvoering van wijzigingen.

Als het een wijziging betreft met impact op de informatiebeveiliging, wordt in overleg met de beveiligingsbeheerder bepaald of er specifieke informatiebeveiligingstesten uitgevoerd moeten worden (penetratietesten, code reviews et cetera). Waar nodig wordt apparatuur en programmatuur gecontroleerd op compatibiliteit met andere systeemcomponenten.

Testen worden uitgevoerd door de ontwikkelaars, degenen die de wijzigingsaanvraag hebben ingediend of vertegenwoordigers daarvan en beheerders van de betrokken informatie verwerkende systemen. Er dient een scheiding te zijn tussen de omgeving waar ontwikkeld is, de omgeving waar getest wordt en de operationele omgeving. Er moeten testen worden uitgevoerd door een partij die niet de ontwikkelaar is.

Acceptatietesten worden uitgevoerd door zowel gebruikers (gebruiksacceptatie) als de beheerders (productie-acceptatietest). De acceptatietest maakt deel uit van het geheel aan testen die in het kader van de wijziging plaatsvinden. Ook zijn duidelijke voorschriften nodig voor het toezicht houden op de kwaliteit van het testen en van de documentatie van de testresultaten.

Post validatie zorgt ervoor dat na de implementatie van de wijziging geverifieerd wordt dat het resultaat van de wijziging het verwacht is en dat er geen negatieve of ongewenste effecten zijn opgetreden na de wijziging. Daarbij wordt gelet op de volgende zaken:

- Heeft de wijziging het beoogde doel bereikt?
- Zijn de gebruikers tevreden met het resultaat?
- Zijn er nevenverschijnselen opgetreden?
- Zijn de geraamde kosten en inspanningen niet overschreden?

Implementeren

Iedereen die vanuit de betrokken afdeling het beheer van de ICT-infrastructuur of ICT-dienstverlening onder zijn verantwoording heeft, kan worden belast met het implementeren van een wijziging.

Wijzigingsbeheer ziet erop toe dat de wijziging op schema ligt. Er moet een duidelijk communicatieplan liggen waarin staat wie van de wijziging op de hoogte gebracht moeten worden gesteld. Bijvoorbeeld: gebruikers, netwerk-, systeembeheer, et cetera.

De wijzigingslog

Het is belangrijk om de historiek van de wijzigingen bij te houden in een wijzigingslog of 'change log'. Deze log laat toe om na te gaan welke wijzigingen wanneer werden uitgevoerd en door wie. De log bevat informatie over:

- De configuratie-items betrokken bij de wijziging;
- Beschrijving van de doelststelling van de wijziging;
- Verwijzing naar de configuratie en/of release documenten;
- De goedkeuringen voor de wijziging: tijdsstip (datum en tijd) van aanvraag en goedkeuring, de aanvrager(s) en geconsulteerde partij(en), de persoon of personen die de validatie en/of goedkeuring hebben gegeven;
- De operationele afspraken;
- Informatie over de uitvoering van de wijziging: tijdsstip (datum en tijd), uitvoerder.

2.3.6. Evaluatie en afsluiting van de wijziging

Doorgevoerde wijzigingen worden na implementatie geëvalueerd in een *lessons learned*, waarbij in elk geval vastgesteld wordt of de wijziging niet tot incidenten heeft geleid en of de juiste classificatie is toegepast. Daarna wordt desgewenst in de CAB besproken of nog verdere nazorg nodig is.

Is de wijziging een succes en zijn alle activiteiten en registraties voor de wijziging gecontroleerd op afronding, dan kan de wijzigingsaanvraag worden afgesloten. Is de wijziging geen succes, dan wordt de procesgang hervat op de plaats waar het misgegaan is, met een aangepaste werkwijze.

Een wijziging mag niet worden afgesloten vooraleer alle bijhorende documentatie is opgeleverd; uitzonderingen op deze regel moeten goedgekeurd worden door de CAB.

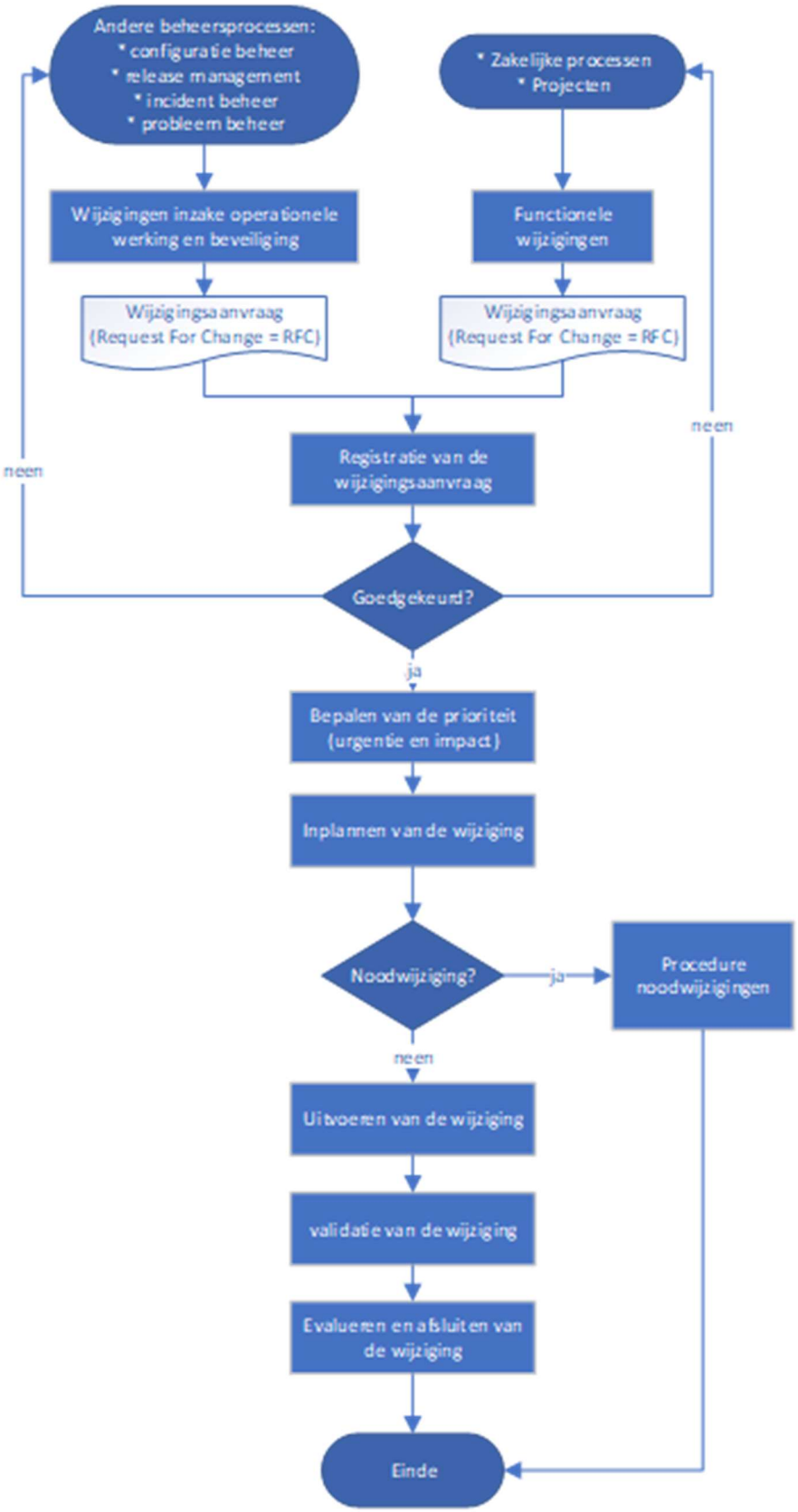
2.3.7. Noodwijzigingen

De noodprocedure is bestemd voor wijzigingsaanvragen die een probleem met belangrijke impact en die acuut de voortgang van een proces belemmert, oplossen. Bij de noodprocedure wordt de levenscyclus van een wijzigingsaanvraag doorbroken. Volgende afwijkingen zijn mogelijk voor de verschillende afhandelingsprocedures:

- Wijzigingsbeheer registreert en beoordeelt het voorstel met voorrang vóór de standaardwerkzaamheden.
- Wijzigingsbeheer meldt het wijzigingsvoorstel ter voorbereidende besluitvorming aan bij de verantwoordelijke met betrekking tot de wijziging (bijvoorbeeld de projectleider). De verantwoordelijke neemt een voorlopig besluit ter voorbereiding van de besluitvorming in de CAB en roept zo snel mogelijk de CAB bijeen.
- Indien niet alle leden van de CAB bereikbaar zijn, zal een beperkte CAB gevormd worden.
- De CAB komt op verzoek van de verantwoordelijke bijeen en beslist onmiddellijk over het voorstel. De verantwoordelijke stelt samen met de eindverantwoordelijken voor de uitvoering de planning vast.

2.3.8. Het proces wijzigingsbeheer

Alle bouwstenen samen maken deel uit van het proces voor het beheer van wijzigingen. Algemeen ziet dat er als volgt uit:



3. LINK MET ANDERE MAATREGELEN

Beheer van wijzigingen is geen alleenstaand proces maar heeft interacties met de andere beheersprocessen:

〉 **Probleembeheer** (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen – probleem beheer*')

Wijziging als oplossing van een probleem

〉 **Incident beheer** (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen – incident beheer*')

Informatie over geplande wijzigingen en hun status	=>	
	<=	• Oplossen van incidenten door uitgevoerde wijzigingen; • Informatie over wijzigingen die incidenten veroorzaken

〉 **Configuratie beheer** (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen - asset en configuratiebeheer*')

• Informatie vanuit wijzigingen voor bijwerken van de CMS; • Koppeling van wijzigingen aan betrokken configuratie-items	=>	
	<=	Informatie over en relatie tussen configuratie-items, voor impact analyse van wijzigingen

〉 **Release en deployment beheer** (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen - release en deployment*')

	<=	• Uitrol van nieuwe versies onder controle van wijzigingsbeheer; • Uitvoerende taken van release management.

〉 **Continuiteitsbeheer** (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen - incident beheer*')

	<=	Bewaking van herstelplannen

4. PRESTATIE-INDICATOREN (KPI'S)

Om de efficiëntie en effectiviteit van een proces te kwalificeren en waar nodig bij te sturen wordt een proces gemeten aan de hand van prestatie-indicatoren. De belangrijkste indicatoren worden KPI's of *Key Performance Indicatoren* genoemd. Per KPI wordt een norm afgesproken en de rapportering gebeurt per periode, bvb maandelijks of halfjaarlijks.

KPI's worden ook gebruikt om bij outsourcing en externe dienstverlening de kwaliteit van het uitbestede proces op te volgen. Deze KPI's worden dan ook vaak opgenomen in de SLA.

Voorbeelden van KPI's voor het proces wijzigingsbeheer zijn:

- Het aantal wijzigingen dat per tijdseenheid wordt doorgevoerd, verdeeld over de verschillende categorieën.
- Het aantal of het percentage afgewezen wijzigingen, verdeeld over de verschillende categorieën.
- Het aantal of het percentage van wijzigingen dat per periode wordt gesignaleerd zonder registratie en autorisatie.
- Het aantal of het percentage (beveiligings)incidenten per impactcategorie dat uit wijzigingen voortkomt.
- Het aantal of het percentage verstoringen dat uit wijzigingen voorkomt.
- Het aantal of het percentage fall backs dat in wijzigingen aan de orde was.
- Het aantal of het percentage wijzigingen dat binnen de geplande doorlooptijd, resources en het budget is uitgevoerd.
- Het gerealiseerde budget of het aantal bestede uren aan wijzigingen per periode.
- Kosten van uitgevoerde wijzigingen.

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.

De doelgroep voor de rapportering bepaalt tevens het type KPI: zo zal de CISO belang stellen in andere prestatie-indicatoren dan bvb de directie.