Informatieclassificatie Vlaamse overheid (Vo-ICR)

Beheer serviceaanvragen voor toegang

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

Classificatie: Klasse 2

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 toegangsbeheer. 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 september 2019	Kristel VAN AKEN	Draft
v.0.2	09 oktober 2019	Kristel VAN AKEN	Feedback pre-taakgroep
v.0.3	07 november 2019	Kristel VAN AKEN	Feedback taakgroep werkgroep informatieveiligheid
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	29 oktober 2020	Beau JANSSEN	Toevoeging kwaliteitskenmerk Integriteit
v.1.3	10 augustus 2021	Beau JANSSEN	Toevoeging kwaliteitskenmerk Beschikbaarheid
v.2.0	21 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 – beheer aanvragen*
  - *Vo Informatieclassificatie - Minimale maatregelen – IAM*
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS)

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

Inhoudsopgave

INLEIDING

De 3 processen voor beheren van toegang

Het verlenen van toegang tot systemen en informatie is een complexe samenwerking van de volgende processen:

- Het proces **beheer serviceaanvragen voor toegang** zorgt ervoor dat de aanvraag tot toegang behandeld wordt en gebruikers toegang krijgen tot de systemen en informatie die ze nodig hebben om hun taken te kunnen uitvoeren. Het is een specifieke toepassing van het proces 'beheer van serviceaanvragen'. Het proces zorgt voor beheer van gebruikers en gebruikersrechten: gebruikers toevoegen of verwijderen, gebruikersrechten toekennen of verwijderen, …
- Het proces **toegangscontrole** verzorgt de technische aspecten nodig voor het verlenen van toegang door de nodige authenticatie middelen te voorzien, rechten te definiëren en te koppelen aan de opbouw van rollen. Het is een specifieke toepassing van het proces 'asset en configuratie beheer'. Toegangscontrole zorgt dus voor een betrouwbare, traceerbare en beveiligde toegang tot ICT-diensten en informatie.
- **Provisioning** verbindt beheer serviceaanvragen voor toegang en toegangscontrole: op basis van de identificatie van de gebruiker en zijn/haar functie binnen de organisatie wordt een account aangemaakt en de nodige autorisaties verleend via rol(len) (service beheer van toegang); om dit mogelijk te maken, moeten authenticatiemechanismen geïmplementeerd zijn, rechten toegekend aan rollen (*role based access control*) en onderhouden (toegangscontrole).

Dit document behandelt het proces beheer service aanvragen voor toegang.

Het proces beheer serviceaanvragen voor toegang

Het proces beheer serviceaanvragen voor toegang verleent geautoriseerde gebruikers het recht om een ICT-dienst of informatie te gebruiken, maar ontzegt niet-geautoriseerde gebruikers de toegang op basis van het toegangsbeleid. Toegang verwijst naar het niveau en de omvang van de functionaliteit van een ICT-dienst of van informatie die een persoon mag gebruiken. Om dit te bereiken, wordt allereerst de identiteit van een persoon nagegaan, waarna hem of haar bepaalde rollen worden toegekend die op hun beurt de nodige rechten voorzien. Deze rechten verwijzen naar de feitelijke technische instellingen voor een persoon.

In het algemeen kan toegang tot een ICT-dienst of informatie verleend worden aan:

- Een gebruiker,
- Een informatiebeheerder,
- Een andere ICT-dienst (toepassing, systeem, …).

In de context van beheer serviceaanvragen voor toegang beperken we ons tot het beheren van toegang van gebruikers. Voor beheer van toegang voor informatiebeheerders – personen met geprivilegieerde rechten – wordt verwezen naar het document '*Vo – Informatieclassificatie – minimale maatregelen – PAM*'.

Het proces beheer serviceaanvragen voor toegang moet in lijn zijn met het toegangsbeleid, maar stelt dit beleid niet zelf op. Er moet een door het management goedgekeurd toegangsbeleid voorhanden zijn dat aangeeft hoe logische toegang moet worden geregeld, rekening houdend met volgende aspecten:

- Wie mag toegang hebben? Hoe wordt de identiteit van de gebruikers geverifieerd? Wanneer wordt gebruikerstoegang verwijderd?
- Welke rollen worden toegekend aan wie? Op welke voorwaarden? Wanneer worden rollen verwijderd?

Het toegangsbeleid moet op zijn beurt conform zijn met de minimale maatregelen opgesteld voor IAM (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen – IAM'*)

De doelstellingen van het proces beheer van serviceaanvragen voor toegang zijn:

- Bewaken van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie d.m.v. het **bewaken van de toegangsmodaliteiten**.
- **Functiescheiding**: het beheer van toegang moet zo ingericht zijn dat er afzonderlijke functies nodig zijn voor aanvragen, toekennen, wijzigen, intrekken/verwijderen en controleren.
- **Minimale rechten** (*least privileges*): het geven van toegang met de minste rechten opdat de gebruiker zijn/haar benodigde functionaliteiten kan gebruiken.

1. MINIMALE MAATREGELEN

Het beheren van servic aanvragen voor toegang 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 beheer serviceaanvragen voor toegang*'):

- Registratie van een aanvraag tot toegang;
- Validatie van de aanvraag;
- Urgentie bepalen;
- Aanvraag uitvoeren;
- Validatie uitvoering en afsluiten.

De minimale beschikbaarheid van het proces 'beheer serviceaanvragen voor toegang' is kantooruren (10ux5dagen).

Een belangrijk aspect van de verificatie is de controle van de identiteit van de gebruiker: hoe dit ingeregeld is voor de verschillende informatieklassen is beschreven in het document 'Vo Informatieclassificatie - Minimale maatregelen' – IAM'.

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

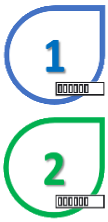
IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Enkelvoudige validatie conform toegangsbeleid en 'Vo Informatieclassificatie - Minimale maatregelen' – IAM'; 〉 Automatische goedkeuring van toegang vooraf goedgekeurd door CISO in samenwerking met de toepassingseigenaar; 〉 Aanmaken van een account, verwijderen van een account, wijzigen van een account.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Registratie van een aanvraag tot toegang; 〉 Urgentie bepalen; 〉 Rollen toekennen, rollen wijzigen, rollen verwijderen; 〉 Minimaal jaarlijkse algemene postvalidatie; 〉 Informeren van de gebruiker en de validator na uitvoering van de aanvraag.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Dubbele validatie conform toegangsbeleid en 'Vo Informatieclassificatie - Minimale maatregelen' – IAM'.

	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Automatische goedkeuring van toegang vooraf goedgekeurd door DPO/CISO in samenwerking met de toepassingseigenaar met rapportering aan DPO/CISO en toepassingseigenaar; 〉 Informeren van alle actoren en de leidend ambtenaar na de uitvoering van de aanvraag.

Integriteit

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Enkelvoudige validatie conform toegangsbeleid en 'Vo Informatieclassificatie - Minimale maatregelen' – IAM'; 〉 Automatische goedkeuring van toegang vooraf goedgekeurd door CISO in samenwerking met de toepassingseigenaar; 〉 Aanmaken van een account, verwijderen van een account, wijzigen van een account.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Registratie van een aanvraag tot toegang; 〉 Urgentie bepalen; 〉 Rollen toekennen, rollen wijzigen, rollen verwijderen; 〉 Minimaal jaarlijkse algemene postvalidatie; 〉 Informeren van de gebruiker en de validator na uitvoering van de aanvraag.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Dubbele validatie conform toegangsbeleid en 'Vo Informatieclassificatie - Minimale maatregelen' – IAM'.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Automatische goedkeuring van toegang vooraf goedgekeurd door DPO/CISO in samenwerking met de toepassingseigenaar met rapportering aan DPO/CISO en toepassingseigenaar; 〉 Informeren van alle actoren en de leidend ambtenaar na de uitvoering van de aanvraag.

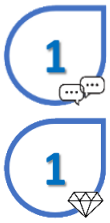
Beschikbaarheid

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

1.2 Minimale specifieke (GDPR) maatregelen

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

Vertrouwelijkheid en integriteit

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1.
	GDPR specifieke maatregelen voor Klasse 2: 〉 Automatische goedkeuring van toegang vooraf goedgekeurd door DPO/CISO in samenwerking met de toepassingseigenaar.

	Klasse 3 en Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 2 + 〉 Automatische goedkeuring van toegang vooraf goedgekeurd door DPO/CISO in samenwerking met de toepassingseigenaar met rapportering aan DPO/CISO en toepassingseigenaar.
	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

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen toegepast worden in het kader van beheer serviceaanvragen voor toegang:

Beschikbaarheid, Integriteit & Vertrouwelijkheid

IC klasse	Minimale maatregelen

Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen:

〉 Iedere organisatie die gebruik wenst te maken van de diensten en toepassingen van het portaal van de sociale zekerheid ten behoeve van zijn gebruikers moet:

- a. minstens één toegangsbeheerder aanstellen (Ref. KSZ 5.6.1);
- b. zijn medewerkers aanzetten tot het lezen en toepassen van de reglementen over het gebruik van de informatiesystemen van de portalen (Ref. KSZ 5.6.1);
- c. de verplichtingen naleven die gepaard gaan met het uitoefenen van de functie beheerder of medebeheerder en die beschreven zijn in de beleidslijn 'veilig toegangsbeheer van portalen' (Ref. KSZ 5.6.1).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Beheer serviceaanvragen voor toegang 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.

Het proces beheer serviceaanvragen voor toegang laat toe om toegang tot diensten en informatie gecontroleerd toe te staan, zodat niet-geautoriseerde toegang wordt vermeden. Beheer van serviceaanvragen voor toegang is dus een proactief proces.

Beheer serviceaanvragen voor toegang is een preventieve maatregel.

2.1.2. Service beheer van toegang

Beheer van toegang tot ICT-diensten en informatie zorgt ervoor dat vertrouwelijkheid, integriteit en beschikbaarheid van ICT-diensten en informatie mogelijk wordt. Het zorgt ervoor dat gebruikers in de mogelijkheid verkeren om een ICT-dienst te gebruiken of informatie te beheren die ze nodig hebben om hun taken te kunnen uitvoeren, maar het verzekert niet noodzakelijk dat deze ICT-dienst of informatie te allen tijde beschikbaar is (hiervoor dient het proces 'beheer van beschikbaarheden' of *availability management*).

Servicebeheer van toegang is nauw verbonden met het proces 'beheer van serviceaanvragen' en houdt volgende activiteiten in (zie hoofdstuk '*De bouwstenen van beheer serviceaanvragen voor toegang*'):

- Aanmaak, indienen en registratie van de aanvraag tot toegang,
- Validatie van de aanvraag,
- Urgentie bepalen,
- Aanvraag uitvoeren,

〉 Validatie uitvoering en afsluiten.

2.2. Succesfactoren voor een goed beheer serviceaanvragen voor toegang

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 beheer serviceaanvragen voor toegang omvatten:

〉 Gecontroleerde toegang tot informatie waarbij gelet wordt op de toegankelijkheid voor geautoriseerde gebruikers;
〉 Gebruikers hebben het juiste niveau van toegang om hun taken te kunnen uitvoeren;
〉 De mogelijkheid om toegang tot informatie te auditen en misbruik van toegangsrechten op te sporen;
〉 De mogelijkheid om snel en efficiënt toegang te blokkeren waar nodig door het intrekken van rechten of het blokkeren van gebruikersaccounts.

2.3. De bouwstenen van beheer serviceaanvragen voor toegang

2.3.1. Het toegangsbeleid

Hoewel het opstellen van het toegangsbeleid geen onderdeel is van het proces beheer serviceaanvragen voor toegang, is het wel een belangrijke pijler ervan.

Doelstelling van het beleid voor logische toegangsbeveiliging is het vaststellen van de identiteit van een gebruiker die toegang krijgt tot informatie, informatiesystemen of ICT-diensten, vaststellen welke functionaliteiten de gebruiker mag verkrijgen en het waarborgen van een gecontroleerde toegang (autoriseren) tot, en gebruik van, informatie, informatiesystemen of ICT-diensten. Hierbij moet je de afweging maken welke invloed deze toegang kan hebben op de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie.

De identiteit van een gebruiker kan worden vastgesteld via verschillende methodes gaande van zwakke identificatie tot sterke identificatie. Zodra een identiteit is vastgesteld, kan worden overgegaan tot authenticatie, waarbij de gebruiker zijn/haar identiteit bewijst. Ook hiervoor zijn verschillende methodes voorhanden van geen of zwakke authenticatie tot sterke authenticatie. Daarnaast is controle op gebruik van de account een belangrijke maatregel: het bijhouden van de nodige audit trails met het oog op traceerbaarheid.

Welke methodes wanneer moeten worden toegepast in functie van de informatieklassen is besproken in het document 'Vo Informatieclassificatie – Minimale maatregelen – IAM'. Het toegangsbeleid moet conform deze IAM minimale maatregelen uitgewerkt worden door de organisatie.

2.3.2. De aanvraag tot toegang

Een aanvraag tot toegang kan ingediend worden aan de helpdesk, servicedesk of een ander meldpunt dat de organisatie heeft aangeduid, of via een *self service* toepassing voor het verwerken van toegangsvragen van gebruikers. Een aanvraag tot toegang is onderdeel van het proces 'beheer van serviceaanvragen' en is besproken in document 'Vo Informatieclassificatie – Minimale maatregelen – beheer aanvragen'.

Er kan toegang gevraagd worden tot toepassingen, maar ook tot netwerken en andere ICT-componenten waar gebruikers taken op moeten kunnen uitvoeren.

De aanvraag kan worden geïnitieerd door de gebruiker of zijn leidinggevende, door de toepassingseigenaar of CISO/DPO en bevat minstens volgende informatie:

- Aanvrager,
- Gebruiker/begunstigde,
- Gewenste ingangsdatum,
- Eventuele einddatum (bij tijdelijke toegang),
- Gewenste bevoegdheden,
- Motivatie van de toegang.

Elke toegang tot informatie of systemen moet gemotiveerd zijn door de gebruiker of zijn/haar leidinggevende. De toepassingseigenaar, CISO/DPO of uitvoerder mogen geen aanvraag tot toegang voor gebruikers motiveren.

2.3.3. Validatie van de aanvraag

De beoordeling van de aanvraag tot toegang houdt in dat gecontroleerd wordt of de aanvraag volgende elementen bevat:

- Is de gebruiker die om toegang vraagt inderdaad de persoon die hij/zij claimt te zijn?
- Is de gebruiker gelegitimeerd om de service of informatie waarvoor hij/zij toegang vraagt, te gebruiken?

De aanvraag kan niet gevalideerd worden door de initiator van de vraag.

Het toegangsbeleid en het document 'Vo Informatieclassificatie – minimale maatregelen – IAM' levert de leidraad voor de beoordeling van de aanvraag: elke aanvraag moet hiermee conform zijn.

Indien de aanvraag beantwoordt aan de vereisten opgelegd door de toepassingseigenaar en in lijn is met het toegangsbeleid, kan toegang tot de betrokken dienst of informatie verleend worden aan de gebruiker.

2.3.4. Urgentie bepalen

Het bepalen van de prioriteit gebeurt enkel op basis van urgentie is beschreven in het document 'Vo Informatieclassificatie – Minimale maatregelen – beheer aanvragen'.

2.3.5. Aanvraag uitvoeren

Beheer serviceaanvragen voor toegang beslist niet wie toegang heeft tot welke dienst of informatie, maar voert slechts het beleid uit. Op deze manier zal beheer serviceaanvragen voor toegang de toegang tot diensten en informatie afdwingen, maar het neemt niet de beslissing over wie toegang mag hebben. De uitvoering gebeurt onder delegatie van de toepassingseigenaar.

Taken van gebruikers kunnen door de tijd veranderen, bijvoorbeeld wanneer ze van functie veranderen of het bedrijf verlaten. Het beheer van toegang houdt dus niet alleen in dat toegang wordt toegekend, maar ook wordt verwijderd of aangepast. Dit is echter niet een beslissing die een gebruiker zelf mag nemen.

Het geven van toegang omvat volgende taken:

- Aanmaken, wijzigen of verwijderen van een account voor de gebruiker,
- Toekennen, wijzigen of verwijderen van rollen.

2.3.6. Monitoren van toegang

Toegangen moeten niet alleen toegekend of verwijderd worden, maar er moet voor worden gezorgd dat de verleende toegang ook goed wordt gebruikt. Daarom moet toegangsbewaking en -beheersing worden opgenomen in de monitoringactiviteiten van alle technische en applicatiebeheerfuncties en alle service productieprocessen. Dit maakt echter geen deel uit van het proces beheer serviceaanvragen voor toegang zelf.

Aspecten waar mee rekening moet worden gehouden:

- Accounts van gebruikers die niet meer werkzaam zijn in de organisatie, moeten verwijderd zijn. Accounts die tijdelijk geblokkeerd zijn, moeten na verloop van tijd definitief verwijderd worden als ze niet meer nodig zijn – in lijn met toegangsbeleid.
- Rechten moeten toegekend zijn in functie van de taken en verantwoordelijkheden van de gebruiker op elk moment, cumulatie van rechten na verloop van tijd moet vermeden worden.
- Opletten voor conflicten in toekennen van rechten (bvb onvoldoende aandacht schenken aan scheiding van functies).
- Periodiek nazicht van toegekende accounts en rechten.
- Controle op het gebruik van rechten (auditeerbaarheid).

2.3.7. Validatie uitvoering en afsluiten aanvraag

Controle na de uitvoering zorgt ervoor dat de juiste accounts en rollen werden toegekend. Dit kan gebeuren door periodieke validatie (bijvoorbeeld jaarlijks). De uitvoering mag niet gevalideerd worden door de gebruiker zelf of zijn leidinggevende.

Een aanvraag voor toegang moet afgesloten worden en – afhankelijk van de informatieklasse – gecommuniceerd naar de gebruiker en/of validator.

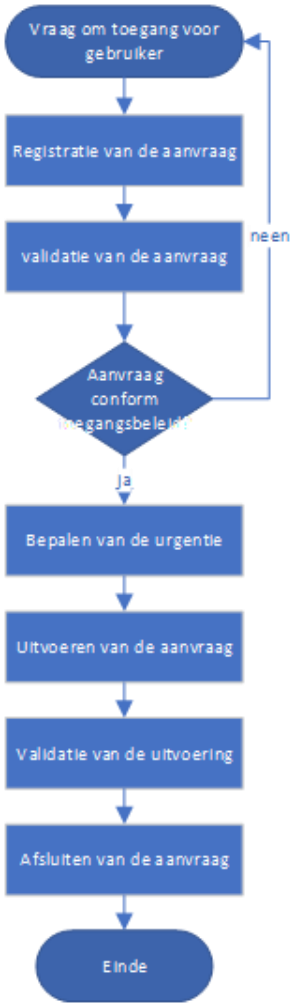
2.3.8. Samenvattend overzicht activiteiten

Volgende tabel geeft een overzicht over de activiteiten en hun mogelijke actoren:

	Gebruiker	N+1	Toep.eigenaar	CISO/DPO	Uitvoerder
Motivatie	V	V	X	X	X
Initiatie	V	V	V	V	X
Validatie	X	Excl initiator	excl. initiator	Exl initiator	Afh. van klasse
Uitvoering	X	X	Excl. initiator	X	V
Hervalidatie	X	X	V	V	Afh. van klasse

2.3.9. Het proces

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



3. LINK MET ANDERE MAATREGELEN

Beheer van serviceaanvragen voor toegang is geen alleenstaand proces maar heeft interacties met de andere beheersprocessen:

- **Beheer van serviceaanvragen**

Er is een link met **beheer van serviceaanvragen**: een vraag voor toegang wordt ingediend via een serviceaanvraag en dus via het proces beheer van serviceaanvragen (voor meer informatie zie document: ‘’).

- **Wijzigingsbeheer** (voor meer informatie zie document: 'Vo Informatieclassificatie – Minimale maatregelen – wijzigingsbeheer')

Soms worden toegangen aangevraagd via het proces **wijzigingsbeheer**, voornamelijk indien het gaat om groot aantal toegangsvragen, bijvoorbeeld in het geval van een nieuwe toepassing (voor meer informatie zie document ‘Vo Informatieclassificatie - Minimale maatregelen - wijzigingsbeheer’)

- **Veiligheidslogging en monitoring**

Er is een link met **veiligheidslogging en monitoring**: traceerbaarheid van toegang moet worden ingericht in de verschillende bronprocessen waar toegang toe wordt verleend. Zie ‘*Vo Informatieclassificatie - Minimale maatregelen - SIEM*’

- **Identity & Access Management (IAM)**

Het proces beheer serviceaanvragen voor toegang regelt de flow van het toekennen, wijzigen en verwijderen van toegang aan een gebruiker. Er zijn echter verschillende deelaspecten die door I*dentity* & *Access Management* (IAM) ingeregeld worden (voor meer informatie zie document: ‘*Vo Informatieclassificatie – minimale maatregelen – IAM*’):

- **Identificatie** van de gebruiker: zwakke versus sterke identificatie,
- **Authenticatie** van de gebruiker: welke type accounts kan gebruikt worden en hoe moeten accounts beheerd worden,
- **Auditeerbaarheid**: wat is nodig om controle uit te voeren op toekenning en beheer van accounts.

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 KPIs of *Key Performance Indicatoren* genoemd. Per KPI wordt een norm afgesproken en de rapportering gebeurt per periode, bvb maandelijks of halfjaarlijks. Deze KPIs moeten een afspiegeling zijn van de door de organisatie gedefinieerde kritische succesfactoren, en zijn gelinkt aan de verschillende kwaliteitskenmerken: vertrouwelijkheid, integriteit en beschikbaarheid.

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 beheer serviceaanvragen voor toegang zijn:

- Aantal nieuwe accounts dat wordt aangemaakt per periode (per maand, trimester, jaar, …);
- Gemiddelde tijd nodig om nieuwe toegang te verlenen;
- Gemiddelde tijd nodig om toegangsrechten te verwijderen.

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.