

Plan van Aanpak Realisatiefase

**{Projectnaam}**

Rubriceringsniveau {Rubriceringsniveau}

Versie {Versienummer}, {Datum}



Inhoudsopgave

##### Colofon

###### Rubricering

Rubricering conform [VIRBI 2013, art. 4](https://wetten.overheid.nl/BWBR0033507/2013-06-01#Artikel4).

{Verwijder deze paragraaf en de rubricering op de titelpagina als rubricering niet van toepassing is}

|  |  |  |
| --- | --- | --- |
| Rubriceringsniveau | Rubriceringsduur | Vaststeller |
| {Rubriceringsniveau} | {Rubriceringsduur} | {Vaststeller van de rubricering: minister, staatssecretaris, secretaris-generaal of een door de secretaris-generaal aangewezen rubriceringsambtenaar} |

###### Goedkeuring

|  |  |  |
| --- | --- | --- |
| Versie | Datum goedkeuring | Goedgekeurd door |
| {versie} | {datum} | {naam} |

###### Revisiehistorie

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Versie | Datum | Status | Auteur | Reviewers | Opmerkingen |
| {versie} | {datum} | {status} | {naam} | {namen} | {opmerkingen} |

###### Betrokkenen bij dit document

{Neem in onderstaande tabel de auteurs, reviewers en goedkeurders van dit document op}

|  |  |  |
| --- | --- | --- |
| Organisatie | Functie/rol | Naam |
| {opdrachtgevende organisatie} | Opdrachtgever | {naam} |
| {opdrachtgevende organisatie} | Projectleider | {naam} |
| {opdrachtgevende organisatie} | Product owner | {naam} |
| {opdrachtgevende organisatie} | Kwaliteitsmanager | {naam} |
| {beheerorganisatie} | Projectleider | {naam} |
| {beheerorganisatie} | Kwaliteitsmanager | {naam} |
| ICTU | Projectleider | {naam} |
| ICTU | Software delivery manager | {naam} |
| ICTU | Kwaliteitsmanager | {naam} |

###### Template versie

Versie wip, 06-12-2024

Verbeterpunten t.a.v. deze template graag melden via [GitHub](https://github.com/ICTU/Kwaliteitsaanpak/issues).

# Managementsamenvatting

{Managementsamenvatting}

# Inleiding

## Over dit document

{Dit template gaat ervan uit dat het plan van aanpak een los document is, als aanvulling op het voorstel inclusief projectovereenkomst. Er kan ook voor worden gekozen delen van dit plan van aanpak op te nemen in het voorstel.}

Bij de uitvoering van softwareontwikkelprojecten hanteert ICTU de ICTU Kwaliteitsaanpak Softwareontwikkeling. Conform deze aanpak volgt na de voorfase een realisatiefase, waarin de software wordt ontwikkeld.

Tijdens de voorfase van {het project} zijn de volgende activiteiten uitgevoerd:

1. Vaststellen of het mogelijk is om binnen de door {opdrachtgevende organisatie} gestelde kaders productierijpe software op te leveren {en operationeel te beheren} met de gevraagde functionaliteit en kwaliteit, en zo ja, onder welke randvoorwaarden. Hierbij wordt gekeken naar:
   1. techniek (zoals platform, voortbrengingsproces software en koppelingen),
   2. scope,
   3. planning,
   4. samenwerking,
   5. risico’s.
2. Voorbereiden van een eventuele start van de realisatie, zodat het Scrumteam van een voldoende uitgewerkte backlog is voorzien bij de start.

Om tot {projectresultaat} te komen, ontwikkelt ICTU in samenwerking met {partijen} {het product}; zie voor een beschrijving hiervan het hoofdstuk "Producten". Dit plan van aanpak beschrijft verder de planning van en werkwijze tijdens de realisatiefase. Het is een aanvulling op het voorstel inclusief projectovereenkomst {titel, versie en datum}.

## Doelgroep

Dit plan van aanpak is in eerste instantie bestemd voor de opdrachtgever van {opdrachtgevende organisatie}. Het plan biedt ook inzicht en overzicht aan andere betrokkenen bij het project, onder wie projectmedewerkers van ICTU.

ICTU voert de realisatiefase uit in nauwe samenwerking met {partijen}, waarbij ICTU zo goed mogelijk gebruik maakt van de bij deze partijen aanwezige kennis en producten. Dit vraagt, naast de inspanning van ICTU, ook significante inzet van medewerkers van {partijen}; zie hiervoor het hoofdstuk "Werkwijze".

{Als de beheerorganisatie bij start van de realisatiefase nog niet bekend is, vormt dat waarschijnlijk een aanzienlijk risico voor het project. Als operationeel beheer onderdeel is van de dienstverlening is dit zelfs onoverkomelijk. Benoem hier dat deze onbekende partij wel degelijk tot de doelgroep van dit document behoort. Verwijs naar het hoofdstuk "Werkwijze" voor de getroffen maatregelen om de late keuze voor een beheerorganisatie zoveel mogelijk te ondervangen. Verwijs naar gemaakte aannames rond zaken als productieplatform, releaseprocessen en beheerfunctionaliteit.}

## Kaders

De volgende kaders zijn van toepassing op het realisatieproces van het project. Kaders die van toepassing zijn op het te realiseren *product* zijn opgenomen in PSA, NFE en/of backlog.

|  |  |
| --- | --- |
| Volgnummer | Kader |
| K01 | NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017 |
| K02 | VIR 2007, VIRBI 2013 en BIO voor het inrichten en beheren van informatiebeveiliging in brede zin. |
| K03 | {Indien van toepassing:} NEN 7510:2017 - Informatiebeveiliging in de zorg. |
| K04 | {Indien van toepassing:} Wbni 2018 - Wet Beveiliging Netwerk- en Informatiesystemen. |
| K05 | ICTU Kwaliteitsaanpak Softwareontwikkeling wip |

## Uitgangspunten

De volgende uitgangspunten zijn van toepassing op dit plan van aanpak:

|  |  |
| --- | --- |
| Nr | Uitgangspunt |
| U01 | Het werven van personeel voor het uitvoeren van dit project start na ondertekening van het eveneens verstuurde voorstel inclusief projectovereenkomst door {opdrachtgevende organisatie}. |
| U02 | {opdrachtgevende organisatie} is verantwoordelijk voor het betrekken van {partijen} en het tijdig opleveren van reviews. |
| U03 | {opdrachtgevende organisatie} is verantwoordelijk voor het aanstellen van een product owner met voldoende tijd en mandaat. |
| {volgnummer} | {uitgangspunt} |

## Relatie met andere documenten

De realisatiefase is een vervolg op de voorfase van {het project}. De documenten die in die voorfase zijn gerealiseerd en die uitgangspunt zijn voor dit plan van aanpak zijn:

* Projectstartarchitectuur (PSA), versie {versie},
* Business impact analysis (BIA), versie {versie},
* Privacy impact assessment (PIA), versie {versie},
* Softwarearchitectuurdocument (SAD), versie {versie},
* Infrastructuurarchitectuur (IA), versie {versie},
* Mastertestplan, versie {versie},
* Detailtestplan softwarerealisatie, versie {versie},
* Informatiebeveiligingsplan (IB-plan), versie {versie},
* Kwaliteitsplan, versie {versie},
* Niet-functionele eisen (NFE), versie {versie},
* Globaal functioneel ontwerp (GFO), versie {versie},
* Interactie-ontwerp (UX), versie {versie},
* Geprioriteerde backlog met user stories, versie {versie},
* Vastgesteld minimal viable product, versie {versie},
* Wireframe, mockup, prototype, animatie, versie {versie},
* Tussentijdse rapportage t.b.v. go/no-go besluit, versie {versie}.

{Beschrijf ook een eventuele relatie met andere documenten die niet afkomstig zijn uit de voorfase}

## Leeswijzer

Hoofdstuk 2 beschrijft de in de realisatiefase op te leveren producten. In hoofdstuk 3 staat de werkwijze voor de realisatie van de software. Hoofdstuk 4 beschrijft de planning en doorlooptijd van het project. Hoofdstuk 5 geeft de randvoorwaarden die ingevuld dienen te zijn bij de start van realisatiefase. Hoofdstuk 6 beschrijft de bekende projectrisico's en de getroffen tegenmaatregelen. Hoofdstuk 7 bevat de verwachte inzet door ICTU. {Vul aan en pas verwijzingen aan, indien nodig}

Bijlage A bevat afkortingen en termen die voorkomen in de ICTU Kwaliteitsaanpak Softwareontwikkeling en bijbehorende templates. Bijlage B verwijst naar regelmatig gebruikte bronnen. Bijlage C bevat een beknopte samenvatting van de ICTU Kwaliteitsaanpak Softwareontwikkeling.

# Projectresultaat

De te {ontwikkelen en/of onderhouden} software {beschrijving functionaliteit in hoofdlijnen van de software}.

De software komt tot stand door middel van een agile aanpak met een doorlooptijd van {doorloop} weken, waarbij ICTU de softwareontwikkeling uitvoert; zie hiervoor het hoofdstuk “Werkwijze”.

## Producten en diensten

ICTU levert de volgende producten en diensten op:

1. Werkende software met de functionaliteiten zoals hierboven beschreven.
2. Per release:
   1. informatie ten behoeve van het vrijgaveadvies,
   2. de release notes,
   3. een bijgewerkte installatiehandleiding,
   4. een bijgewerkt software-architectuurdocument (SAD),
   5. een bijgewerkt globaal functioneel ontwerp (GFO),
   6. de broncode, inclusief unit testen,
   7. een set van automatische regressietesten (ART),
   8. een beschrijving van de logische testgevallen,
   9. een actuele versie van de kwaliteitsrapportage,
   10. {eventueel bijgewerkte andere documentatie waarvoor ICTU verantwoordelijk en/of penvoerder is, zoals testplannen en kwaliteitsplan}.

{Als operationeel beheer onderdeel is van de dienstverlening: Het DevOps-team voert operationele beheertaken uit, conform overeengekomen kwaliteitsniveaus (quality of services). Hiertoe maakt het project beheerafspraken met de opdrachtgevende organisatie en de beheerorganisatie en legt deze vast in een dossier afspraken en procedures (DAP). Het vastleggen en rapporteren van informatie over de software tijdens het gebruik en over de uitgevoerde beheeractiviteiten kan hiervan deel uitmaken. De afspraken zijn afgestemd op het beheerplan van de beheerorganisatie, waarin is beschreven hoe de verschillende vormen van beheer van de applicaties en de infrastructuur worden uitgevoerd.}

{Als operationeel en/of applicatiebeheer onderdeel is van de dienstverlening: beschrijf wanneer en hoe de dienstverlening eindigt of verlengd wordt. Bijvoorbeeld, geef aan wat de minimale hoeveelheid aan ontwikkel- en onderhoudwerk is waarbij ICTU nog een geschikte partij is om het operationeel en applicatiebeheer uit te voeren.}

## Scope

Binnen de scope van de opdracht valt de {ontwikkeling en/of het onderhoud} van {het product}, inclusief:

* Ontwikkel, test- en demo-omgevingen,
* Engineering tools voor versiebeheer (GitLab of Azure DevOps), bouwen en testen (Azure DevOps, GitLab en/of Jenkins), kwaliteitscontrole (SonarQube), beveiligingscontrole (SonarQube, OWASP Dependency-Check en/of Dependency-Track, ZAP by Checkmarx, OpenVAS), toegankelijkheid (Axe), performancetesten (JMeter) en integrale kwaliteitsrapportage (Quality-time),
* {Als operationeel beheer onderdeel is van de dienstverlening:} Uitrollen in de productieomgeving (Ansible), container registry (Harbor), performance monitoring (APM), security monitoring ({vul aan met concreet product}), controle van kwetsbaarheden in frameworks ({vul aan met concreet product}), controle van images van containers (Trivy), registratie van incidenten bij gebruik en beheer (Topdesk of Jira).
* Backlog management tools (Jira en/of Azure DevOps),
* Beveiligings- en performancetesten in de ICTU-testomgevingen. ICTU voert deze tests uit voordat een nieuwe versie van de software wordt opgeleverd. {Beschrijf hier eventuele andere afspraken met de opdrachtgevende organisatie}.

{Als operationeel beheer geen onderdeel is van de dienstverlening:} Buiten de scope van de opdracht valt:

* Acceptatie- en productieomgevingen en de installatie van de software op acceptatie- en productieomgevingen,
* Beveiligings- en performancetesten in acceptatie- en productieomgevingen, die onder verantwoordelijkheid van de opdrachtgevende organisatie worden uitgevoerd,
* Keten- en integratietesten met aanpalende systemen in acceptatie- en productieomgevingen,
* Testen met (geanonimiseerde) productiedata,
* Beheeractiviteiten door ICTU.

# Werkwijze

Het succes van het uit te voeren realisatietraject is sterk afhankelijk van de beschikbaarheid en inzet van alle betrokkenen. Deze betrokkenheid dient daarom voor aanvang van het project expliciet te worden geborgd door de betrokken organisaties. Dit zal door de projectleider ICTU en {opdrachtgevende organisatie} gemonitord worden.

## Scrum-aanpak

Tijdens dit project wordt agile gewerkt volgens de Scrum-aanpak. ICTU propageert de kernwaarden van Scrum. Dit vertaalt zich concreet in:

* Een Scrumteam, bestaande uit een product owner, door {opdrachtgevende organisatie} aangesteld, die de uiteindelijke inhoudelijke keuzes maakt, en ontwikkelaars (zoals programmeurs, testers en ontwerpers) en een Scrummaster, door ICTU aangesteld.
* Een proces met sprints van {twee of drie} weken waarin de Scrumactiviteiten sprint planning, sprint refinement, daily scrum, sprint demonstratie/review en retrospective plaatsvinden.
* Een definition of ready en een definition of done voor respectievelijk het beginnen en afronden van werk.
* Een product backlog en een sprint backlog.

## DevOps-werkwijze

{Verwijder deze paragraaf indien niet van toepassing}

Tijdens het project wordt DevOps toegepast. Dit vertaalt zich concreet in:

* Het na elke sprint in productie brengen van de nieuwe release.
* Het monitoren van de software tijdens het gebruik en het afhandelen van monitoring-alerts.
* Het oplossen van incidenten.
* Het ondersteunen van functioneel beheerders.
* Rapporteren over de beheerafspraken.
* Het maken van backups en restoren indien nodig.
* {Vul aan en pas aan waar nodig}

## Werving

Direct na de opdrachtverstrekking start ICTU met de bemensing van het project ten behoeve van de realisatiefase. {Beschrijf de eventueel te werven functies}

## Kick-off

Voor een goede start wordt er, bij aanvang van de realisatiefase, een kick-off georganiseerd met alle projectmedewerkers, beoogde stuurgroepleden en de opdrachtgever. In de kick-off komen, naast een kennismaking, eventuele acties aan bod die nog uitgevoerd moeten worden voordat daadwerkelijk met de realisatiefase kan worden begonnen. {Als er al dergelijke acties bekend zijn, voeg ze eventueel hier in.} Ook worden de risico’s geïdentificeerd die van toepassing zijn op de realisatiefase en het verdere verloop van het project. Na opdrachtverstrekking zal de projectleider van ICTU de kick-off voorbereiden en plannen.

## Samenwerking

{opdrachtgevende organisatie}, {partijen} en ICTU werken gezamenlijk aan de op te leveren software in een Scrumteam. Voor een goed resultaat is het van belang dat er minimaal {aantal} {dagen/dagdelen} per week door alle partijen wordt samengewerkt. {partij} stelt hiervoor {fysieke en/of online} ruimte en samenwerkhulpmiddelen beschikbaar; projectmedewerkers zorgen zelf voor een laptop. {Als met hulpmiddelen van ICTU wordt gewerkt: Om deze bij ICTU te gebruiken moeten de laptops voldoen aan de bij ICTU geldende beveiligingsnormen, welke zijn opgenomen in het ICTU-voorschrift Zakelijk gebruik ICT-diensten en voorzieningen.}

Vertegenwoordigers van het project nemen deel aan de volgende overleggen met {opdrachtgevende organisatie} en de beheerorganisatie:

* het architectuuroverleg,
* het informatiebeveiligingsoverleg,
* het beheeroverleg,
* {vul aan en pas aan, indien nodig}

## Projectbesturing

{Beschrijf kort de governancestructuur: stuurgroep, rapportage- en escalatielijnen}

## Oplevering software

De realisatiefase bestaat uit {aantal} sprints. Tijdens elke sprint verwerkt het Scrumteam door de product owner geselecteerde functionaliteit in de software. Geselecteerde functionaliteit die niet afkomt tijdens de sprint kan door de product owner opnieuw geselecteerd worden voor de volgende sprint, of voor een latere sprint. Als er na afronding van de realisatiefase nieuwe wensen of fouten aan het licht komen, dan kan {opdrachtgevende organisatie} deze later alsnog verwerken of ICTU vragen dit in een eventuele vervolgopdracht uit te voeren.

{Beschrijf hier de afspraken tussen ICTU en de opdrachtgevende organisatie over de opzet van vrijgaveadvies, release notes en goedkeuringsproces.}

## Kwaliteitsbeheersing

De kwaliteitsbeheersing is door ICTU beschreven in het Kwaliteitsplan. Eén van de kwaliteitsmaatregelen is dat ICTU een geautomatiseerd kwaliteitssysteem (Quality-time) inricht dat de kwaliteit van de software en het ontwikkelproces bewaakt. De ICTU-kwaliteitsmanager configureert de metrieken in Quality-time en bewaakt de metingen.

## Inzet {opdrachtgevende organisatie} en {partijen}

Betrokkenheid van inhoudsdeskundigen van {opdrachtgevende organisatie} en {partijen} is randvoorwaardelijk voor de uitvoering van de opdracht. Van de betrokken medewerkers van deze organisatie{s} wordt het volgende verwacht:

* Actief bijdragen aan workshops en demo's;
* Buiten de workshops uitzoeken van onduidelijkheden en binnen de eigen organisatie(s) op zoek gaan naar antwoorden;
* Opstellen, onderhouden en/of reviewen van documenten namens de opdrachtgevende organisatie.

Onderstaand is de verwachte inzet van per rol van {opdrachtgevende organisatie} en {partijen} voor de uitvoering van dit plan van aanpak (één persoon kan eventueel meer dan één rol vervullen):

{Selecteer de juiste rollen en vul aan, vul ook de juiste verantwoordelijkheden in, onderstaande is een eerste opzet met zoveel mogelijk rollen}

|  |  |  |
| --- | --- | --- |
| Rollen | Verwachte inzet per week | Verantwoordelijkheden |
| Projectleider ({opdrachtgevende organisatie}) | {aantal} dagen | Bespreken voortgang en eventuele exceptions met de projectleider (opdrachtnemer), deelname aan demo's en eventuele workshops |
| Product owner | {aantal} dagen | Prioritering user stories, sprintplanning, demo, onderhouden backlog |
| Business analist | {aantal} dagen | Epics opstellen voor de product backlog, eventueel uitgewerkt in user stories |
| Architect | {aantal} dagen | Bewaken en onderhouden van de softwarearchitectuur |
| Infrastructuurarchitect | {aantal} dagen | Bewaken en onderhouden infrastructuurarchitectuur, opstellen infrastructuurarchitectuur (IA) |
| Testmanager | {aantal} dagen | Testen van nieuwe softwarereleases voordat deze voor gebruik worden vrijgegeven |
| Expert informatiebeveiliging | {aantal} dagen | Bewaken en onderhouden BIA, opstellen TVA en IB-plan |
| Privacy-expert | {aantal} dagen | Bewaken en onderhouden PIA |
| Diverse inhoudelijk deskundigen | {aantal} dagen | Inbrengen domeinexpertise en vertegenwoordiging van (eind)gebruikers en belanghebbenden |
| Technisch beheerder beheerorganisatie | {aantal} dagen | Leveren en beheer acceptatie- en productieomgeving |
| Functioneel beheerder | {aantal} dagen | Functioneel beheer |
| Servicedeskmedewerker | {aantal} dagen | Gebruikersondersteuning en incidentbeheer |
| Diverse technisch en inhoudelijk specialisten | ad hoc | Inzet op ad-hocbasis ter ondersteuning van de andere rollen |

## Afstemming met gerelateerde projecten

{Beschrijf de afstemming met gerelateerde projecten, indien van toepassing}

## Projectafsluiting

Omdat ICTU tijdens het project de software, inclusief documentatie, regelmatig oplevert is er geen speciale eindoplevering nodig. ICTU archiveert de projectartifacten zoals beschreven in de bijlage "Projectafsluiting".

# Planning en doorlooptijd

De start van het project vindt uiterlijk {aantal} weken na ondertekening van het voorstel inclusief projectovereenkomst plaats. In deze periode bemensen zowel ICTU als {opdrachtgevende organisatie} het project. Daarbij is rekening gehouden met de doorlooptijd van de werving en selectie van de geschikte mensen.

De verwachte doorlooptijd van de uitvoering van dit plan van aanpak is {aantal} weken.

Met een eventuele vakantieperiode is nog geen rekening gehouden, dit zal direct na de “go” op het voorstel inclusief projectovereenkomst afgestemd worden. Mogelijk wordt hierdoor de doorlooptijd langer. Op dat moment wordt ook de verdere invulling van de planning en de sprints afgestemd.

{Hieronder een voorbeeld van een planning}

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Onderdeel/week | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Bemensen project | X | X | X |  |  |  |  |  |  |  |  |  |
| Voorbereiden en plannen kick-off |  | X | X |  |  |  |  |  |  |  |  |  |
| Kick-off |  |  |  | X |  |  |  |  |  |  |  |  |
| Inrichten ontwikkelstraat sprint 0 |  |  |  | X | X |  |  |  |  |  |  |  |
| Realisatie producten sprint 1 |  |  |  |  |  | X | X |  |  |  |  |  |
| Realisatie producten sprint 2 |  |  |  |  |  |  |  | X | X |  |  |  |
| Realisatie producten sprint 3 |  |  |  |  |  |  |  |  |  | X | X |  |
| Afronden en afsluiten realisatiefase |  |  |  |  |  |  |  |  |  |  |  | X |

# Randvoorwaarden

Voor de uitvoering van de realisatiefase gelden de volgende randvoorwaarden:

|  |  |
| --- | --- |
| Nr | Randvoorwaarde |
| R01 | De vereiste inzet van betrokkenen van {opdrachtgevende organisatie} en {partijen} is georganiseerd en gegarandeerd. |
| R02 | De product owner is gemandateerd om zelfstandig besluiten te nemen over de functionaliteit van de software. |
| R03 | Er is een afgestemde en afgesproken werkwijze tussen {opdrachtgevende organisatie}, {beheerorganisatie} en ICTU. Deze is in lijn met de ICTU Kwaliteitsaanpak Softwareontwikkeling. |
| R04 | De voorfaseproducten {producten} zijn beschikbaar voor aanvang van de realisatiefase. |
| R05 | Koppelvlakbeschrijvingen van aanpalende systemen zijn beschikbaar. |
| {volgnummer} | {randvoorwaarde} |

# Projectrisico’s

De onderstaande projectrisico’s, die het succes van de realisatiefase kunnen belemmeren, zijn reeds onderkend; daarbij zijn per risico de maatregelen benoemd.

De risico’s worden door het project bijgehouden in het risicolog. De risico’s en de mitigerende maatregelen worden in de realisatiefase bewaakt en waar nodig geactualiseerd.

{Deze tabel dient op basis van het concrete project en voorstel aangepast te worden.}

|  |  |
| --- | --- |
| Projectrisico | Maatregel |
| Verwachtingen over dit project tussen verschillende partijen ({partijen}, ICTU) kunnen niet waargemaakt worden, waardoor vertraging ontstaat | Wekelijks projectoverleg, samenwerken door middel van werkgroepen en fysiek bij elkaar komen, kick-off met alle betrokkenen waarbij opdrachtgever of product owner de productvisie uiteenzet. |
| Scope-uitbreiding, gebrek aan focus | Scope bewaken, alleen de scope uitbreiden als dit noodzakelijk is voor {doel} |
| Onvoldoende bemensing door vakanties | Rekening houden met langere doorlooptijd dan de (te) eenvoudige rekensom suggereert. |
| {Bij DevOps werkwijze} Onduidelijkheid over de verdeling van verantwoordelijkheden tussen DevOps-team en beheerorganisatie (incident management, backup & restore, etc.) | Afspraken over onderlinge samenwerking vastleggen in een dossier afspraken en procedures (DAP). |
| {risico} | {maatregel} |

# Verwachte inzet ICTU

Onderstaand is de verwachte inzet per rol van ICTU voor de uitvoering van dit plan van aanpak:

{Selecteer de rollen die nodig zijn en vul ze aan. Vul de juiste verantwoordelijkheden in. De onderstaande tabel is een eerste opzet met veel voorkomende rollen.}

|  |  |  |
| --- | --- | --- |
| Rol | Verwachte inzet | Verantwoordelijkheden |
| Software-architect/senior ontwikkelaar | {x} uur | Onderhouden SAD, bewaken architectuurkeuzes, ontwerpen, ontwikkelen en testen van de software |
| Scrummaster | {x} uur | Bewaken Scrumproces, faciliteren Scrumevents |
| Ontwikkelaar | {x} uur | Ontwerpen, ontwikkelen en testen van de software |
| DevOps-engineer | {x} uur | Ontwerpen, ontwikkelen en testen van de software, daarnaast uitvoeren beheeractiviteiten, waaronder het oplossen van incidenten |
| Tester | {x} uur | Opstellen logische testgevallen, ontwikkelen en uitvoeren fysieke testgevallen, opstellen testrapportages |
| Functioneel ontwerper | {x} uur | Onderhouden GFO, ondersteunen product owner bij opstellen en uitwerken van de user stories |
| Database administrator | {x} uur | Onderhouden logisch datamodel en fysiek database ontwerp, ontwikkelen migratiescripts, database tuning |
| UX-designer | {x} uur | Gebruikersonderzoek, onderhouden UX-richtlijnen, maken en onderhouden prototype {of wireframe/mockup/animatie}, toetsen prototypes met gebruikers |
| Informatiebeveiligingsexpert | {x} uur | Onderhouden IB-plan, toetsen IB-maatregelen |
| Kwaliteitsmanager | {x} uur | Inrichten, onderhouden en bewaken kwaliteitsrapportage |
| Software delivery manager | {x} uur | Bewaken plan van aanpak realisatiefase, faciliteren en coördineren van het Scrumteam, inhoudelijke rapportage |
| Projectleider | {x} uur | Bewaken overeenkomst realisatiefase, opleveren tussentijdse rapportage, bespreken voortgang en exceptions met opdrachtgever |
| Projectsecretaris | {x} uur | Ondersteuning, rapportage, administratie |
| Diverse technisch specialisten | {x} uur | Ondersteunen, adviseren en meeschrijven daar waar nodig op onderdelen waar kennis of tijd van teamleden niet toereikend is |
| **Totaal** | **{x} uur** |  |

{In de projectovereenkomst moet in de begroting met onderstaande opmerkingen rekening worden gehouden.}

{Voor de begroting wordt uitgegaan van een gemiddeld bruto tarief. De werkelijke kosten worden bekend als de projectmedewerkers bekend zijn. Wanneer overschrijding van het budget dreigt (bijvoorbeeld vanwege substantieel hogere tarieven), wordt dit tijdig met de opdrachtgever besproken.}

Naast kosten voor de inzet van ICTU-medewerkers worden de volgende kosten voor door ICTU te benutten diensten verwacht:

|  |  |  |
| --- | --- | --- |
| Dienst | Verwachte kosten | Toelichting |
| Performancetests |  |  |
| Securitytests |  |  |
| Onderhoudbaarheidstoetsen |  |  |
| Usabilitytests |  |  |
| Toegankelijkheidstests |  |  |

Bijlagen

1. Terminologie en afkortingen

De onderstaande tabel bevat afkortingen en termen die voorkomen in de ICTU Kwaliteitsaanpak Softwareontwikkeling en bijbehorende templates.

|  |  |
| --- | --- |
| Term/afkorting | Toelichting |
| **actor** | een persoon die, of een extern informatiesysteem dat, een handeling verricht op het **informatiesysteem** |
| **architectuur** | een beschrijving van de structuur van een systeem, inclusief onderdelen, relaties tussen die onderdelen en eigenschappen van die onderdelen en relaties |
| **API** | application programming interface |
| **ART** | automatische **regressietest** |
| **auditing** | Vastlegging van de door een actor verrichte handelingen |
| **authenticatie** | het vaststellen van de identiteit van een **actor** |
| **autorisatie** | aan een **actor** toegekende rechten |
| **beheerorganisatie** | een (samenwerkingsverband van) organisatie(s) die in opdracht van een **opdrachtgevende organisatie** het **operationeel beheer**, applicatief beheer en/of functioneel beheer van **software** uitvoert |
| **BIA** | business impact analysis |
| **BIO** | Baseline Informatiebeveiliging Overheid |
| **broncode** | **software** in een vorm die leesbaar is voor mensen en de intentie van een programmeur uitdrukt |
| **deployment** | installatie van **software** op een systeem waardoor de software beschikbaar wordt gemaakt voor gebruik door **actor**en |
| **developers** | Developers zijn de mensen in het **Scrumteam** die iedere sprint gecommitteerd zijn aan het maken van elk aspect van een bruikbaar increment [Scrumgids] |
| **DevOps** | een praktijk die tot doel heeft **softwareontwikkeling** en **operationeel beheer** samen te brengen |
| **DoD** | definition of done |
| **DoR** | definition of ready |
| **gebruikskwaliteit** | mate waarin een systeem, product of dienst kan worden gebruikt door gespecificeerde gebruikers, voor het bereiken van gespecificeerde doelen, met effectiviteit, efficiëntie en tevredenheid in een gespecificeerde gebruikscontext |
| **GFO** | globaal functioneel ontwerp |
| **IB-plan** | informatiebeveiligingsplan |
| **informatiesysteem** | een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en **programmatuur** alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie [VIR 2007, NORA] |
| **infrastructuurarchitectuur** | een **architectuur** die vooral de hardwareonderdelen en -relaties (housing, hardware, virtuals, standaard software en middleware) van een systeem beschrijft |
| **IPO** | intern projectoverleg |
| **ISD** | ICTU Software Diensten, afdeling van ICTU die **softwareontwikkelprojecten** ondersteunt met ontwikkel- en testomgevingen, tools en diensten |
| **ISE** | ICTU Software Expertise, afdeling van ICTU die **softwareontwikkelprojecten** ondersteunt met expertise op het gebied van **softwareontwikkeling** en die de ICTU Kwaliteitsaanpak Softwareontwikkeling onderhoudt |
| **ISO** | International Organization for Standardization |
| **Jira** | tool om **use cases**, user stories, logische testgevallen en issues vast te leggen |
| **klantreis** | alle directe en indirecte interactie van een klant of gebruiker met een product of dienst |
| **KPI** | key performance indicator |
| **kwaliteitsmanager** | controleert en borgt de kwaliteit van **software** conform de vastgestelde eisen en de Kwaliteitsaanpak en rapporteert aan de **projectleider** |
| **minimum viable product** | de eerste versie van een product of dienst, die zo vroeg mogelijk wordt uitgerold naar de gebruikers; het bevat net voldoende functionaliteit om het gestelde doel te behalen, en niet meer dan dat |
| **MTP** | master testplan |
| **MVP** | **minimum viable product** |
| **NFE** | niet-functionele eis(en) |
| **NORA** | Nederlandse Overheidsreferentie-architectuur |
| **NPR** | Nederlandse Praktijkrichtlijn |
| **ontwikkelaars** | Ontwikkelaars (*developers* in de Scrumgids) zijn de mensen in het **Scrumteam** die iedere sprint gecommitteerd zijn aan het maken van elk aspect van een bruikbaar increment [Scrumgids] |
| **opdrachtgevende organisatie** | overheidsorganisatie die opdracht geeft aan ICTU tot ontwikkeling en/of onderhoud van **software** |
| **opdrachtgever** | medewerker van de **opdrachtgevende organisatie** die eindverantwoordelijk is voor de opdracht aan ICTU |
| **operationeel beheer** | activiteiten die zorgen dat software operationeel is en blijft, zoals het oplossen van incidenten, het uitvoeren van onderhoud, het implementeren van upgrades en patches, het beheren van configuraties, en het monitoren van prestaties en beschikbaarheid |
| **OTAP** | ontwikkel, test, acceptatie, productie; gebruikt om verschillende soorten omgevingen aan te duiden |
| **persona** | een min of meer realistische beschrijving van een fictief persoon, veelal met naam, persoonskenmerken, drijfveren en behoeften, die een groep gebruikers representeert en gebruikt wordt om te redeneren over de gewenste functionele en niet-functionele eigenschappen van de **software** |
| **PIA** | privacy impact assessment |
| **PKI** | public key infrastructure |
| **PRA** | productrisicoanalyse |
| **Product owner** | De product owner is verantwoordelijk voor het maximaliseren van de waarde van het product, dat het resultaat is van het werk van het **Scrumteam** [Scrumgids] |
| **programmatuur** | zie **software** |
| **project** | een tijdelijke organisatie voor het realiseren van een resultaat - bij ICTU bestaat een **softwareontwikkelproject** uit medewerkers van ICTU, de **opdrachtgevende organisatie**, beheerorganisatie en eventueel andere partijen |
| **projectleider** | medewerker eindverantwoordelijk voor het projectresultaat - bij ICTU-softwareontwikkelprojecten is de projectleider een medewerker van ICTU |
| **PSA** | De projectstartarchitectuur is een concreet en doelgericht ICT-architectuurkader waarbinnen het **project** moet worden uitgevoerd |
| **PvE** | programma van eisen |
| **Quality-time** | een door ICTU ontwikkeld, open source, geautomatiseerd kwaliteitssysteem |
| **realisatiefase** | fase van een **softwareontwikkelproject** waarin de **software** daadwerkelijk wordt gebouwd en onderhouden, en bij een **DevOps** werkwijze ook operationeel wordt beheerd |
| **regressietest** | test die na een wijziging controleert of niet-gewijzigde delen van een systeem nog steeds correct functioneren |
| **release notes** | een overzicht van de wijzigingen in een **release** |
| **release** | een voor gebruik vrijgegeven versie van de **software** |
| **SAD** | software-architectuurdocument |
| **Scrum** | Scrum is een lichtgewicht raamwerk dat mensen, teams en organisaties helpt om waarde te creёren door middel van adaptieve oplossingen voor complexe problemen [Scrumgids] |
| **Scrummaster** | De Scrummaster is verantwoordelijk voor het opzetten van **Scrum**, zoals staat beschreven in de Scrumgids [Scrumgids] |
| **Scrumteam** | Een Scrumteam bestaat uit één **Scrummaster**, één **product owner** en **ontwikkelaars** (*developers* in de Scrumgids) [Scrumgids] |
| **softwarearchitectuur** | een **architectuur** die vooral de softwareonderdelen en -relaties (processen, modules, interfaces, datamodel) van een systeem beschrijft |
| **software delivery manager** | organiseert het ontwikkelen en opleveren van **software** conform de vastgestelde eisen en de Kwaliteitsaanpak en rapporteert aan de **projectleider** |
| **software** | software is de verzameling instructies die bepalen wat een computer uitvoert en is uiteindelijk wat de gebruiker ziet, ervaart en waarmee hij interacteert |
| **softwareontwikkeling** | een activiteit die nieuwe **software** maakt en/of bestaande software aanpast |
| **softwareontwikkelproject** | een **project** dat de oplevering van **software** als enige of voornaamste projectresultaat heeft |
| **solution architectuur** | beschrijving van de gewenste oplossing van een specifiek probleem, of het eindresultaat van een **project** [NORA] |
| **technische schuld** | eigenschappen van de **software** die de lange-termijninzetbaarheid en onderhoudbaarheid bedreigen |
| **TVA** | threat and vulnerability assessment |
| **usability** | gebruiksvriendelijkheid |
| **use case** | een afgebakende eenheid van interactie tussen een **actor** en het systeem |
| **UX** | user experience |
| **VIR** | Voorschrift Informatiebeveiliging Rijksdienst |
| **VIRBI** | Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie |
| **VM** | virtual machine, virtuele machine |
| **voorfase** | fase van een **softwareontwikkelproject**, voorafgaande aan de **realisatiefase**, waarin de uitgangspunten, risico's en randvoorwaarden voor de realisatiefase worden bepaald en waarin wordt gezorgd dat aan de randvoorwaarden wordt voldaan en dat voor zoveel mogelijk risico's maatregelen getroffen zijn |
| **vrijgaveadvies** | advies om een **release** vrij te geven voor ingebruikname, met een testverslag dat tenminste alle nog openstaande testbevindingen en geconstateerde beveiligingsbevindingen bevat |

1. Bronnen

De onderstaande tabel verwijst naar regelmatig gebruikte bronnen.

|  |  |
| --- | --- |
| Bron | Toelichting |
| [BIO](https://bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf) | Baseline Informatiebeveiliging Overheid. |
| [ISO 9241-210:2019](https://www.iso.org/standard/77520.html) | Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems. |
| [NCSC ICT-beveiligingsrichtlijnen voor webapplicaties](https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties) | De ICT-beveiligingsrichtlijnen voor webapplicaties geven een leidraad voor veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. |
| [NEN-ISO/IEC 25010:2011](https://www.nen.nl/nen-iso-iec-25010-2011-en-157265) | Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models. |
| [NEN-ISO/IEC 27001:2017](https://www.nen.nl/nen-en-iso-iec-27001-2017-a11-2020-nl-265545) | Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen |
| [NEN-ISO/IEC 27002:2017](https://www.nen.nl/nen-en-iso-iec-27002-2017-nl-245390) | Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging |
| [NEN 7510:2017](https://www.nen.nl/nen-7510-1-2017-a1-2020-nl-267179) | Informatiebeveiliging in de zorg. |
| [NEN NPR 5325:2017](https://www.nen.nl/npr-5325-2017-nl-238298) | Praktijkrichtlijn voor het overdragen van software. |
| [NEN NPR 5326:2019](https://www.nen.nl/npr-5326-2019-nl-262885) | Praktijkrichtlijn voor risicobeheersing bij softwareontwikkeling. |
| [NORA](https://www.noraonline.nl) | Referentiearchitectuur voor de Nederlandse Overheid. |
| [OWASP Top-10](https://owasp.org/www-project-top-ten/) | De OWASP Top-10 is een op consensus gebaseerd overzicht van de meest kritische beveiligingsrisico's voor webapplicaties. |
| [Scrumgids](https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Dutch.pdf) | De Scrum Gids - De Definitieve Gids voor Scrum: De Regels van het Spel. |
| [VIR 2007](https://wetten.overheid.nl/BWBR0022141/2007-07-01) | Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007. |
| [VIRBI 2013](https://wetten.overheid.nl/BWBR0033507/2013-06-01) | Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013. |
| [Wbni 2018](https://wetten.overheid.nl/BWBR0041515/2020-07-15) | Wet Beveiliging Netwerk- en Informatiesystemen. Beschrijft de meldplicht en de zorgplicht die van toepassing zijn op organisaties die vitaal zijn én op digitale dienstverleners. |

1. De ICTU Kwaliteitsaanpak Softwareontwikkeling

De overheid is in hoge mate afhankelijk van informatiesystemen voor de uitvoering van haar taken. Veel van die informatiesystemen zijn dusdanig specifiek dat de benodigde software “op maat” gemaakt moet worden. De totstandkoming van op maat gemaakte software is meestal een complex proces, waarin vele belangen en behoeften worden afgewogen en afgezet tegen de mogelijkheden die technologie biedt. Eenmaal operationeel zal een informatiesysteem verantwoord onderhouden moeten worden; behoeften en technologie veranderen in de loop van de tijd.

Overheidsprojecten waarin software wordt ontwikkeld of onderhouden kampen nog vaak met vertraging, budgetoverschrijding of een eindresultaat met te lage kwaliteit. Zo concludeerde de commissie-Elias in haar [eindrapport](https://www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf): "De Rijksoverheid heeft haar ICT (Informatie- en communicatietechnologie)-projecten niet onder controle". Eén van de fundamentele problemen is dat de risico's, die inherent zijn aan softwareontwikkeling, door organisaties nog onvoldoende worden herkend, erkend en gemitigeerd. Dit terwijl de risico's bij de ontwikkeling van software, binnen het ICT-domein, algemeen bekend zijn en er ook voor veel risico's passende maatregelen bestaan.

ICTU heeft jarenlange ervaring met het realiseren van software en past de opgedane ervaring toe bij de ontwikkeling van nieuwe software. Die ervaring is vastgelegd in een werkwijze, deze “ICTU Kwaliteitsaanpak Softwareontwikkeling”, die telkens wordt aangepast en aangevuld op basis van de praktijk.

ICTU is ervan overtuigd dat het bouwen van duurzame software, die goed aansluit bij de behoeften van gebruikers en andere belanghebbenden, bijdraagt aan betere informatiesystemen en een betere dienstverlening door de overheid. Dienstverlening die betrouwbaar moet zijn voor burgers, bedrijven en ambtenaren. Om samen met opdrachtgevende organisaties passende oplossingen te realiseren ontwikkelt ICTU daarom software volgens een agile proces. En om de duurzaamheid en betrouwbaarheid te bevorderen besteedt ICTU standaard aandacht aan beveiliging, privacy, performance, gebruikskwaliteit en toegankelijkheid. De Kwaliteitsaanpak dient daarvoor als leidraad, maar de aanpak voorziet ook in mogelijkheden om het project en het eindproduct aan te passen aan de specifieke situatie.

Om projecten, die software realiseren volgens de Kwaliteitsaanpak, efficiënt en effectief te ondersteunen, heeft ICTU twee gespecialiseerde afdelingen in het leven geroepen. Deze afdelingen staan projecten bij door middel van kennis, menskracht en technische hulpmiddelen. Zo profiteren projecten van schaalgrootte en hergebruik van inzichten.

Met behulp van de ICTU Kwaliteitsaanpak Softwareontwikkeling heeft ICTU samen met andere overheden inmiddels enige tientallen projecten succesvol uitgevoerd. ICTU wil deze aanpak graag aanvullen met de ervaringen en geleerde lessen van andere organisaties en deze overdraagbaar maken en breder uitdragen. Om die reden stelt ICTU deze Kwaliteitsaanpak aan iedereen beschikbaar via <https://www.ictu.nl/kwaliteitsaanpak> en heeft zij, samen met normalisatie-instituut NEN en partijen uit overheid en markt, een praktijkrichtlijn “Risicobeheersing bij ontwikkeling en onderhoud van maatwerksoftware” [NEN NPR 5326:2019] gepubliceerd, die mede is gebaseerd op de ICTU Kwaliteitsaanpak Softwareontwikkeling.

De ICTU Kwaliteitsaanpak Softwareontwikkeling heeft drie doelstellingen:

1. Opdrachtgevende organisaties helpen bekende risico's bij softwareontwikkeling, zoals technische schuld, vertraging en defecten, zo veel mogelijk te voorkomen.
2. ICTU helpen om software te ontwikkelen die de missie van ICTU, namelijk bijdragen aan een betere digitale overheid, ondersteunt.
3. De overheid als geheel helpen bij het zo goed mogelijk ontwikkelen van software.

De Kwaliteitsaanpak zelf is geformuleerd in de vorm van maatregelen die elke software-ontwikkelende organisatie kan treffen om risico's van softwareontwikkeling te mitigeren en de kans op succesvolle softwareontwikkelprojecten te vergroten. De maatregelen zijn gebaseerd op geleerde lessen uit de praktijk van ICTU.

De Kwaliteitsaanpak is een evoluerende aanpak, gebaseerd op de ervaringen die ICTU continu opdoet in de projecten waarin ICTU samen met opdrachtgevende organisaties maatwerksoftware ontwikkelt en onderhoudt. ICTU hanteert daarbij de vuistregel dat als tenminste 80% van de projecten minstens 80% van de tijd een bepaalde werkwijze hanteren, voor die werkwijze een maatregel in de Kwaliteitsaanpak wordt opgenomen. Maar het kan ook voorkomen dat maatregelen om andere redenen landen in de Kwaliteitsaanpak; denk aan het toegankelijk maken van software dat wettelijk verplicht is. Zie ook de wijzigingsgeschiedenis in [PDF-formaat](https://ictu.github.io/Kwaliteitsaanpak/wip/ICTU-Kwaliteitsaanpak-Wijzigingsgeschiedenis.pdf) of [HTML-formaat](https://ictu.github.io/Kwaliteitsaanpak/wip/ICTU-Kwaliteitsaanpak-Wijzigingsgeschiedenis.html).

De maatregelen vormen het startpunt voor de aanpak van ieder ICTU-softwareproject, waarbij ruimte wordt geboden voor variatie of alternatieve invulling. Bijvoorbeeld stelt de Kwaliteitsaanpak: software wordt minimaal bij iedere grote release of tenminste twee keer per jaar onderworpen aan een beveiligingstest door beveiligingsexperts die ICTU daarvoor inhuurt (zie M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen). Een alternatief is dat de opdrachtgevende organisatie de verantwoordelijkheid neemt voor het laten uitvoeren van beveiligingstests. Hierover maakt de projectleider nadere afspraken met de opdrachtgever.

De Kwaliteitsaanpak is dus zowel voorschrijvend als beschrijvend. Voorschrijvend omdat ICTU verwacht dat projecten die maatwerksoftware ontwikkelen en onderhouden de aanpak toepassen, en alleen aanpassen als daar een goede reden voor is, en mits dat wettelijk is toegestaan. Tegelijkertijd is de aanpak beschrijvend omdat de meeste maatregelen voortkomen uit de bestaande werkwijzen van de projecten. Zoals blijkt uit de self-assessment die ICTU regelmatig uitvoert op de toepassing van de Kwaliteitsaanpak.

1. Projectafsluiting

De onderstaande tabel geeft aan welke archiveringsactiviteiten aan het einde van een project worden uitgevoerd. De software delivery manager is verantwoordelijk voor het archiveren.

|  |  |  |  |
| --- | --- | --- | --- |
| Wat | Waar staat het | Wie archiveert het | Bewaartermijn |
| Broncode, testscripts en documentatie | Git | Scrumteam | 5 jaar |
| Overige documentatie | Sharepoint of andere samenwerkruimte | Scrumteam | 5 jaar |
| Final Release | {waar} | Scrumteam | 5 jaar |
| Performancetestscripts | Git performanceteam | Scrumteam | 5 jaar |
| Kwaliteitsrapportage | Quality-time database | ISD | 2 jaar |
| Bugs, user stories en andere issues | Jira | ISD | 2 jaar |
| VM’s Scrumteam | {waar} | ISD | 2 jaar |
| {Projectspecifieke producten} | {waar} | {wie} | {termijn} |

Bij projectafsluiting zorgt de software delivery manager verder dat volgende acties worden uitgevoerd:

* ISD trekt credentials van projectmedewerkers zoals VPN-keys en LDAP-accounts in,
* projectmedewerkers verwijderen broncode, testscript en documentatie van hun laptops.