

Inwerkplan Kwaliteitsmanager

**{Projectnaam/-namen}**

Rubriceringsniveau {Rubriceringsniveau}

Versie {Versienummer}, {Datum}



Inhoudsopgave

##### Colofon

###### Rubricering

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

{Verwijder eventueel deze paragraaf en de rubricering op de titelpagina indien 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} |

###### Revisiehistorie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versie | Auteur | Datum | Status | Opmerkingen |
| {versie} | {naam} | {datum} | {concept/definitief} | {opmerkingen} |

###### Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Functie/rol | Naam | Datum | Versie |
| Kwaliteitsmanager {opdrachtgever} | {naam} | {datum} | {versie} |
| Kwaliteitsmanager {beheerorganisatie} | {naam} | {datum} | {versie} |
| Kwaliteitsmanager ICTU | {naam} | {datum} | {versie} |

###### Vereiste goedkeuringen

|  |  |  |  |
| --- | --- | --- | --- |
| Functie/rol | Naam | Datum | Versie |
| Projectleider {opdrachtgever} | {naam} | {datum} | {versie} |
| Projectleider {beheerorganisatie} | {naam} | {datum} | {versie} |
| Projectleider ICTU | {naam} | {datum} | {versie} |
| Product owner | {naam} | {datum} | {versie} |

###### Verzendlijst huidige versie

|  |  |  |
| --- | --- | --- |
| Naam | Organisatie | Functie/rol |
| {naam} | {opdrachtgever} | Projectleider |
| {naam} | {opdrachtgever} | Product owner |
| {naam} | {beheerorganisatie} | Projectleider |
| {naam} | ICTU | Projectleider |
| {naam} | ICTU | Software delivery manager |

###### Template versie

Versie 4.0.0-dev, 06-06-2023

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

# Managementsamenvatting

Dit inwerkplan beschrijft de leerdoelen die de nieuwe kwaliteitsmanager voor de projecten {projecten} zou moeten behalen tijdens de inwerkfase. De leerdoelen betreffen kennis over ICTU als organisatie, kennis van de softwareontwikkelaanpak van ICTU, kennis van de projecten waar de nieuwe kwaliteitsmanager op wordt ingezet en kennis over de rol van kwaliteitsmanager zoals die binnen ICTU wordt gehanteerd.

# Inleiding

## Over dit document

Dit document beschrijft de leerdoelen die een kwaliteitsmanager softwareontwikkeling bij ICTU tijdens de inwerkfase zou moeten halen.

Dit document bevat niet de kennis zelf. Een ervaren kwaliteitsmanager draagt deze over aan de nieuwe kwaliteitsmanager. Waar mogelijk bevat dit document wel linkjes naar de standaardbronnen (denk aan de ICTU Kwaliteitsaanpak Softwareontwikkeling).

De nieuwe kwaliteitsmanager houdt zelf de voortgang bij van het halen van de leerdoelen en het uitvoeren van de acties.

## Doelgroep

Doelgroep van dit document zijn mensen die nieuw bij ICTU beginnen als kwaliteitsmanager bij een project dat maatwerksoftwareontwikkeling uitvoert volgens de ICTU Kwaliteitsaanpak Softwareontwikkeling.

## Kaders

De volgende kaders zijn van toepassing op het inwerkplan.

|  |  |
| --- | --- |
| 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 4.0.0-dev |

## Uitgangspunten

De volgende uitgangspunten zijn van toepassing op dit document:

|  |  |
| --- | --- |
| Volgnummer | Uitgangspunt |
| U01 | De projecten waarop de kwaliteitsmanager wordt ingezet ontwikkelen software conform de ICTU Kwaliteitsaanpak Softwareontwikkeling. |
| U02 | De vertrekkende kwaliteitsmanager draagt de kennis over aan de nieuwe kwaliteitsmanager. |
| U03 | {uitgangspunt} |
| {volgnummer} | {uitgangspunt} |

## Relatie met andere documenten

Relevant voor dit inwerkplan zijn de volgende documenten:

|  |  |
| --- | --- |
| Titel | Versie |
| Projectstartarchitectuur {projectnaam} | {versie} |
| Niet-functionele eisen {productnaam} | {versie} |
| Kwaliteitsplan {projectnaam} | {versie} |
| {titel} | {versie} |

## Leeswijzer

Het volgende hoofdstuk beschrijft wat je moet weten over ICTU als organisatie. Hoofdstuk 3 beschrijft wat je moet weten over de manier waarop ICTU software ontwikkelt. Hoofdstuk 4 beschrijft de leerdoelen specifiek voor de projecten waarop je als kwaliteitsmanager wordt ingezet. Hoofdstuk 5 beschrijft wat je moet weten over je eigen rol.

Dit plan gaat uit van een inwerkperiode van vier weken. ICTU-projecten die software ontwikkelen hanteren een sprintlengte van twee of drie weken. Dat betekent dat in een periode van vier weken alle Scrumceremonies minimaal één keer langskomen. Bij alle leerdoelen en activiteiten staat als suggestie aangegeven in welke week je deze zou moeten kunnen behalen danwel uitvoeren.

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.

# Wat je moet weten over ICTU

Dit hoofdstuk bevat leerdoelen over ICTU als organisatie binnen het Nederlandse overheidslandschap en voorzieningen die ICTU biedt aan al haar medewerkers. Dit hoofdstuk is daarmee niet specifiek voor de rol van kwaliteitsmanager, maar voor de volledigheid toch hier opgenomen.

## ICTU-organisatie

Leerdoelen (week 1):

* Je weet wat [de missie van ICTU](https://www.ictu.nl/over-ons) is
* Je weet [voor wie ICTU werkt](https://www.ictu.nl/over-ons/voor-wie-we-werken) en [welke diensten ICTU levert](https://www.ictu.nl/dienstenoverzicht)
* Je weet welke [directies en afdelingen ICTU](https://ictubeheer.sharepoint.com/teams/Organisatie_DirectieICTU/SitePages/Organisatieschets.aspx) heeft en wat in grote lijnen de taken en verantwoordelijkheden van die afdelingen zijn
* Je weet wie de [directie van ICTU](https://www.ictu.nl/over-ons/bestuur-directie) bemensen

Acties (zodra mogelijk):

* Je hebt deelgenomen aan de [ICTU-onboarding](https://ictubeheer.sharepoint.com/teams/Onboarding2)
* Je hebt deelgenomen aan de [ICTU-live update](https://ictubeheer.sharepoint.com/teams/Corona-info/SitePages/coronavirus--updates.aspx)

## ICTU-voorzieningen

Leerdoelen (week 1):

* Je weet hoe je hulp kunt vragen van de [Service Desk](https://ictubeheer.sharepoint.com/teams/Organisatie_ServicedeskenFacilitairezaken) bij het gebruik van de ICTU-voorzieningen

Je hebt toegang tot (week 1):

* [MS Outlook](https://webmail.ictu.nl) voor e-mail en agenda
* [Timetell](https://timetell.ictu.nl) voor het registreren van uren
* [Sharepoint](https://ictubeheer.sharepoint.com) voor het delen van documenten
* [MS Teams](https://teams.microsoft.com) voor online vergaderen en teamconversaties (chat)
* [Topdesk](https://topdesk.ictu.nl) voor het reserveren van vergaderzalen, parkeerplaatsen en andere diensten
* [Yammer](https://www.yammer.com) voor niet-urgente communicatie en organisatiebrede conversaties (ook bereikbaar via MS Teams)

# Wat je moet weten over softwareontwikkeling bij ICTU

ICTU-projecten die software ontwikkelen en/of onderhouden worden ondersteund met een aanpak (de ICTU Kwaliteitsaanpak Softwareontwikkeling) en een ontwikkelplatform inclusief kwaliteitssysteem. De Kwaliteitsaanpak wordt geleverd door de afdeling ICTU Software Expertise. Het ontwikkelplatform (meestal Ecosysteem genoemd) inclusief kwaliteitssysteem (Quality-time genaamd) wordt geleverd door de afdeling ICTU Software Diensten.

Leerdoelen (week 3):

* Je weet welke [softwareontwikkelprojecten](https://ictubeheer.sharepoint.com/teams/TEAMSDM/SitePages/ISR-Projecten-SDM-ers.aspx?source=https://ictubeheer.sharepoint.com/teams/TEAMSDM/SitePages/Forms/ByAuthor.aspx) ICTU uitvoert
* Je weet met welke leveranciers ICTU [raamovereenkomsten](https://ictubeheer.sharepoint.com/teams/Organisatie_Inkoop/SitePages/Raamovereenkomsten.aspx) heeft voor het uitvoeren van securitytesten, performancetesten en onderhoudbaarheidstoetsen en hoe deze ondersteuning ingekocht kan worden

## ICTU Software Expertise (ISE)

### Over de afdeling

Acties (week 1)

* Je bent lid van de mailgroep ISR-leden (ja, die naam moet nog worden aangepast)
* Je bent lid van de mailgroep kwaliteitsmanagers

Leerdoelen (week 2):

* Je weet welke diensten de afdeling [ISE](https://ictubeheer.sharepoint.com/teams/Organisatie_SoftwareExpertise) levert aan de projecten die software ontwikkelen
* Je weet wie het afdelingshoofd is en welke teams er zijn binnen ISE

Acties (zodra mogelijk):

* Je hebt deelgenomen aan de ISE-onboarding
* Je hebt deelgenomen aan een ISE-zeepkist
* Je hebt deelgenomen aan een ISE-guild
* Je neemt deel aan het periodieke kwaliteitsmanagersoverleg

### Over de ICTU Kwaliteitsaanpak Softwareontwikkeling

Leerdoelen kwaliteitsaanpak (week 2):

* Je weet waar je de [publieke versie van de kwaliteitsaanpak](https://www.ictu.nl/kwaliteitsaanpak) kunt vinden en waar je de [interne versie van de kwaliteitsaanpak inclusief templates](https://ictubeheer.sharepoint.com/:f:/r/teams/Organisatie_SoftwareExpertise/Open/ICTU%20Kwaliteitsaanpak%20Softwareontwikkeling?csf=1&web=1&e=v7lK2Z) kunt vinden.
* Je weet welke maatregelen de kwaliteitsaanpak bevat en waarom
* Je weet wat de relatie is tussen de kwaliteitsaanpak en de missie van ICTU
* Je weet welke ICTU-collega's de kwaliteitsaanpak onderhouden en gebruikers ondersteunen
* Je weet hoe je een [fout of een wijzigingsverzoek](https://github.com/ICTU/Kwaliteitsaanpak/issues) kunt opvoeren

Leerdoelen self-assessment (week 3):

* Je weet waar je de self-assessment template kunt vinden (hint: zie locatie interne versie van de kwaliteitsaanpak hierboven)
* Je weet hoe je de self-assessment kunt invullen
* Je weet wat het doel van de self-assessment is en hoe ICTU dit instrument toepast
* Je kent de [uitkomsten van recente gezamenlijke self-assessments](https://ictubeheer.sharepoint.com/:f:/r/teams/Organisatie_SoftwareExpertise/Besloten/Gez.%20self-assessments?csf=1&web=1&e=lXs65L)

Leerdoelen templates (week 4):

* Je weet de templates te vinden (hint: zie locatie interne versie van de kwaliteitsaanpak hierboven)
* Je weet welke templates er zijn en waar ze voor gebruikt worden
* Je weet hoe je de templates kunt gebruiken

## ICTU Software Diensten (ISD)

### Over de afdeling

Leerdoelen (week 2):

* Je weet welke diensten de afdeling [ISD](https://ictubeheer.sharepoint.com/teams/Organisatie_SoftwareDiensten) levert aan de projecten die software ontwikkelen
* Je weet wie het afdelingshoofd is en welke teams er zijn binnen ISD

### Over het kwaliteitsysteem

Leerdoelen (week 2):

* Je weet wat het doel van [Quality-time](https://quality-time.readthedocs.io/en/latest/) is
* Je kent de [functies](https://quality-time.readthedocs.io/en/latest/intro.html#features) van Quality-time
* Je kunt de [gebruikersdocumentatie](https://quality-time.readthedocs.io/en/latest/usage.html) van Quality-time vinden
* Je weet welke ICTU-collega's Quality-time onderhouden en gebruikers ondersteunen
* Je weet hoe je een [fout of een wijzigingsverzoek](https://github.com/ICTU/quality-time/issues) kunt opvoeren
* Je weet welke metrieken ICTU typisch gebruikt om de kwaliteit van softwareproducten en -processen te meten en bewaken
* Je kunt metrieken en bronnen configureren
* Je kunt issues toevoegen aan metrieken
* Je kunt technische schuld administreren
* Je kunt tijdreizen in Quality-time (vooral relevant als je voor je project periodieke kwaliteitsrapportage gaat maken)

### Over het ontwikkelplatform

Leerdoelen (week 3):

* Je kent de [functies](https://ictubeheer.sharepoint.com/teams/Organisatie_SoftwareDiensten/SitePages/ECO2.aspx) van het Ecosysteem
* Je weet dat er twee generaties ontwikkelplatform zijn, te weten "Eco1" en "Eco2", en kent de belangrijkste verschillen
* Je weet wie de product owner van het Ecosysteem is
* Je weet hoe je problemen met het ecosysteem kunt [melden aan ISD](https://jira.ictu-sd.nl/jira/secure/CreateIssueDetails!init.jspa?pid=11709&issuetype=10100)
* Je weet hoe je je Ecosysteem VPN-key kan verlengen

# Wat je moet weten over je project

## Projectcontext

Leerdoelen (week 1):

* Je begrijpt wat de doelstelling van de opdrachtgever met het project is, c.q. je weet welk probleem het project moet oplossen
* Je weet wie de beoogde gebruikers zijn en wie er verder belanghebbende zijn bij het projectresultaat
* Je weet welke organisaties naast de opdrachtgever en ICTU bij het project zijn betrokken

## Projectorganisatie

Leerdoelen (week 2):

* Je weet welke governancestructuur er is afgesproken (stuurgroep, projectleidersoverleg, rapportages, e.d.)
* Je weet wie welke rol speelt bij de opdrachtgever, ICTU en andere betrokken organisaties (projectleider, product owner, software delivery manager, e.d.)
* Je weet wie welke rol speelt binnen het/de Scrumteam(s) in je project (ontwikkelaar, tester, devops-engineer, ontwerper, etc.)
* Je hebt kennisgemaakt met de kwaliteitsmanager aan de kant van de opdrachtgever

## Proces

Acties (week 1):

* Je bent uitgenodigd voor en neemt deel aan het periodieke IPO (Intern Project Overleg)
* Je bent uitgenodigd voor en neemt deel aan de daily scrum van het Scrumteam

Acties (zodra mogelijk):

* Je bent uitgenodigd voor en neemt deel aan de demo's van het Scrumteam
* Je hebt deelgenomen aan een refinement, sprintplanning en retrospective

Leerdoelen Quality-time kwaliteitsrapportage (week 1):

* Je weet uit welke onderdelen (subjects) de rapportage is opgebouwd en waarom
* Je weet welke metrieken en bronnen er zijn
* Bij afwijkende normen weet je waarom er wordt afgeweken van de default norm
* Je weet welke technische schuld is vastgelegd en waarom en welke acties daarover zijn afgesproken in je project

Leerdoelen periodieke kwaliteitsrapportage (indien van toepassing, zodra mogelijk):

* Je kunt de periodieke kwaliteitsrapportage maken en verspreiden
* Je kunt oude periodieke kwaliteitsrapportages vinden
* Je kent de inhoud van recente periodieke kwaliteitsrapportages

Leerdoelen diensten (week 3):

* Je weet welke ondersteuning je project krijgt van ISD (en of dat Eco1 of Eco2 is)
* Je weet welke ondersteuning je project krijgt van de security tool engineer
* Je weet welke ondersteuning je project krijgt van de performancetestdienstverlener (momenteel Sentia)

Leerdoelen self-assessment (week 4):

* Je weet waar je de recente self-assessments van je project kunt vinden
* Je weet wat de uitkomsten zijn van de recente self-assessments zijn
* Je weet welke acties er zijn afgesproken n.a.v. de recent self-assessments en hoe de voortgang ervan wordt bewaakt

Leerdoelen externe onderzoeken/audits, zoals securitytesten en onderhoudbaarheidstoetsen (week 4):

* Je kunt oude auditrapportages vinden
* Je kent de inhoud van recente auditrapportages
* Je weet welke acties er zijn afgesproken n.a.v. de recente audits en hoe de voortgang ervan wordt bewaakt
* Je weet welke audits gepland zijn

## Product

Leerdoelen (week 3):

* Je kent in grote lijnen de huidige en beoogde functionaliteit van de software die je project ontwikkelt en/of onderhoudt
* Je kent de gewenste en actuele kwaliteitseigenschappen van de software die je project ontwikkelt en/of onderhoudt
* Je bent op de hoogte van de in het product aanwezige technische schuld en de daarvoor afgesproken verbeteracties
* Je weet wat er in het kwaliteitsplan van je project staat en welke projectspecifieke kwaliteitsmaatregelen er zijn afgesproken

## Tools

Acties (week 3):

* Je bent lid van de mailgroep van je project (indien van toepassing)
* Je hebt toegang tot het MS Teams-team van je project
* Je hebt toegang tot de Sharepoint teamsite van je project
* Je hebt toegang tot de ontwikkelomgeving (VLAN) van je project, d.w.z. dat je beschikt over een VPN-key die daartoe toegang geeft
* Je hebt toegang tot het versiebeheersysteem van je project (GitLab of Azure DevOps)
* Je hebt toegang tot de build server van je project (GitLab CI, Azure DevOps of Jenkins)
* Je hebt toegang tot je project in [Jira](https://jira.ictu-sd.nl/jira/)
* Je hebt toegang tot de securityrapportages in de build pipeline (OWASP Dependency Check, OWASP ZAP, OpenVAS)
* Je hebt toegang tot de toegankelijksrapportage (Axe) in de build pipeline
* Je hebt toegang tot de testrapportages in de build pipeline (Robot Framework, JUnit, Cypress, etc.)
* Je hebt toegang tot de SonarQube van je project
* Je hebt toegang tot de Quality-time van je project
* Je hebt toegang tot de performancerapportage van je project (zie [overzicht performancetestrapportages](https://reports.pc.iesprd.ictu-sr.nl))
* Je hebt toegang tot de actie- en besluitenlijst van je project (in Trello of MS Planner)
* Je hebt toegang tot het risicolog van je project
* Je beschikt over een urencode voor je project in [Timetell](https://timetell.ictu.nl)

# Wat je moet weten over je eigen rol

Leerdoelen (week 2):

* Je kent de taken en verantwoordelijkheden van een kwaliteitsmanager (zie templates Kwaliteitsplan, Plan van Aanpak Voorfase en Plan van Aanpak Realisatiefase)
* Je weet welke specifieke afspraken zijn gemaakt over je taken en verantwoordelijkheden binnen je project (zie Kwaliteitsplan van je eigen project)

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** |
| **API** | application programming interface |
| **ART** | automatische **regressietest** |
| **auditing** | Vastlegging van de door een actor verrichtte handelingen. |
| **authenticatie** | het vaststellen van de identiteit van een **actor** |
| **autorisatie** | aan een **actor** toegekende rechten |
| **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] |
| **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] |
| **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, opdrachtgever, beheerorganisatie en eventueel andere partijen |
| **projectleider** | medewerker eindverantwoordelijk voor het projectresultaat - bij ICTU-softwareontwikkelprojecten is de projectleider een medewerker van ICTU |
| **PSA** | De projectsoftwarearchitectuur 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]. |
| **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 |
| **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, 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 opdrachtgevers 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. Opdrachtgevers 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 opdrachtgevers 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.

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 opdrachtgever 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.