Informatieclassificatie Vlaamse overheid (Vo-ICR)

Beheer van problemen (problem management)

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (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 beheer van problemen. 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 3 delen. Eerst worden de minimale maatregelen besproken, alvorens in het tweede deel al de nodigde aanvullende informatie ter beschikking wordt gesteld. Vervolgens bespreken we de link met andere maatregelen.

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

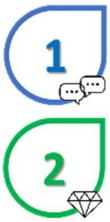
Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

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	22 juli 2019	Kristel VAN AKEN	Draft
v.0.2	29 augustus 2019	Kristel VAN AKEN	Feedback taakgroep verwerkt
v.0.3	12 december 2019	Kristel VAN AKEN	Feedback leespanel en consistentie check
v.1.0	12 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	21 januari 2021	Beau JANSSEN	Toevoeging Integriteit als kwaliteitskenmerk
v.1.3	10 augustus 2021	Beau JANSSEN	Toevoeging Beschikbaarheid als kwaliteitskenmerk
v.2.0	19 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 de 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 - incident 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 proces probleembeheer (*problem management*)

Incidentbeheer en probleembeheer zijn nauw verwante maar toch verschillende processen. Het verhelpen van incidenten mag immers niet beperkt blijven tot symptoombestrijding. Probleembeheer is het proces dat de achterliggende problemen identificeert en hun oorzaken achterhaalt.

Bij het verhelpen van incidenten wordt continu gereageerd op gebeurtenissen in de exploitatie. Bij elk incident dat plaatsvindt moet zo spoedig mogelijk het vereiste niveau hersteld worden. Onder deze omstandigheden is het vaak moeilijk zo niet onmogelijk om de nodige tijd te nemen om tot een goede analyse of beoordeling van de oorzaak te komen.

Om de oorzaak van de incidenten te achterhalen dient de infrastructuur structureel gecontroleerd te worden op fouten. Het achterhalen en wegnemen van fouten in de infrastructuur is het belangrijkste doel van probleembeheer.

Beheren van problemen

Probleembeheer streeft naar een zo hoog mogelijke stabiliteit van de ICT-dienstverlening door het achterhalen en wegnemen van fouten in de infrastructuur, waardoor verstoringen zo goed mogelijk vermeden worden. Op het moment dat zich verstoringen toch voordoen, is het de taak van incidentbeheer om de gevolgen ervan zo veel mogelijk te beperken (voor meer informatie zie document: ‘Vo Informatieclassificatie - Minimale maatregelen - incidentbeheer'). De belangrijkste bijdrage van probleembeheer is het nemen van structurele maatregelen om (herhaling van) verstoringen te voorkomen.

Door de inspanning van de organisatie te verleggen van het reageren op grote aantallen incidenten naar het voorkomen van deze incidenten via probleembeheer, kan doelmatiger gebruik worden gemaakt van de beschikbare kennis in de organisatie. Incidenten die zich op willekeurige momenten voordoen, vergen meer tijd van de organisatie dan het aanbrengen van een structurele wijziging waarmee deze incidenten voorkomen worden. Dit komt vooral tot uiting wanneer zich veel overeenkomstige incidenten voordoen.

Daarnaast kan het gericht zoeken naar structurele verbeteringen van de infrastructuur op een meer planmatige manier plaatsvinden, zodat een grotere controle over de werkzaamheden wordt verkregen. Hoewel in eerste instantie een grotere inspanning vereist is om een probleem aan te pakken dan om een incident te verhelpen, zal na verloop van tijd het aantal incidenten teruglopen als gevolg van een stabieler systeem.

Daar waar de helpdesk of service desk zich voornamelijk richt op het oplossen van incidenten, wordt probleembeheer opgenomen door experten van de tweede- of derdelijnsondersteuning.

1. MINIMALE MAATREGELEN

1.1. Minimale algemene maatregelen

Het beheren van problemen 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 ook hoofdstuk: '*De bouwstenen van probleem beheer*'):

- Identificatie en registratie van het probleem;
- Classificatie;
- Prioriteit toekennen;
- Mensen en middelen alloceren;
- Onderzoek en diagnose;
- Gekende fout documenteren (KED);
- Actie ondernemen;
- Probleem afsluiten.

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

Vertrouwelijkheid

IC klasse	Minimale maatregelen

 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen:
	› Enkel P1 incidenten moeten verplicht doorgegeven worden naar probleembeheer;
	› Registratie van het probleem in een logboek;
	› Classificatie van het probleem – dezelfde classificatie als voor incidenten wordt toegepast;
	› Mensen en middelen alloceren;
	› Onderzoek en diagnose uitvoeren;
	› Gekende fout documenteren (KED) voor P1 problemen;
	› Actie ondernemen:
	  › Geplande wijziging: deze wordt verder opgenomen door wijzigingsbeheer;
	  › Niet-geplande wijziging: deze wordt verder opgenomen door release en deployment beheer;
	  › Indien beslist wordt om geen actie te ondernemen en indien er een rest risico aanwezig is, moet dit rest risico formeel geaccepteerd worden.
	› Probleem afsluiten.

	Alle maatregelen van Klasse 1 / Klasse 2 + › Incidenten vanaf P2 moeten verplicht doorgegeven worden naar probleembeheer; › Registratie van het probleem in een centraal logboek onder beheer van een probleembeheerder; › Gekende fout documenteren (KED) voor problemen vanaf P2;

	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Alle incidenten moeten verplicht doorgegeven worden naar probleembeheer; 〉 Alle gekende fouten documenteren (KED).
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Er moet steeds actie ondernomen worden door middel van een geplande (via wijzigingsbeheer) of niet-geplande (via release en deployment beheer) wijziging.

Integriteit

IC klasse	Minimale maatregelen


 
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen:
	
	〉 Enkel P1 incidenten moeten verplicht doorgegeven worden naar probleembeheer;
	〉 Registratie van het probleem in een logboek;
	〉 Classificatie van het probleem – dezelfde classificatie als voor incidenten wordt toegepast;
	〉 Mensen en middelen alloceren;
	〉 Onderzoek en diagnose uitvoeren;
	〉 Gekende fout documenteren (KED) voor P1 problemen;
	〉 Actie ondernemen:
	  〉 Geplande wijziging: deze wordt verder opgenomen door wijzigingsbeheer;
	  〉 Niet-geplande wijziging: deze wordt verder opgenomen door release en deployment beheer;
	  〉 Indien beslist wordt om geen actie te ondernemen en indien er een rest risico aanwezig is, moet dit rest risico formeel geaccepteerd worden.
	〉 Probleem afsluiten.

	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Incidenten vanaf P2 moeten verplicht doorgegeven worden naar probleembeheer; 〉 Registratie van het probleem in een centraal logboek onder beheer van een probleembeheerder; 〉 Gekende fout documenteren (KED) voor problemen vanaf P2;
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Alle incidenten moeten verplicht doorgegeven worden naar probleembeheer; 〉 Alle gekende fouten documenteren (KED).

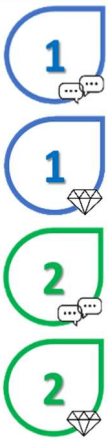
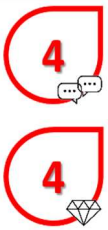
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Er moet steeds actie ondernomen worden door middel van een geplande (via wijzigingsbeheer) of niet-geplande (via release en deployment beheer) wijziging.

Beschikbaarheid

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Beschikbaarheid van het proces probleembeheer 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

Vertrouwelijkheid en integriteit

IC klasse	Minimale maatregelen
	Er zijn geen maatregelen voor klasse 1 en Klasse 2.
	Maatregelen voor Klasse 3: 〉 Alle incidenten moeten verplicht doorgegeven worden naar probleembeheer; 〉 Alle gekende fouten documenteren (KED).
	Maatregelen voor Klasse 4: Alle maatregelen van Klasse 1 / Klasse 2 / Klasse 3 + 〉 Er moet steeds actie ondernomen worden door middel van een geplande (via wijzigingsbeheer) of niet-geplande (via release en deployment beheer) wijziging.
	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 (NIS II) 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 problemen 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 van problemen' laat toe om structurele verbeteringen in te plannen zodat deze op een meer gecontroleerde manier geïmplementeerd worden. Hierdoor worden fouten voorkomen of weggenomen.

Beheer van problemen is een preventieve maatregel.

2.1.2. Wat is een probleem

In feite geldt voor alle incidenten dat hieraan een fout ten grondslag ligt. In sommige gevallen wordt dan een probleem geïdentificeerd. Een probleem kan men beschouwen als een ongewenste situatie, geïdentificeerd uit één of meer incidenten, die indicatief zijn voor een fout in de ICT-infrastructuur. Deze fout, die de oorzaak is van de incidenten, is nog onbekend. Het is van belang dat het probleem onderkend wordt, zodat de gevolgen hiervan beperkt kunnen worden en gericht gezocht wordt naar de fout in de infrastructuur en oplossingen om de fout te herstellen dan wel te voorkomen dat zij zich nogmaals voordoet.

Pas op het moment dat de werkelijke oorzaak van de incidenten gevonden is, is sprake van een gekende fout. Een gekende fout is gedefinieerd als de ongewenste situatie met betrekking tot de ICT-infrastructuur, waarbij een bepaald configuratie-item geïdentificeerd is als de oorzaak van een (potentiële) degradatie van het ICT-dienstenniveau.

Een gekende fout komt in de meeste gevallen voort uit een verstoring. Door het met succes onderzoeken en diagnosticeren van de situatie wordt een verstoring omgezet in een gekende fout. Het betreffende configuratie-item zal door een wijziging hersteld, aangepast of vervangen moeten worden.

Niet alleen als gevolg van incidenten en probleemdiagnose kunnen fouten in de infrastructuur bekend worden. Ook door leveranciers en gebruikersgroepen kan informatie verstrekt worden over foutieve configuratie-items. Voorbeelden hiervan zijn de regelmatige verbeteringen en correcties die leveranciers van hardware en software ter beschikking stellen om geconstateerde fouten te verhelpen. Hetzelfde geldt voor nieuwe of gewijzigde toepassingen die door ontwikkeling opgeleverd worden. Door tijdsdruk of als gevolg van wettelijke bepalingen kan de broncode die tijdens het testen niet geheel foutvrij blijkt, toch in exploitatie worden genomen. Indien deze fouten bekend zijn bij

ontwikkeling dient de informatie hierover tezamen met de toepassing beschikbaar gemaakt te worden aan probleembeheer.

2.1.3. Het verschil met incidenten

Wat is nu het verschil tussen een probleem en een incident?

Incidenten treden op bij het beschikbaar stellen of de exploitatie van de ICT-infrastructuur. Elk incident is het gevolg van een fout in de te beheren infrastructuur. Om die fout te achterhalen wordt een probleem geïdentificeerd.

Eens de oorzaak gevonden, moet de fout hersteld worden. Na een succesvolle wijziging of implementatie is de oorzaak van de incidenten, de fout, weggenomen en zullen deze incidenten, niet meer voorkomen. Pas dan is een structurele oplossing voor de incidenten aangebracht. In tussen tijd moet er natuurlijk voor gezorgd worden dat het incident binnen de gestelde doorlooptijd bepaald door de prioriteit van het incident opgelost wordt. Daarvoor dient de *work around*. Deze tijdelijke oplossing wordt gedocumenteerd in de KED (*known error database*) zodat deze beschikbaar is zou het incident zich nogmaals voordoen. Zodra de oorzaak van een probleem gekend is en de tijdelijke oplossing in de KED gedocumenteerd, is er sprake van een gekende fout en zal een gelijkaardig incident (mocht dit zich voordoen) hersteld kunnen worden met de gekende tijdelijke oplossing tot er een structurele oplossing is geïmplementeerd. Zulk incident, waarvan de oorzaak gevonden is (gekende fout) mag niet meer opnieuw doorstromen naar het proces probleembeheer.

Voor de gebruiker van de ICT-infrastructuur is het van essentieel belang dat incidenten zo spoedig mogelijk worden verholpen. De dienstverlening dient met minimale gevolgen voor de afnemers hersteld te worden.

Voor het kwaliteitsniveau van de dienstverlening is het van belang dat de infrastructuur zodanig is ingericht dat incidenten zoveel mogelijk voorkomen worden. Probleembeheer richt zich dan ook op het aanbrengen van structurele verbeteringen op de infrastructuur.

Een incident kan nooit ‘escaleren’ naar een probleem; een probleem wordt aangemaakt en gelinkt aan één of meer incidenten. In principe zou aan elk incident waarvan de oorzaak onbekend is, een probleem kunnen worden gekoppeld. Om een pragmatische invulling van probleembeheer te geven, wordt dit enkel gedaan voor:

- Herhaalde incidenten,
- Een groep aan elkaar gerelateerde incidenten,
- Een ernstige verstoring die een structurele oplossing vereist.

2.1.4. Wat is beheer van problemen

Daar waar incident beheer zich voornamelijk richt op het oplossen van incidenten, bestaat het doel van probleembeheer uit het wegnemen of voorkomen van fouten in de infrastructuur teneinde een zo hoog mogelijke stabiliteit in de dienstverlening te bereiken. Het probleemafhandelingstraject begint met het identificeren van een probleem en eindigt met het afsluiten van de gekende fout. Om dit proces inhoud te geven worden volgende activiteiten onderscheiden (zie ook hoofdstuk: *'De bouwstenen van probleembeheer'*):

- Probleemidentificatie en registratie;
- Classificatie;
- Prioriteit toekennen;
- Allocatie van mensen en middelen;
- Onderzoek en diagnose;
- Foutbeheer;
- Rapporteren aan management.

2.2. Succesfactoren voor een goed probleembeheer

Een optimaal proces voor beheer van problemen bereikt men als er rekening wordt gehouden met volgende factoren:

- Draag zorg voor de juiste verhoudingen tussen probleembeheer, wijzigingsbeheer, de helpdesk en de ondersteunende afdelingen.
- Voorkom dat probleembeheer ondergeschikt wordt aan ad hoc incidentafhandeling.
- Voorzie de betrokken medewerkers van voldoende hulpmiddelen om het onderzoek en de diagnose juist uit te voeren.
- Zorg voor overdracht van in de ontwikkelomgeving gekende fouten naar de operationele programmatuur.

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 (KPI's). Voor beheer van problemen zijn diverse KPI's mogelijk (er zijn uiteraard nog meer mogelijkheden, maar het is aan de organisatie om de juiste keuze te maken), voorbeelden zijn:

- Bestede tijd aan onderzoek en diagnose per afdeling of leverancier uitgesplitst naar de verschillende problemen;
- Planning van openstaande problemen met betrekking tot inzet van mensen, middelen en kosten;
- Doorlooptijd van gesloten problemen;
- Aantal incidenten dat doorstroomt naar probleembeheer.

2.3. De bouwstenen van probleembeheer

2.3.1. Probleem identificatie en registratie

Bij het identificeren van problemen wordt uitgegaan van het principe dat aan elk incident een fout ten grondslag ligt. In geval een incident optreedt waarvan de oorzaak (nog) niet bekend is, wordt gesproken van een probleem. Het aantal problemen zal in het algemeen een stuk lager zijn dan het aantal incidenten.

Wanneer een probleem geïdentificeerd wordt, moet ook de registratie van het probleem plaats vinden. Belangrijk is dat de kenmerken, de aan het probleem gerelateerde incidenten en een eventueel beschikbare oplossing worden vastgelegd en gedocumenteerd. Met behulp van deze gegevens kan incidentafhandeling achteraf sneller plaatsvinden.

Probleemregistratie is ook nodig om te voorkomen dat problemen aan de aandacht van de organisatie ontsnappen. Naast de eerdergenoemde informatie dienen daarom ook gegevens vastgelegd te worden ten behoeve van het bewaken van de problemen. Hieronder vallen de status van het probleem, welke expert betrokken is bij de verdere afhandeling van het probleem en welke acties inmiddels uitgevoerd zijn.

Mogelijke statussen van een probleem zijn:

- In behandeling,
- Analyse/diagnose,
- Gekende fout,
- Zoeken oplossing,
- Verzoek tot wijziging ingediend,
- Evaluatie,
- Afsluiten van het probleem.

Met behulp van deze informatie kan voortgangscontrole op de probleemafhandeling plaatsvinden.

2.3.2. Classificatie van een probleem

Wanneer een probleem geïdentificeerd is, dient bepaald te worden of en hoeveel aandacht besteed moet worden aan dit probleem om het foutieve configuratie-item in de infrastructuur te ontdekken en te herstellen. Hiervoor is het noodzakelijk inzicht te hebben in de gevolgen van de fout voor de dienstverlening. Na identificatie van een probleem wordt daarom altijd overgegaan tot classificatie van het probleem.

Hiervoor is het raadzaam hetzelfde classificatieschema te gebruiken als voor incidentbeheer. Dit garandeert consistentie en vergemakkelijkt de uitwisseling van informatie tussen de processen. Zie ook document ‘Vo Informatieclassificatie - Minimale maatregelen - incidentbeheer’.

2.3.3. Prioriteit bepalen

Om de prioriteit van een probleem te bepalen, moet een inschatting gemaakt worden van de urgentie en de impact. Hiervoor worden volgende schalen gebruikt:

Urgentie	**Omschrijving**
Hoog	• Geen controle op oorzaak noch gevolgen • Controle op oorzaak maar niet op gevolgen • Schade veroorzaakt door het incident neemt snel toe • Werk dat moet worden hersteld door medewerkers is zeer arbeidsintensief • Voorkomen dat incident leidt tot een groot incident door snel op te treden
Medium	• Geen controle op oorzaak maar gevolgen zijn onder controle • Schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe • Er gaat werk verloren maar dit is relatief snel te herstellen
Laag	• Oorzaak en gevolgen zijn onder controle • Schade veroorzaakt door het incident neemt in de tijd weinig toe • Het werk dat blijft liggen is niet arbeidsintensief

Impact	**Omschrijving**
Hoog	• Ernstige of bedreigende schade of impact op de organisatie. Deze impact kan verband houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en hun rol in het bedrijfsproces • Lange onderbreking of permanente onbeschikbaarheid van de dienstverlening is mogelijk • Hoge financiële impact • Hoge reputatieschade • Ernstige materiële of lichamelijke schade voor individuen
Medium	• Belangrijke schade of impact op de organisatie. Deze impact kan verband houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en hun rol in het bedrijfsproces • Korte onderbreking van de dienstverlening is mogelijk • Matige financiële impact • Matige reputatieschade • Matige materiële schade voor individuen
Laag	• Geen of minimale schade of impact op de organisatie. Deze impact kan verband houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en hun rol in het bedrijfsproces • Dienstverlening gegarandeerd of slechts kort onderbroken • Geen of beperkte financiële impact • Geen of beperkte reputatieschade • Geen of beperkte materiële schade voor individuen

Dit leidt tot de volgende prioriteitsschalen:

		Impact		
		Hoog	Medium	Laag
Urgentie	Hoog	**Blokkerend** (P1)	**Ernstige storing** (P2)	**Matig storend** (P3)
	Medium	**Ernstige storing** (P2)	**Matig storend** (P3)	**Niet storend** (P4)
	Laag	**Matig storend** (P3)	**Niet storend** (P4)	**Niet storend** (P4)

Voor de afhandeling van een probleem worden volgende oplostijden gehanteerd:

Blokkerend (P1)	48u
Ernstige storing (P2)	1 week (kalenderdagen)
Matig storend (P3)	1 maand (30 kalenderdagen)
Niet storend (P4)	1 maand (30 kalenderdagen)

Zie ook document '[Vo Informatieclassificatie - Minimale maatregelen - incidentbeheer]'. Merk op dat de oplostijden voor problemen aanzienlijk langer zijn dan voor incidenten.

2.3.4. Allocatie van mensen en middelen

Gezien de beperkte beschikbaarheid van mensen en middelen in een organisatie zal vastgelegd moeten worden waar en wanneer deze ingezet worden. Op basis van de classificatie en prioriteit van de problemen is het mogelijk de juiste mensen en middelen in te zetten. Hiervoor dient voldoende inzicht te bestaan in de kennis die in de organisatie aanwezig is.

Voor sommige problemen is het noodzakelijk een beroep te doen op externe expertise. In deze gevallen zal de inhoud van onderhoudscontracten en garantiebepalingen bekend moeten zijn. Voor zowel de interne als de externe medewerkers dient duidelijk te zijn welke verantwoordelijkheden en bevoegdheden zij hebben bij het afhandelen van het probleem.

Vaak wordt een probleembeheerder aangeduid. Naargelang de grootte van de organisatie is dit een aparte functie of – bij kleine organisaties – wordt de functie al dan niet informeel opgenomen door een senior persoon van de organisatie. De probleembeheerder volgt het probleem op, stelt een team van experten samen en doet zo nodig beroep op de leverancier of een andere externe expert.

2.3.5. Onderzoek en diagnose

Onderzoek en diagnose moeten leiden tot het vaststellen van de werkelijke oorzaak van de incidenten. Hierbij is het van belang dat men zich niet beperkt tot de apparatuur, programmatuur en datacommunicatiefaciliteiten. In sommige gevallen zal de fout gevonden worden in procedures, documentatie of menselijk handelen. Om al deze aspecten te kunnen betrekken in het onderzoek is een breed, multidisciplinair team nodig. Het kan bijvoorbeeld noodzakelijk zijn om de afdeling ontwikkeling of de leverancier te betrekken bij het onderzoek en de diagnose.

Voor diagnose van het probleem dienen zowel feitelijke gegevens als historische en diagnostische gegevens verzameld te worden. Feitelijke gegevens kunnen bijvoorbeeld bestaan uit systeemdocumentatie en installatievoorschriften. Op schrift gestelde procedures en interne werkinstructies kunnen in combinatie met systeemdocumentatie en technische specificaties fouten aan het licht brengen. De configuratiebeheer database (CMS) geeft inzicht in de relatie van het betreffende configuratie-item met andere delen van de ICT-infrastructuur.

Historische gegevens zijn van belang om de ontwikkeling van een probleem inzichtelijk te maken. Deze kunnen verzameld worden aan de hand van de incidenten-, probleem- en foutregistratie. Ook informatie met betrekking tot uitgevoerde wijzigingen kan hierbij relevant zijn. Voor diagnose van het probleem kunnen gegevens worden verzameld in de vorm van een geheugendumps, journalen en logboeken. Met speciale daartoe geëigende diagnostische hulpprogrammatuur kunnen de precieze locaties en de omstandigheden opgespoord worden waaronder het incident optreedt. Om diagnose en onderhoud aan toepassingen te vereenvoudigen is het aan te bevelen diagnostische routines in de programmatuur op te nemen.

2.3.6. Foutenbeheer

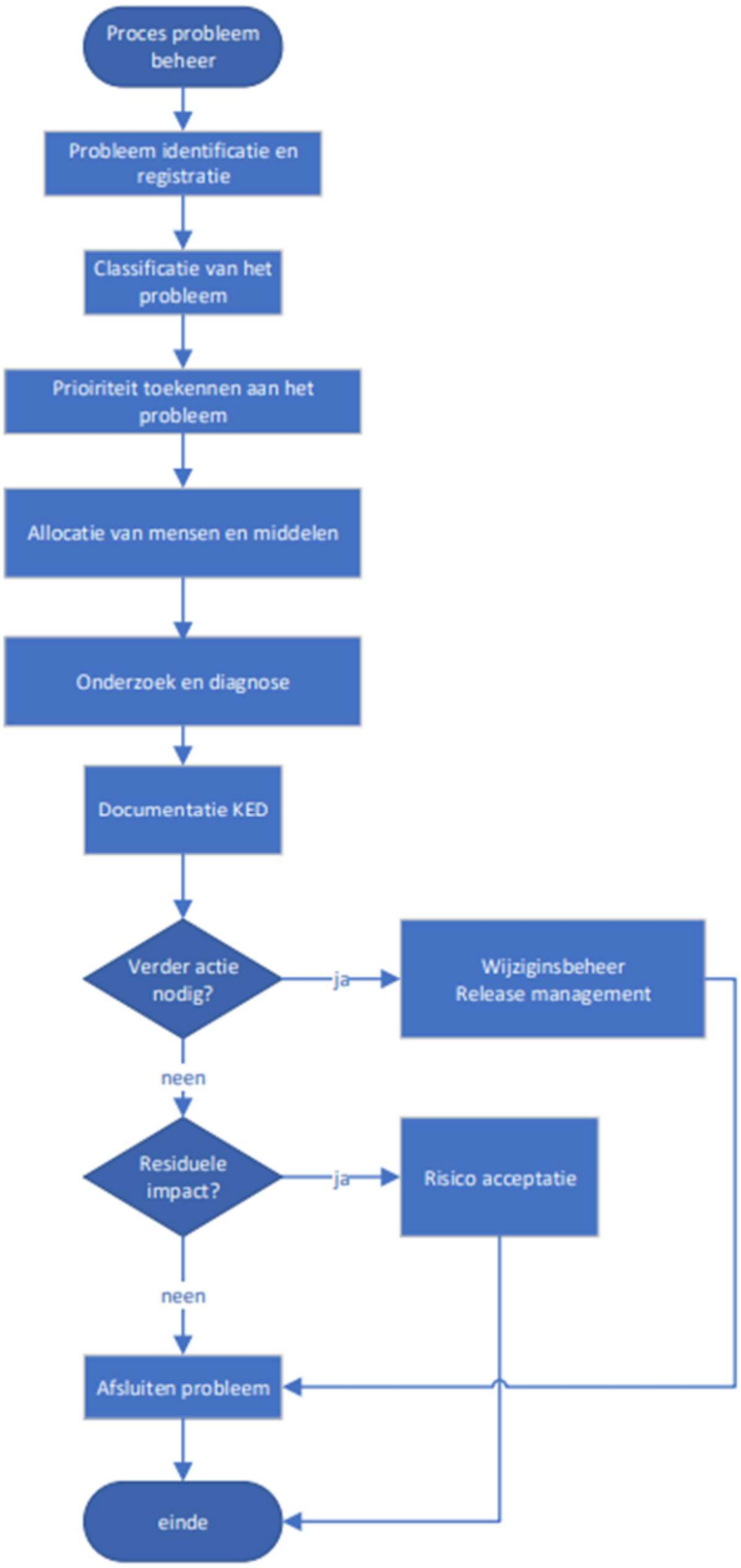
Wanneer de oorzaak van de incidenten door onderzoek en diagnose van het probleem geïdentificeerd is, resulteert dit in een gekende fout. Een gekende fout wordt gedocumenteerd in een *Known Error Database (KED)*: naast een beschrijving van het probleem worden ook de oorzaak (*root cause*), de tijdelijke oplossing (*work around*) en de finale oplossing hierin opgenomen. Deze KED is een belangrijk en efficiënt hulpmiddel voor het snel aanpakken van incidenten: als een incident gelinkt kan worden aan een gekende fout, kan uit de KED afgeleid worden welke *work around* kan worden aangeboden en of/wanneer een finale oplossing in zicht is. Door documentatie van de gekende fout kan veel tijd uitgespaard worden als een incident zich meermaals voordoet vooraleer een definitieve oplossing is geïmplementeerd.

Hoewel een groot deel van de fouten aan het licht gebracht worden door probleemanalyse kan ook ontwikkeling een bron van gekende fouten zijn. Tijdens de ontwikkeling van nieuwe systemen kunnen zich problemen voordoen die door onderzoek en diagnose een (voor ontwikkeling) gekende fout worden. Als gevolg van interne of externe factoren, bijvoorbeeld nieuwe producten of wettelijke vereisten, is het mogelijk dat een toepassing in exploitatie genomen moet worden inclusief de op dat moment gekende fouten. In deze situaties is het noodzakelijk dat met de bij de programmatuur behorende documentatie ook de gekende fouten worden overgedragen aan de beheersorganisatie.

Het doel van foutbeheer is het verhelpen van fouten in de ICT-infrastructuur, zodat het overeengekomen dienstenniveau gerealiseerd kan worden. Naast het wegnemen van fouten bestaat foutbeheer ook uit het minimaliseren van de negatieve gevolgen van een bestaande fout. Om een fout te herstellen zal in veel gevallen een wijzing op de ICT-infrastructuur nodig zijn. Het uitvoeren van deze wijziging vindt plaats onder controle van de processen wijzigingsbeheer (geplande wijziging) of release en deployment beheer (niet geplande wijziging).

Het voorbereiden van een wijzigingsvoorstel is onderdeel van foutbeheer en houdt onder andere in dat verschillende oplossingsalternatieven afgewogen worden. Een van deze alternatieven dient uitgewerkt te worden met betrekking tot de benodigde middelen en de te verwachten inzet. Pas wanneer de evaluatie van de wijziging heeft plaatsgevonden en is vastgelegd dat de oorzaak van de incidenten inderdaad is weggenomen kan de gekende fout worden afgesloten.

2.3.7. Het proces



3. Link met andere beheerprocessen

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

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

Er is een directe link met incident beheer aangezien alle problemen aangeleverd worden door dit proces.

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

Om een gekende fout te herstellen en dus de oorzaak van één of meerdere incidenten structureel weg te werken, dient vaak een wijziging uitgevoerd te worden. Indien het gaat om een in te plannen wijziging, wordt dit opgenomen door wijzigingsbeheer.

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

Indien het gaat om een niet-geplande wijziging, dient dit opgenomen te worden door dit proces.

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

Dit proces levert informatie over de betrokken configuratie-items aan probleembeheer. De informatie die de Eigenaar moet bijhouden is de classificatie op gebied van Vertrouwelijkheid, Integriteit en Beschikbaarheid.