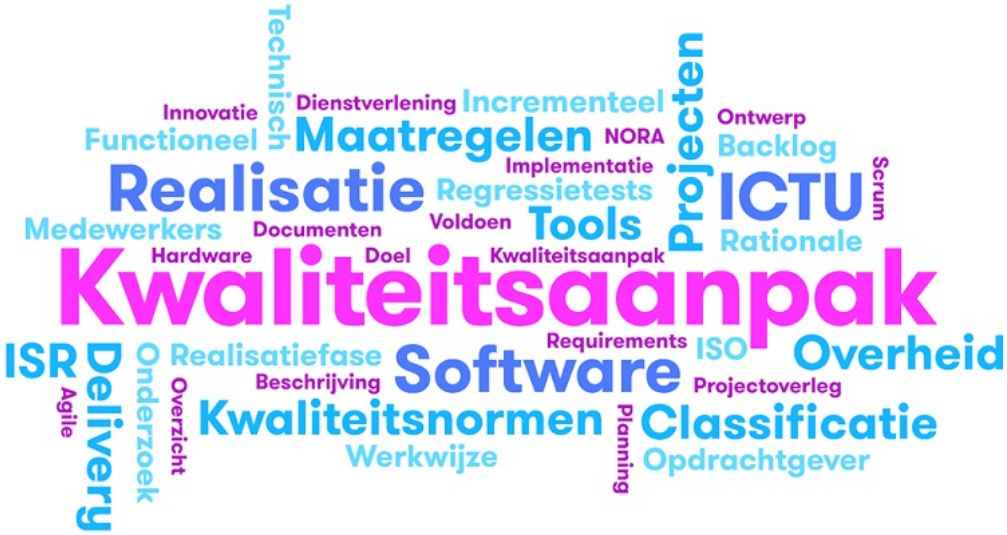
Niet-Functionele Eisen
{Projectnaam}
Versie {versienummer}
Datum {datum}



Inhoudsopgave

Revisiehistorie

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

Vereiste goedkeuringen

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

Verzendlijst huidige versie

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

Template versie

Versie 1.3.1-build.9, 29-08-2019

1 Inleiding

1.1 Over dit document

Dit document beschrijft de niet-functionele eisen aan {systeem}. Basis voor de niet-functionele eisen zijn de kwaliteitsattributen, zoals gedefinieerd in de ISO/IEC-25010:2011 standaard. Deze standaard maakt onderscheid in het Product Quality model en het Quality-in-Use model. Dit document richt zich op het Product Quality model.

ISO/IEC-25010:2011 definieert de kwaliteitseigenschappen voor een softwareproduct. Deze zijn onderverdeeld in acht hoofdeigenschappen: Functionele geschiktheid, Efficiëntie, Uitwisselbaarheid, Bruikbaarheid, Betrouwbaarheid, Beveiligbaarheid, Onderhoudbaarheid en Overdraagbaarheid.

Deze hoofdeigenschappen zijn nog te globaal en te abstract om de gewenste eigenschappen van een softwareproduct bespreekbaar, hanteerbaar en realiseerbaar te maken. Een hoofdeigenschap wordt dan ook weer onderverdeeld in eigenschappen. Deze eigenschappen vormen de basis voor de structurering van de niet-functionele eisen.

In totaal zijn de volgende 31 eigenschappen onderkend:

- Functionele geschiktheid
  - Functionele compleetheid
  - Functionele correctheid
  - Functionele toepasbaarheid
- Efficiëntie
  - Snelheid
  - Middelenbeslag
  - Capaciteit
- Uitwisselbaarheid
  - Beïnvloedbaarheid
  - Koppelbaarheid
- Bruikbaarheid
  - Herkenbaarheid van geschiktheid
  - Leerbaarheid
  - Bedienbaarheid
  - Voorkomen gebruikersfouten
  - Volmaaktheid gebruikersinterface
  - Toegankelijkheid
- Betrouwbaarheid
  - Volwassenheid
  - Beschikbaarheid
  - Foutbestendigheid
  - Herstelbaarheid

- Beveiligbaarheid
  - Vertrouwelijkheid
  - Integriteit
  - Onweerlegbaarheid
  - Verantwoording
  - Authenticiteit
- Onderhoudbaarheid
  - Modulariteit
  - Herbruikbaarheid
  - Analyseerbaarheid
  - Wijzigbaarheid
  - Testbaarheid
- Overdraagbaarheid
  - Aanpasbaarheid
  - Installeerbaarheid
  - Vervangbaarheid

1.2 Doelgroep

Dit document is relevant voor de volgende partijen:

- de eigenaar/eigenaren van het systeem,
- de beheerder(s) van het systeem,
- de ontwikkelaar(s) van het systeem.
- de hostingpartij(en).

1.3 Kaders

De volgende kaders zijn van toepassing op het projectresultaat:

Volgnummer	Kader
K01	ISO/IEC 27001:2005, ISO/IEC 27001:2013, 27002:2007, VIR, VIR-BI en BIO:2017 voor het inrichten en beheren van informatiebeveiliging in brede zin.
K02	WCAG2.1 (Web Content Accessibility Guidelines) voor eisen met betrekking tot toegankelijkheid
{volgnummer}	{kader}

1.4 Uitgangspunten

De volgende uitgangspunten zijn van toepassing op dit document:

Volgnummer	Uitgangspunt
U01	{uitgangspunt}
U02	{uitgangspunt}
U03	{uitgangspunt}
{volgnummer}	{uitgangspunt}

1.5 Relatie met andere documenten

{Relatie met andere documenten}

1.6 Leeswijzer

Hoofdstukken 2 tot en met 9 bevatten hebben elk betrekking op een hoofdeigenschap. De hoofdstukken zijn verder onderverdeeld conform de in de tabel genoemde eigenschappen.

Per eis is een identificatie toegekend (“Nr.”), een beschrijving van de eis (“Eis”), wat de prioritering is (“Prio”) en welk document de bewijslast bevat van de invulling van de eis (“Bewijs”). Waar mogelijk en relevant wordt verwezen naar de overige documentatie.

2 Functionele geschiktheid

De mate waarin een softwareproduct of computersysteem functies levert die voldoen aan de uitgesproken en veronderstelde behoeften, bij gebruik onder gespecificeerde condities.

Opmerking: functionele geschiktheid gaat alleen over of, en in welke mate, expliciete en impliciete behoeften worden afgedekt en betreft niet de functionele eisen zelf.

2.1 Functionele compleetheid

De mate waarin de set van functies alle gespecificeerde taken en gebruikersdoelen ondersteunen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

2.2 Functionele correctheid

De mate waarin het systeem de juiste resultaten met de benodigde nauwkeurigheid beschikbaar stelt.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

2.3 Functionele toepasbaarheid

De mate waarin de functies bijdragen aan het behalen van specifieke taken en doelen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

3 Prestatie-efficiëntie

Prestatie van het systeem in verhouding tot het aantal resources, onder bepaalde condities.

3.1 Snelheid

De mate waarin antwoord- en verwerkingstijden en doorvoersnelheid van een product of systeem, tijdens de uitvoer van zijn functies, voldoet aan de wensen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

3.2 Middelenbeslag

De mate waarin de hoeveelheid en type middelen die gebruikt worden door een product of systeem, tijdens de uitvoer van zijn functies, voldoet aan de wensen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

3.3 Capaciteit

De mate waarin de maximale limieten van een product- of systeemparameter voldoet aan de wensen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

4 Uitwisselbaarheid

De mate waarin een product, systeem of component informatie uit kan wisselen met andere producten, systemen of componenten, en/of het de gewenste functies kan uitvoeren terwijl het dezelfde hard- of software-omgeving deelt.

4.1 Beïnvloedbaarheid

De mate waarin een product zijn vereiste functies kan vervullen terwijl het een omgeving en resources deelt met andere producten, zonder negatieve impact op enig product.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

4.2 Koppelbaarheid

De mate waarin twee of meer systemen, producten of componenten informatie kunnen uitwisselen en deze uitgewisselde informatie kunnen gebruiken.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

5 Bruikbaarheid

De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om effectief, efficiënt en naar tevredenheid gespecificeerde doelen te bereiken in een gespecificeerde gebruikscontext.

5.1 Herkenbaarheid van geschiktheid

De mate waarin gebruikers kunnen herkennen of het product of systeem geschikt is voor hun behoeften.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

5.2 Leerbaarheid

De mate waarin het systeem gebruikt kan worden door gespecificeerde gebruikers om gespecificeerde (leer)doelen te bereiken met betrekking tot het gebruik van het systeem met effectiviteit, efficiëntie, vrijheid van risico en voldoening, in een gespecificeerde gebruikscontext.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

5.3 Bedienbaarheid

De mate waarin het systeem kenmerken heeft die het makkelijk maken om het te bedienen en beheersen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

5.4 Voorkomen gebruikersfouten

De mate waarin het systeem gebruikers beschermt tegen het maken van fouten.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

5.5 Volmaaktheid gebruikersinterface

De mate waarin een gebruikersinterface het de gebruiker mogelijk maakt om een plezierige en voldoening gevende interactie te hebben.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

5.6 Toegankelijkheid

De mate waarin het systeem gebruikt kan worden door mensen met de meest uiteenlopende eigenschappen en mogelijkheden om een gespecificeerd doel te bereiken in een gespecificeerde gebruikscontext.

Als standaard voor toegankelijkheid hanteert de Nederlandse overheid, en dus ICTU, de WCAG 2.1 (Web Content Accessibility Guidelines); zie https://www.w3.org/TR/WCAG21/. Conform de EN 301 549, hanteert ICTU de succescriteria voor Level A en AA als eisen.

Nr.	Eis	Prio	Bewijs
1	Waar van toepassing voldoet de applicatie aan de richtlijnen uit WCAG2.1, Level A en AA	{prio}	{bewijs}
{nr}	{eis}	{prio}	{bewijs}

6 Betrouwbaarheid

De mate waarin een systeem, product of component gespecificeerde functies uitvoert onder gespecificeerde condities gedurende een gespecificeerde hoeveelheid tijd.

6.1 Volwassenheid

De mate waarin het systeem onder normale condities de betrouwbaarheidsnormen haalt.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

6.2 Beschikbaarheid

De mate waarin het systeem operationeel en toegankelijk is wanneer men het wil gebruiken.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

6.3 Foutbestendigheid

De mate waarin het systeem werkt zoals bedoeld ondanks de aanwezigheid van hard- of software-fouten.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

6.4 Herstelbaarheid

De mate waarin het systeem, in geval van een onderbreking of bij een fout, de direct betrokken gegevens kan herstellen en het systeem in de gewenste staat kan terug brengen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

7 Beveiligbaarheid

De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

7.1 BIR- en SSD-eisen

De Rijksoverheid is gebonden aan kaderstelling op het gebied van informatiebeveiliging, zoals de Baseline Informatiebeveiliging Rijksdienst (BIR). Handvatten zoals Secure Software Development (SSD) van het Centrum informatiebeveiliging en privacybescherming dienen als leidraad voor het veilig ontwikkelen van software die het voldoen aan de BIR ondersteunt. De BIR is een toepassing van de (ISO 27001:2005) op het domein van de Rijksoverheid. In die toepassing zijn het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI) verwerkt.

BIR en SSD bevatten ook een aantal maatregelen ten aanzien van software en/of de infrastructurele componenten waar deze software gebruik van maakt. Deze maatregelen zijn hieronder als eisen opgenomen.

Nr.	Eis	Prio	Bewijs
1	Applicaties zijn gebaseerd op een formele, met de beheerpartij afgestemde standaard stack, zodat integrale beveiliging mogelijk is en het risico op nieuwe en onbekende zwakheden door het gebruik van onbekende componenten of services beperkt wordt.	{prio}	{bewijs}
2	De architectuur van een (web)applicatie is gebaseerd op een gelaagde structuur door de presentatielaag, de applicatielaag en de gegevens te scheiden, zodat de lagen beschermd kunnen worden binnen de netwerkzones.	{prio}	{bewijs}
3	(Web)applicaties stellen de identiteit van externe gebruikers vast op basis van een mechanisme voor identificatie en authenticatie, waarbij de authenticatiegegevens in een geconsolideerde authenticatievoorziening worden beheerd.	{prio}	{bewijs}
4	(Web)applicaties stellen de identiteit van interne gebruikers vast op basis van een mechanisme voor identificatie en authenticatie, waarbij de authenticatie- en autorisatiegegevens in een geconsolideerde authenticatie- en autorisatievoorziening worden beheerd.	{prio}	{bewijs}
5	De autorisaties van gebruikers (inclusief beheerders) binnen een (web)applicatie zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet te verenigen autorisaties mogelijk is:	{prio}	{bewijs}
5a	In de applicatie zijn de autorisaties op een beheersbare wijze geordend. De applicatie maakt daartoe gebruik van autorisatiegroepen.	{prio}	{bewijs}
5b	Op basis van taken, verantwoordelijkheden en bevoegdheden zijn de niet te verenigen taken en autorisaties geïdentificeerd.	{prio}	{bewijs}

Nr.	Eis	Prio	Bewijs
5c	Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.	{prio}	{bewijs}
5d	Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerswerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.	{prio}	{bewijs}
6	Applicaties hebben een beheerinterface dat gescheiden is van de standaard gebruikersinterface. Deze scheiding komt zowel in de operationele interfaces (dat wil zeggen de deployment van de onderdelen) als in de autorisaties die toegang geven tot de interfaces tot uitdrukking. Het uiterlijk van de beheerinterface onderscheidt zich eveneens van de gebruikersinterface.	{prio}	{bewijs}
7	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.	{prio}	{bewijs}
8	Applicaties normaliseren de invoer, valideren de invoer op syntax en semantiek en normaliseren uitvoer waar dit toepasbaar is. Normaliseren en valideren van de invoer beschermt een applicatie tegen manipulatie (cross-site scripting, cross-site request forgery SQL-injectie, buffer overflow, et cetera). Normaliseren van uitvoer beschermt de ontvanger tegen manipulatie.	{prio}	{bewijs}
9	Wanneer de invoervalidatie faalt, stopt de verwerking van de betreffende invoer in zijn geheel en hervat de applicatie zijn normale functies alsof de invoer nooit ontvangen was. Het falen wordt wel zodanig gelogd dat analyse van de opgetreden situatie mogelijk is.	{prio}	{bewijs}
10	Applicaties maken gebruik van statisch geconfigureerde queries en/of commando's, waarbij parameters/variabelen zodanig worden ingevoegd dat zij de beoogde werking niet kunnen beïnvloeden. Voor databases is dit bekend als een 'prepared query'. Voor commando's is een constructie gekozen die interpretatie van een parameter/variabele door een commando interpreter/shell uitsluit. Mocht het niet mogelijk zijn hieraan te voldoen, dan wordt de waarde van elke parameter/variabele voor gebruik zodanig behandeld dat dezelfde zekerheid wordt verkregen. Te allen tijde wordt voorkomen dat vrije toegang tot het commando- of query-interface gegeven wordt. Dit geldt zowel voor waarden die door een gebruiker (in)direct worden aangeleverd, als voor waarden uit configuraties of databases.	{prio}	{bewijs}
11	Een (web)applicatie is voorzien van Concurrent Session Control, die slechts één sessie per gebruiker toestaat, tenzij onderbouwd is dat meer noodzakelijk is.	{prio}	{bewijs}
12	Een applicatie heeft een instelbare maximale sessieduur en een maximale duur van inactiviteit. Na deze periode wordt een sessie automatisch afgesloten, alsof de gebruiker zelf de sessie beëindigd heeft.	{prio}	{bewijs}
13	De maximale sessieduur en maximale inactiviteit zijn door (of namens) de opdrachtgever in te stellen. De instelbare waarden zijn per default begrenst op 10 uur (sessieduur) en 15 minuten (inactiviteit). Alleen op expliciet aangeven van de opdrachtgever kan hiervan worden afgeweken.	{prio}	{bewijs}

Nr.	Eis	Prio	Bewijs
14	Applicaties maken gebruik van gangbare protocollen en cryptografische technieken, versleutelen informatie volgens de maatregelenselectie in het IB-plan en borgen de onweerlegbaarheid van daartoe aangewezen transacties via cryptografische technieken. De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst. De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).	{prio}	{bewijs}
15	(Web)applicatie voorkomen de mogelijkheid van dynamische file includes. Indien gebruik gemaakt wordt van een applicatieserver sluit de serverconfiguratie file includes uit. Mocht het niet mogelijk zijn aan hieraan te voldoen, dan wordt voor de includes gebruik gemaakt van een vertrouwde locatie en een expliciete whitelist voor de files.	{prio}	{bewijs}
16	Applicaties hebben geen run-time afhankelijkheid van externe codebronnen.	{prio}	{bewijs}
17	Applicaties zijn gemaakt met de op het moment van uitleveren meest recente en/of door de leverancier aanbevolen versies van externe bibliotheken, raamwerken of andersoortige bouwblokken.	{prio}	{bewijs}
18	Een applicatie vangt interne fouten (excepties) af op hoofdniveau, zonder ongecontroleerd te falen (crash). Afgevangen fouten worden vastgelegd (log) en aan gebruikers wordt een melding getoond die geen inhoudelijke details bevat. Een betekenisloze referentie (code) van de fout ten behoeve van communicatie over de fout mag wel getoond worden.	{prio}	{bewijs}
19	Een applicatie heeft een uniforme en veilige wijze van applicatie-logging. De logging bevat geen inloggegevens (credentials) of vertrouwelijke gegevens over personen. Referenties (bv identifiers) zijn wel toegestaan. De logging zorgt voor traceerbaarheid van gebeurtenissen en activiteiten in relatie tot ten minste personen, systemen, applicaties en tijd.	{prio}	{bewijs}
20	Een applicatie beperkt de gebruikte protocollen, parameters (headers) en functionaliteit tot wat nodig is. Hieronder vallen ook HTTP-headers en HTTP-methoden (liefst niet meer dan GET en POST):	{prio}	{bewijs}
20a	De webserver stuurt bij een antwoord aan een gebruiker alleen die informatie in de HTTP-headers mee die van belang is voor het functioneren van HTTP.	{prio}	{bewijs}
20b	De webapplicatie toont alleen noodzakelijke informatie in HTTP-headers die van belang is voor het functioneren van HTTP.	{prio}	{bewijs}
20c	De webserver gebruikt alleen de HTTP-functionaliteiten die nodig zijn voor het functioneren van de webapplicatie.	{prio}	{bewijs}
21	De aan de gebruiker aangeboden scripts / code bevat geen commentaar, zodat die niet kunnen worden misbruikt.	{prio}	{bewijs}
22	De aan de gebruiker getoonde informatie bevat geen directory listings, zodat die niet kunnen worden misbruikt.	{prio}	{bewijs}
23	Wanneer toegang tot (de inhoud van) het filesysteem nodig is, gebeurt dit altijd onder expliciete autorisatie en controle door de applicatie.	{prio}	{bewijs}
24	In de (web)applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	{prio}	{bewijs}
{nr}	{eis}	{prio}	{bewijs}

7.2 Vertrouwelijkheid

De mate waarin een product of systeem ervoor zorgt dat gegevens alleen toegankelijk zijn voor diegenen die geautoriseerd zijn.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

7.3 Integriteit

De mate waarin een systeem, product of component ongeautoriseerde toegang tot of aanpassing van computerprogramma's of gegevens verhindert.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

7.4 Onweerlegbaarheid

De mate waarin kan worden bewezen dat acties of gebeurtenissen plaats hebben gevonden, zodat later deze acties of gebeurtenissen niet ontkend kunnen worden.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

7.5 Verantwoording

De mate waarin acties van een entiteit getraceerd kunnen worden naar die specifieke entiteit.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

7.6 Authenticiteit

De mate waarin bewezen kan worden dat de identiteit van een onderwerp of bron is zoals wordt beweerd.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

8 Onderhoudbaarheid

De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden door de aangewezen beheerders

8.1 Modulariteit

De mate waarin het systeem opgebouwd is uit losstaande componenten zodat wijzigingen van een component minimale impact heeft op andere componenten.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

8.2 Herbruikbaarheid

De mate waarin een bestaand onderdeel gebruikt kan worden in meer dan één systeem of bij het bouwen van een nieuw onderdeel.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

8.3 Analyseerbaarheid

De mate waarin het mogelijk is om effectief en efficiënt de impact, van een geplande verandering van één of meer onderdelen, op een product of systeem te beoordelen, om afwijkingen en/of foutoorzaken van een product vast te stellen of om onderdelen te identificeren die gewijzigd moeten worden.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

8.4 Wijzigbaarheid

De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden zonder fouten of kwaliteitsvermindering tot gevolg.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

8.5 Testbaarheid

De mate waarin effectief en efficiënt testcriteria vastgesteld kunnen worden voor een systeem, product of component en waarin tests uitgevoerd kunnen worden om vast te

stellen of aan die criteria is voldaan.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

9 Overdraagbaarheid

De mate waarin een systeem, product of component effectief en efficiënt overgezet kan worden van één hardware, software of andere operationele of gebruiksomgeving naar een andere.

9.1 Aanpasbaarheid

De mate waarin een product of systeem effectief en efficiënt aangepast kan worden voor andere of zich ontwikkelende hardware, software of andere operationele of gebruiksomgevingen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

9.2 Installeerbaarheid

De mate waarin het product of het systeem effectief en efficiënt geïnstalleerd of verwijderd kan worden in een gespecificeerde omgeving.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

9.3 Vervangbaarheid

De mate waarin een product een ander specifiek softwareproduct, met hetzelfde doel in de zelfde omgeving, kan vervangen.

Nr.	Eis	Prio	Bewijs
{nr}	{eis}	{prio}	{bewijs}

Bijlagen

A Terminologie en afkortingen

De onderstaande tabel bevat afkortingen en termen die regelmatig voorkomen in ICTU-documentatie.

Term/afkorting	Toelichting
actor	Persoon die of extern systeem dat een handeling verricht op het systeem.
authenticatie	Vaststellen van de identiteit van een actor.
autorisatie	Aan een actor toegekende rechten.
BIO	Baseline Informatiebeveiliging Overheid
DoD	Definition of Done
DoR	Definition of Ready
GFO	globaal functioneel ontwerp
IPO	intern projectoverleg
ISR	ICTU Softwarerealisatie
Jira	Tool om use cases, user stories, logische testgevallen en issues vast te leggen.
KPI	key performance indicator
Minimum Viable Product	De eerste versie van een product of dienst, die zo vroeg mogelijk wordt uitgerold naar de opdrachtgever. Het bevat net voldoende functionaliteit om het gestelde doel te behalen, en niet meer dan dat.
MVP	Minimum Viable Product
OTAP	Ontwikkel, Test, Acceptatie, Productie
PID	projectinitiatiedocument
PSA	projectstartarchitectuur
PvE	programma van eisen
use case	Een afgebakende eenheid van interactie tussen een actor en het systeem.
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie

B Kwaliteitsaanpak ICTU Software Realisatie

Met de verregaande automatisering en digitalisering wordt software meer en meer belangrijk, ook binnen de overheid. Naast het op orde hebben van zaken als licenties van standaardsoftware, ligt er een uitdaging als het gaat om de ontwikkeling van maatwerksoftware. Projecten waarin software wordt ontwikkeld of onderhouden kampen nog vaak met vertraging, budgetoverschrijding of een eindresultaat met te lage kwaliteit. Zo concludeerde de commissie-Elias bijvoorbeeld in haar eindrapport: '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 erkend en gemitigeerd. Dit terwijl de risico's bij de ontwikkeling van maatwerksoftware, binnen het ICT-domein, inmiddels algemeen bekend zijn en er ook voor veel risico's passende maatregelen bestaan.

ICTU werkt sinds 2010 met de agile softwareontwikkelaanpak Scrum en heeft deze aanpak aangevuld en uitgebreid om zoveel mogelijk de kans op die risico's te verminderen. Denk hierbij aan geautomatiseerde regressietesten om het risico op fouten bij nieuwe opleveringen van de software (die bij Scrum elke twee of drie weken plaatsvinden) te voorkomen. Een ander voorbeeld is het zeer frequent – meerdere keren per uur - geautomatiseerd rapporteren over de kwaliteit van de software om zogenaamde 'technische schuld' te voorkomen.

Met behulp van de ICTU Kwaliteitsaanpak Software Realisatie 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. Daarom stelt ICTU deze kwaliteitsaanpak ter beschikking aan andere partijen en overheden die zelf maatwerksoftware ontwikkelen of dit laten doen.

De kwaliteitsaanpak 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 softwareontwikkeling en -onderhoudsprojecten te vergroten. De maatregelen zijn beschreven in algemene termen; waar van toepassing is ook de ICTU-specifieke invulling van de maatregel telkens separaat bijgevoegd.

De beschrijving van de kwaliteitsaanpak is gebaseerd op de huidige aanpak van softwareontwikkeling en -onderhoud bij ICTU. De kwaliteitsaanpak evolueert op basis van praktijkervaringen bij ICTU en bij andere organisaties.