Programma
Digitaal Stelsel Omgevingswet

Non-functional requirements

Digitaal Stelsel Omgevingswet

Versie 0.55

Datum 17 December 2019
Status Definitief
Afgestemd RWS en Kadaster

Colofon

Programma Digitaal Stelsel Omgevingswet

Contactpersoon

Bas Crompvoets
Domeinarchitect Digitaal Stelsel Omgevingswet
M +31(0)6-55884797
bas.crompvoets@rws.nl

Victorine Binkhorst
Lead architect Digitaal Stelsel Omgevingswet
M +31(0)6-51397648
Victorine.binkhorst@rws.nl

Versie

0.55

Auteur

Bas Crompvoets
Domeinarchitect Digitaal Stelsel Omgevingswet
M +31(0)6-55884797
bas.crompvoets@rws.nl

Victorine Binkhorst
Lead architect Digitaal Stelsel Omgevingswet
M +31(0)6-51397648
Victorine.binkhorst@rws.nl

1 Inleiding

Ten behoeve van eis BEH01 uit het Globaal Programma van Eisen (GPvE) worden in dit document de product kwaliteitseisen geformuleerd waarbinnen de realisatie en het beheer van het Digitaal Stelsel Omgevingswet plaats dient te vinden. Deze eisen worden non-functionele eisen of non-functional requirements genoemd. Gebaseerd op IT 'best practices' leidt dit tot een kwalitatief hoogwaardig systeem.

In de opbouw van dit document zal in eerste instantie nader worden ingegaan op (product-)kwaliteit en het ISO kwaliteitsraamwerk. Vervolgens wordt gekeken hoe kwaliteitseisen ook daadwerkelijk getoetst kunnen worden door middel van testen. Ook wordt de relatie met de hogerliggende OGAS architectuurprincipes beschreven. Vervolgens worden in aparte hoofdstukken de concrete eisen met normen per kwaliteitscategorie beschreven.

Vooralsnog is voldoen aan de eisen gericht op de fase permanent beheer. Op basis van de belangrijkste productrisico's en gebruikers-/beheerdersbehoefte kunnen de eisen volgtijdelijk worden geïmplementeerd (groeimodel).

2 Kwaliteit

Kwaliteit is het geheel van eigenschappen dat aangeeft in welke mate het geschikt is voor het bedoelde gebruik (‘fitness for use’). Een maat hiervoor is de mate waarin aan de verwachtingen van de gebruiker/klant wordt voldaan. Deze verwachtingen zijn vastgelegd in requirements en vertaald in specificaties. ‘Conformance to requirements’ is dan het kwaliteitscriterium dat gemeten kan worden.

Requirements zijn echter te verdelen in de ‘uitgesproken’ en de ‘vanzelfsprekende’ of impliciete (‘I know it when I see it’) requirements. De mate waarin de vanzelfsprekende (maar niet herkende of geïmplementeerde) requirements leiden tot een grote kloof in verwachtingen is één van de grootste valkuilen van systeemontwikkeling. Een testproces op basis van toetsbare requirements kan het risico van deze kloof verkleinen en daarmee de ‘herstelkosten’ om de kloof te overbruggen.

Daarnaast is een gedefinieerde productkwaliteit essentieel voor het goed kunnen uitvoeren van beheer. Daarom kunnen beheerpartijen additionele non-functional requirements opstellen als acceptatie eisen. Dit is een zogenaamde whitebox aanpak waarbij ‘in’ het opgeleverde product wordt gekeken versus de blackbox aanpak waarbij slechts naar de dienstverlening met het product wordt gekeken op basis van een service level agreement. De whitebox aanpak wordt gehanteerd ook in dienstverleningssituaties gehanteerd indien de behoefte aanwezig is om op lange termijn de bestendigheid van het dienstverleningsniveau te borgen.

In het algemeen zijn ‘uitgesproken’ requirements meer functioneel van aard en ‘vanzelfsprekende’ meer non-functioneel (in ieder geval vanuit klantperspectief), hoewel dit een grove versimpeling is van de realiteit aangezien er voldoende goede voorbeelden zijn van uitgesproken non-functionele en vanzelfsprekende functionele requirements.

Door in ieder geval ook non-functionele requirements zo goed mogelijk te specificeren wordt het risico van uiteenlopende verwachtingen verkleind. Echter in alle gevallen geldt dat om verwachtingen zo goed mogelijk te matchen met de actualiteit de kwaliteit gemeten dient te worden. Hiervoor zijn standaardmodellen om requirements concreet (SMART) te maken. In het volgende hoofdstuk wordt het ISO kwaliteitsraamwerk nader beschreven.

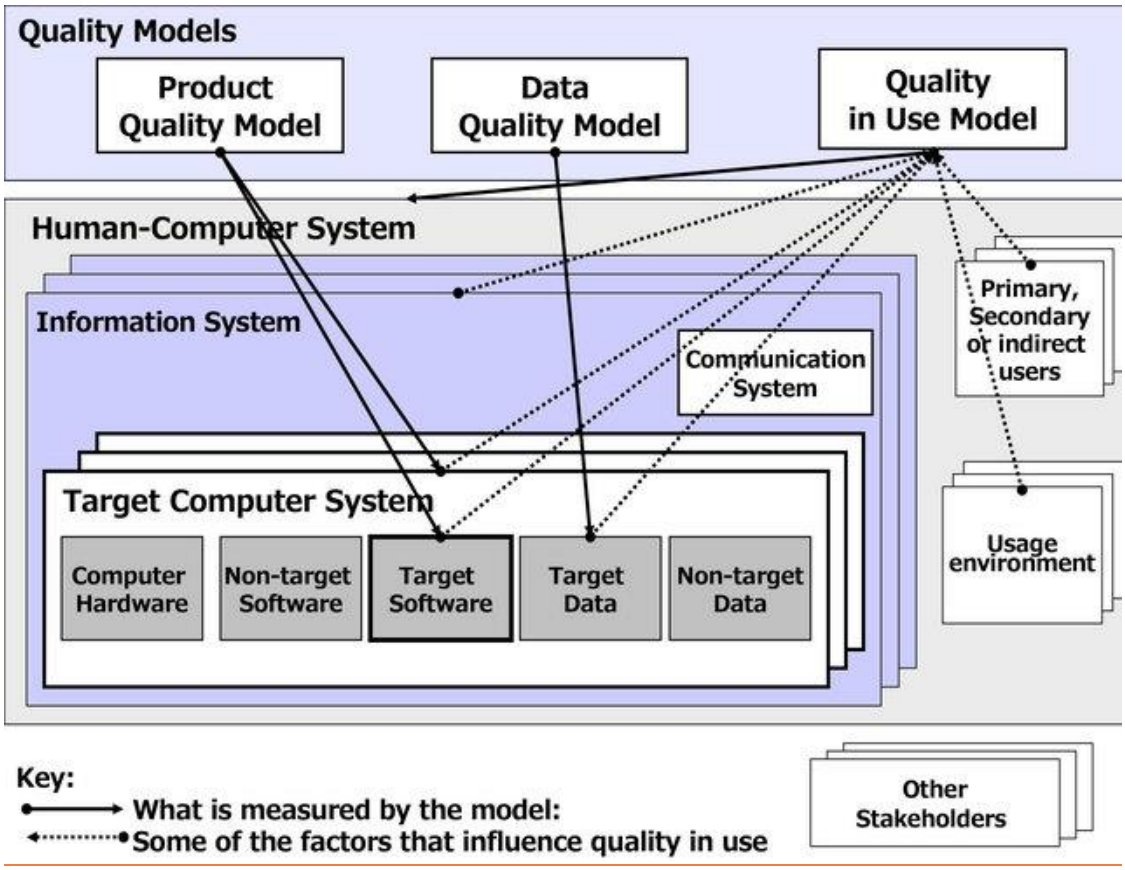
3 ISO kwaliteitsraamwerk

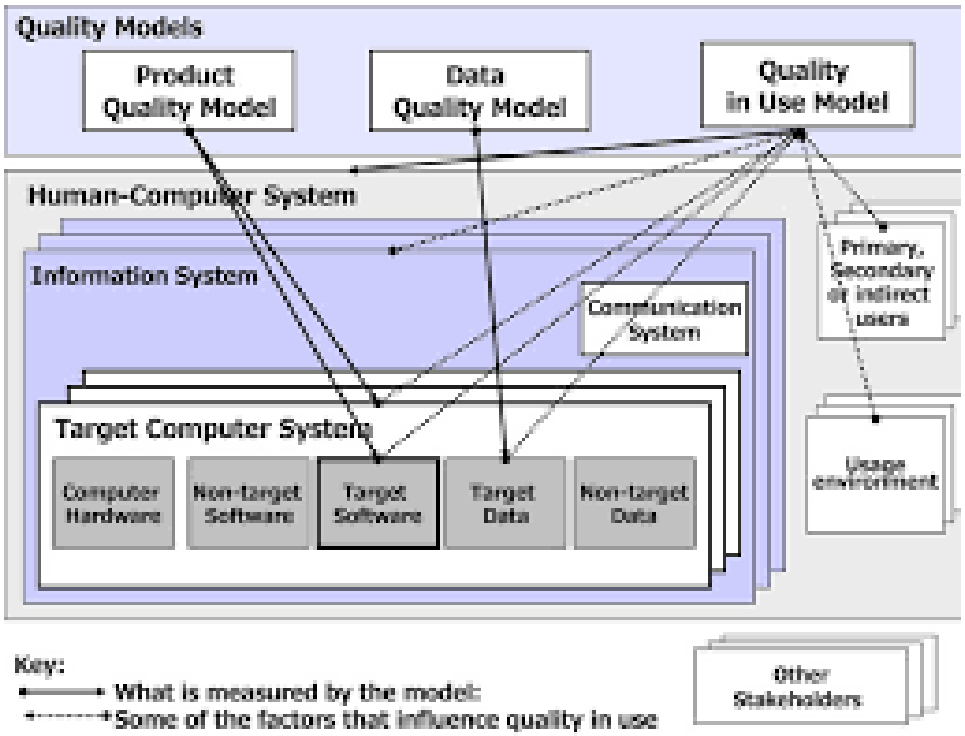
Een veelgebruikte standaard die als referentie kan dienen voor productkwaliteit is ISO25010 (opvolger van ISO9126). Deze is onderdeel van de SQuaRE (Software product Quality Requirements and Evaluation) serie van standaarden. Dit is de reeks ISO 250xx standaarden.

Binnen ISO 25010 zijn er twee kwaliteitsmodellen gedefinieerd, software product kwaliteit en kwaliteit van systeem gebruik (quality in use). Productkwaliteit zijn de (statische en dynamische) eigenschappen die intrinsiek onderdeel zijn van computer software of systeem. Kwaliteit tijdens gebruik dekt de bredere scope van de interactie van gebruikers met software en computer systemen (in een bepaalde context) af.

In dit document wordt de scope beperkt tot productkwaliteit en wordt kwaliteit tijdens gebruik (quality in use) niet meegenomen.

Tevens is binnen ISO 25012 een data kwaliteitsmodel gedefinieerd dat complementair is aan ISO25012. Voor toepassing binnen Informatiehuizen is een separate analyse gemaakt hoe dit model toe te passen en op welke manier er SMART requirements kunnen worden gedefinieerd. Binnen DSO wordt ook gekeken op welke manier het toepasbaar kan worden gemaakt.





ISO25010 is een referentiemodel omdat blijft gelden dat de risicoanalyse leidend is. Op basis van een risicoanalyse wordt daadwerkelijk bepaald welke (test-)maatregelen in welke intensiteit worden getroffen. Dit is een kosten/batenanalyse op basis van de kosten van de risicomaatregelen (zoals testen) en de kosten van het optreden van het risico (kans x impact).

4 Toepassing

Dit document is een uitwerking van eis BEH01 uit het Globaal Programma van Eisen voor het DSO (de Informatiehuizen en Generieke Gegevensvoorzieningen worden alleen qua aansluiting gedekt). "De digitale voorzieningen binnen het DSO voldoen aan de kwaliteitseisen van softwareproducten volgens ISO 25010. Hiertoe worden deze kwaliteitseisen nader gespecificeerd per component".

Naast deze algemene eis kent het GPvE nog een aantal andere expliciete non-functional eisen. Deze zijn hieronder weergegeven en verder door vertaald naar de eisen in dit document. Waar noodzakelijk wordt een voorstel gedaan om de bestaande eisen aan te passen; dit wordt in overleg met de opdrachtgever verder uitgewerkt.

Nr	*Eis*	*Wet*	*Visie*	*Scen.*	*Fase 1*	*Fase 2*
ARC02	*Er wordt een generiek zorgplicht raamwerk opgesteld waarmee per stelselcomponent bepaald kan worden voor welke informatieobjecten (waaronder gegevens, informatieproducten, berichten, gebruikerstoepassingen) de zorgplicht geldt (en welke partij deze zorgplicht heeft) en welke maatregelen hierbij horen. Maatregelen zijn gebaseerd op zorgplichtniveaus die op hun beurt weer bepalen welke maatregelen genomen moeten worden voor het Duurzaam Toegankelijk maken van de informatie. Voor het bepalen van de maatregelen wordt aangesloten bij de bestaande werkwijze en diensten van het Nationaal Archief.*	*-*	*[C5]*	*1*	*M*	*M*
BEH02	*Er wordt een Service Level Agreement (SLA) opgesteld met daarin tenminste afspraken over: performance (in relatie tot verwachte volumes), servicedesk, incident management, change management en probleem management conform ITIL, ASL en BiSL.*	*-*	*[B4] 5.7.1*	*2*	*M*	*M*
BEH04	*Het loket is 24 uur, 7 dagen per week open, m.u.v. gepland onderhoud. Alle gebruikerstoepassingen zijn dan voor alle gebruikers beschikbaar.*	*-*	*[A3] 3.2*	*2*	*S*	*M*
BEH05	*De centrale helpdesk is open tijdens het service window, zijnde van 8.00 uur tot 19.00 uur op werkdagen en van 10.00 tot 16.00 uur op zaterdag, zondag en nationale feestdagen (*)*	*-*	*[A3] 3.2*	*2*	*S*	*M*
BEH06	*Het beschikbaarheidswindow van het loket is van 06.00-24.00 uur, 7 dagen per week.*	*-*	*[A3] 3.2*	*2*	*S*	*M*
BEH07	*Gedurende het beschikbaarheids window zoals genoemd in BEH06 is het loket minimaal 99,8% van de tijd beschikbaar.*	*-*	*[A3] 3.2*	*2*	*S*	*M*
LOK03	*Het loket voldoet aan de webrichtlijnen van de Nederlandse overheid en is voorbereid op de webrichtlijnen van de Europese Unie.*	*-*	*[D3] 6*	*1*	*M*	*M*

(*) hiervoor is een alternatief voorstel in de maak met alleen ma-do van 8-20 en vr 8-17 openstelling.

Als startpunt worden de non-functional requirements op stelselniveau geformuleerd. Dit omdat voor een stelsel dat zo uitgebreid en divers is als DSO niet alle non-functional requirements ‘op maat’ van iedere component direct kunnen worden gespecificeerd. Als requirements niet van toepassing zijn (of een andere invulling dienen te krijgen) kan middels het ‘pas-toe-of-leg-uit’ principe worden uitgelegd waarom deze niet binnen de scope valt of een andere invulling beter recht doet aan het kwaliteitsdoel.

Anderzijds dienen requirements waar nodig op componentniveau een nadere detaillering te vergen om deze in context van de toepassing SMART te maken. Dit zal in de PSA plaatsvinden. Indien nodig kunnen in een master testplan ook de omgevingsomstandigheden die bij de acceptatietest zullen gelden nader worden gespecificeerd. De samenvattende beschrijving hier laat geen ruimte voor al deze details.

Ter ondersteuning is de nummering van de NFR’s uitgebreid met een indicatie van de beoogde scope van de betreffende NFR (P=project, S=Stelselbreed en E=Extern).

De vertaling van principes en kaders naar non-functional requirements is een iteratief proces tussen opdrachtgevers, -nemers en beheerders in een brede discussie over kwaliteit, risico’s, marktconformiteit en kosten.

Let op. Doel is niet iedere NFR zelf, maar om de formulering van de NFR te gebruiken om de ‘engineering’ kwaliteit van software en systemen te verhogen op het gebied van performance, betrouwbaarheid, beveiliging enz.

5 Testen

Om de productkwaliteit te kunnen verifiëren wordt er getest. Testen is feitelijk risicomanagement:

> *Testing is a process of planning, preparing, executing and analyzing, aimed at establishing the characteristics of an information system, and demonstrating the difference between the actual status and the required status. Testing reduces the level of uncertainty about the quality of a system. The level of testing effort depends on the risks involved in bringing this system in to operation, and on the decision of how much time and money is to be spent on reducing the level of uncertainty*

Feitelijk wordt dus met testen het verschil tussen feitelijke en gewenste kwaliteit bepaald zodat actie kan worden ondernomen om de feitelijke kwaliteit minimaal op het gewenste niveau te krijgen. NFRs dienen dus voldoende SMART te zijn dat er voor iedere NFR een toets, test, inspectie, audit of ander kwaliteitsmeting instrument kan worden gedefinieerd. Alleen dan wordt kwaliteit hanteerbaar gemaakt. Een niet verifieerbare requirement is feitelijk 'waste'.

De essentie is om de testinspanning te relateren aan de verwachte productrisico's voor de business. Een productierisico is de kans dat het product faalt in relatie tot de verwachte schade wanneer dit optreedt.

- Productrisico = faalkans * schade
- Faalkans = foutkans * frequentie van gebruik

Schade: omzet verlies, schade aan derden, economisch verlies, fysieke schade, milieuschade, imagoschade, klantverlies, verlies van vertrouwen, overbelasting helpdesk, enz. Schade wordt onderverdeeld in directe (bijvoorbeeld omzet en economisch verlies) en indirecte schade (bijvoorbeeld imagoschade en verlies van klantvertrouwen).

Foutkans: De waarschijnlijkheid dat een storing zal optreden in een systeem of programma in een bepaald tijdsverloop. De verwachtingswaarde van optreden van fouten is dus het gemiddeld aantal storingen per tijdseensheid (gemeten over een representatieve periode)

De foutkans stijgt bij complexe functies, nieuwe functies, veelvuldig aangepaste functies, functies die gebouwd zijn met nieuwe tools of technieken, functies die gedurende de ontwikkeling aan anderen zijn overgedragen, functies waarin al eerder veel fouten zijn gevonden, functies met veel interfaces. De risico's worden in kaart gebracht op basis van een productrisicoanalyse (PRA). Hierin kan op aspecten worden bepaald wat de impact op de business is bij onvoldoende functioneren van een (component van een) informatiesysteem op een kwaliteitsaspect. Bijvoorbeeld als een callcenter medewerker 10 sec. i.p.v. 2 sec. moet wachten totdat klantgegevens op het scherm worden getoond.

Op basis hiervan kan de teststrategie worden gekozen, de planning en begroting worden opgesteld en de testsoorten worden gekozen waarna de test kan worden uitgevoerd. Startpunt van een productrisicoanalyse (PRA) kan een risico inschatting zijn die wettelijk verplicht is of beleidsmatig vastgesteld zoals een BIV classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) uit een BIA (Business Impact Analyse). Andere risicomethodes zoals QuickscanBIO of IRAM kunnen ook worden gebruikt.

In principe is voor ieder kwaliteitseigenschap (-attribuut) een bijbehorende testsoort te bedenken. Op basis van de risicoanalyse is van belang dat de dekking voldoende is en aangetoond kan worden. Dekking is de verhouding tussen datgene wat (grosso modo) getest kan worden en datgene wat met de testset getest wordt.

- dekkingsvorm: de vorm (testsoorten) waarin het afdekken van de te testen situaties die afleidbaar zijn uit de testbasis uitgedrukt wordt.

- dekkingsgraad: het percentage van de door de dekkingsvorm bepaalde testsituaties dat door de test gedekt is.

6 OGAS Architectuurprincipes.

Dit hoofdstuk herhaalt de 10 OGAS Architectuurprincipes uit het hoofddocument van de OGAS. Deze principes zijn de verbinding tussen de principes op het niveau van de Doelarchitectuur en de doorvertaling naar de onderliggende GAS-en. Het is het vertrekpunt voor de kaders- en richtlijnen waaraan de realisatie en beheer van het Digitaal Stelsel Omgevingswet gehouden is. De implicaties van deze principes komen concreet tot uiting in de vorm van de toetsbare non-functional requirements zoals in dit document geformuleerd.

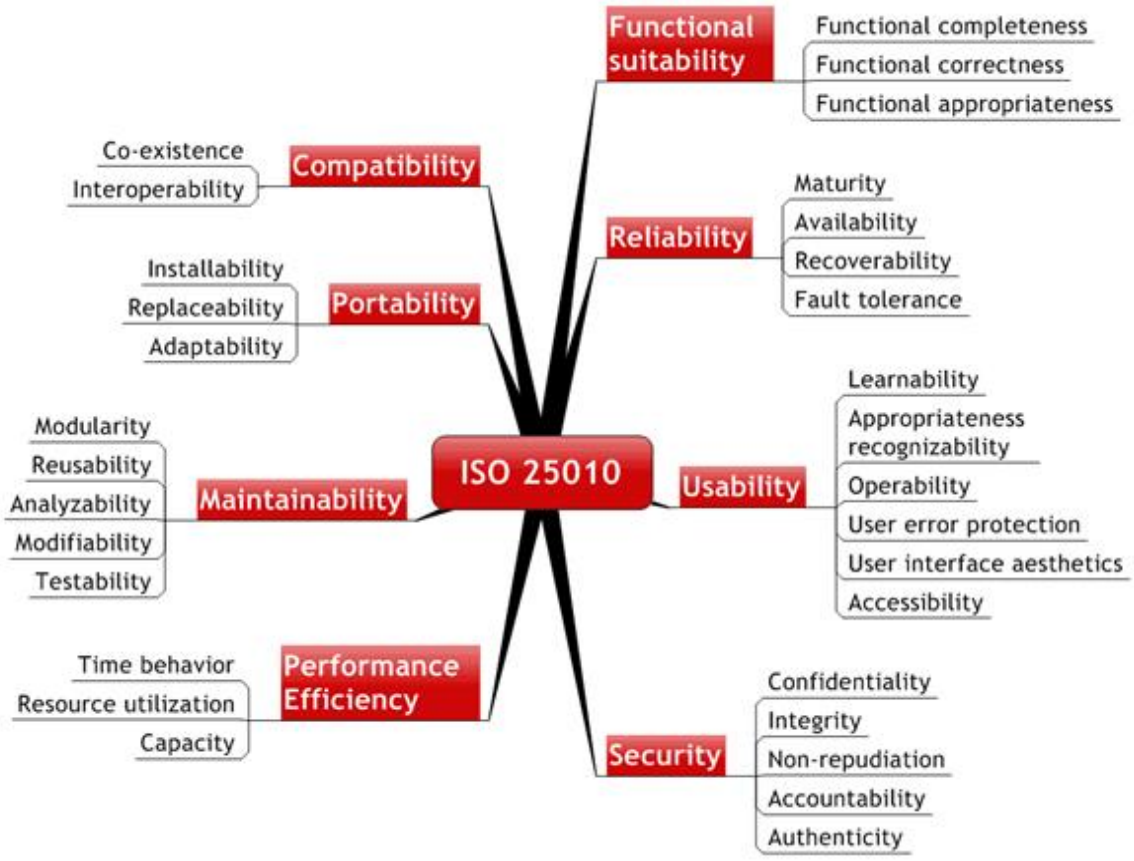
Hieronder volgt de opsomming van de 10 OGAS architectuurprincipes:

Identificatie & Categorie	Statement
DSO1 - BA	De klant staat centraal.
DSO2 - BA	Het stelsel functioneert als 1 geheel voor zowel personen als systemen.
DSO3 - IA	Data is de brandstof van het stelsel.
DSO4 - IA	Oplossingen zijn eenvoudig, generiek en kosten effectief.
DSO5 - IA	Alles is een service.
DSO6 - IA	Het stelsel is open, transparant en innoverend.
DSO7 - IA	Hergebruik voor koop voor maak
DSO8 - BP	Continuïteit en compliance is geborgd.
DSO9 - BP	Passende beveiliging & privacy op basis van reële risico’s.
DSO10 - BH	Beheerfunctionaliteit is primaire functionaliteit

Legenda BA=Business Architectuur, IA=Informatie Architectuur, BP=Beveiliging & Privacy, BH=Beheer.

7 Non-functional requirements.

Zoals hierboven aangegeven wordt als rubricering (conform GPvE) het ISO25010 kwaliteitsraamwerk toegepast. Naast een korte opsomming van de subcategorieën hieronder is de definitie van iedere individuele ISO 25010 kwaliteitseigenschap in de bijlage opgenomen.



Naast de productkwaliteit eisen zijn er ook de eisen aan proces, organisatie en afspraken (SLA's). Die worden aan de eigenaren, afnemers, beheerders en leveranciers van DSO gesteld en niet aan de voorzieningen. Deze behoren daarom niet binnen de scope van dit document.

8 Prestatie efficiency (performance efficiency)

Principes(s):
DSO1, 2, 8

Onderwerpen:
Snelheid, Middelenbeslag en Capaciteit

Kaders:

Wetgeving:
Geen

Doelarchitectuur:

Eisen / Non-functional requirements

Nr.	NFR	Test
1SPE	De responsetijd van de webinterface voor pagina's met eenvoudige verwerking bedraagt maximaal 0,5sec voor 80% van de schermen. En maximaal 3 seconden voor 95% van de schermen.	Performance test
2SPE	De responsetijd van de webinterface voor pagina's met complexe verwerking bedraagt maximaal 1,0 sec voor 80% van de schermen. En maximaal 5 seconden voor 95% van de schermen.	Performance test
3P	Indien een eenvoudige of complexe verwerking langer duurt dan respectievelijk 3 of 5 sec wordt feedback aan de gebruiker gegeven.	Functionele / Usability test
4SPE	Er kunnen op enig moment gelijktijdig tijdens openstelling 100 interactieve gebruikers (ingelogd) via de DSO gebruikerstoepassingen en 250 service afnemende gebruikers (via apps en andere toepassingen) actief zijn. Het aantal is 5-10x groter voor alleen leesacties van niet-ingelogde gebruikers.	Loadtest
5SP	De throughput van representatieve vergunning-aanvragen/meldingen bedraagt minimaal de huidige OLO2 throughput + 100% (is totaal plusminus 7500 per week).	Flow test
6S	De latency (responstijd) van een service (intern en extern) bedraagt maximaal 0,5sec voor 90% van de serviceaanroepen.	Performancetest
7P	De knooppunt resources (incl. connecties) dienen tot maximaal 80% van de beschikbare resources vol te lopen.	Stresstest
8P	Bij piekbelasting van het knooppunt is de verwerkingstijd van vergunningaanvraag/melding maximaal 50% boven de reguliere verwerkingstijd (te meten bij 50% belasting).	Mixed workload performance test
9S	De fair use workload van het Open Stelsel door Derden beïnvloedt niet de noodzakelijke workload van de	Mixed workload performance test

	services van de landelijke voorziening voor DSO ketenprocessen.	
10S	Afwijkend gedrag van gebruikers bij 'anonieme' functionaliteiten zoals checken en oriënteren mag geen invloed hebben op de niet anonieme functionaliteiten.	Mixed workload test
11P	Bij toevoegen van verwerkingscapaciteit neemt de daadwerkelijke verwerking vrijwel lineair toe.	Performance test

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: performance test, loadtest, mixed workload performancetest, stresstest.

Opmerkingen/Openstaande punten

- Hoe fair use definieren om te kunnen toetsen?

9 Uitwisselbaarheid (Compatibility)

Principes(s):
DSO8

Onderwerpen:
Beinvloedbaarheid en Koppelbaarheid (Interoperabiliteit)

Kaders:

Wetgeving:
Geen

Doelarchitectuur:

Eisen / Non-functional requirements

Nr.	NFR	Test
1	Software componenten zijn ontwikkeld om op het Standaard Platform (SP) te kunnen draaien, tenzij afwijking hiervan is overeengekomen.	Architecture review
2	Software componenten kunnen binnen redelijke tijd (1 à 2 weken) worden aangepast om op een willekeurig cloudplatform te draaien door middel van containertechnologie (12factor.net richtlijn). De afhankelijkheden dienen in kaart te zijn gebracht.	Architecture review
3S	Service aanroepen van binnen en buiten stelsel functioneren technisch correct over de voor DSO toegepaste software platforms c.q. technologische omgevingen heen.	Architecture review
4S	Software componenten worden ontwikkeld conform de DSO API/URI strategie en de DSO gedefinieerde lijst van (technische) standaarden(*).	Compliance test

(*) Dit is de formeel vastgestelde standaardenlijst (van project PR07). De marktconforme daadwerkelijk geïmplementeerde subset van de standaard geldt daarbij als norm.

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: infratest.

10 Bruikbaarheid (Usability)

Principes(s):
DSO1, 10

Onderwerpen:
Herkenbaarheid van geschiktheid, Leerbaarheid, Bedienbaarheid

Kaders:

Wetgeving:
Geen

Doelarchitectuur:

Eisen / Non-functional requirements

Nr.	NFR	Test
1P	Eindgebruikers dienen zonder training en zeer beperkte helpondersteuning de basistaken binnen gebruikerstoepassingen te kunnen uitvoeren. Complexiteit kan voor de gebruiker worden verborgen indien dit voor de specifieke taakuitoefening niet relevant is.	Usabilitytest
2S	De toegankelijkheid van het publieke deel van het loket en de gebruikerstoepassingen moet voldoen aan de DSO huisstijl, de richtlijnen gesteld in de norm "Digitale Toegankelijkheid" (WCAG, GPvE LOK03), in het Nederlands zijn en begrijpelijk voor eenieder met taalniveau B1.	IJkpunten Drempelvrij level 3 toets
3P	Een nieuwe berichtenstroom (op het knooppunt) dient binnen 1 dag toegevoegd te kunnen worden.(*)	Usabilitytest
4S	Een nieuwe stelselbeheerder (medior) dient na 1 week (knooppunt-)basistaken te kunnen uitvoeren.(*)	Audit
5S	Een nieuwe stelselbeheerder (medior) dient na 1 maand (knooppunt) complexe taken te kunnen uitvoeren.(*)	Audit
6P	Een nieuwe aanbieder/afnemer van services dient na 1 dag basistaken te kunnen uitvoeren.	Usabilitytest
7S	De layout is vormgegeven conform DSO Stijlgids en UI richtlijnen.	Audit

(*) hoewel dit proceseigenschappen lijken gaat het in deze context om de eigenschap van het product dat de beheerder in staat stelt binnen een bepaalde tijd bepaalde werkzaamheden te verrichten.

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: usabilitytest, mouse of eyeball tracking test

11 Betrouwbaarheid (Reliability)

Principes(s):
DSO2, 8

Onderwerpen:
Volwassenheid, Beschikbaarheid, Foutbestendigheid, Herstelbaarheid

Kaders:

Wetgeving:
Geen

Doelarchitectuur:

Eisen / Non-functional requirements

Nr.	NFR	Test
1S	Iedere stelselcomponent moet active/active kunnen draaien. Er zijn hiervoor geen technische of architecturele belemmeringen.	Bedrijfszekerheidstest
2S	Bij het parallel schakelen van componenten werken ze in een twin-datacentre infrastructuur configuratie.	Bedrijfszekerheidstest
3SP	Ketens en 'reliable' berichtstromen zijn 'resilient' tegen uitvallen van parallel geschakelde componenten.	Bedrijfszekerheidstest
4SP	Teruggang naar herstart en/of terugrolmomenten geschiedt zonder data/berichtverlies (idempotentie).	Rollback/Restoretest
5S	QoS kan ten behoeve van SLA's worden afgedwongen. Services die noodzakelijk zijn voor interactief gebruik van eindgebruikers hebben in principe voorrang op andere services.	Mixed workload test
6S	De belasting van het open stelsel wordt technisch gelimiteerd zodanig dat deze de QoS van de landelijke voorziening niet negatief beïnvloedt.	Architecture review Mixed workload test
7S	Bij een calamiteit is de RPO (recovery point objective) 15 min in x% van de gevallen.	Rollback/Restoretest
8S	Bij een calamiteit is de RTO (recovery time objective) 4 uur in x% van de gevallen. Deze tijdsperiode geldt vanaf recoverybesluit tot vrijgave voor sanitytest.	Rollback/Restoretest
9SP	Applicatie beschikbaarheid(*) is 99,8% tijdens opstellingsuren conform GPvE (zie H3) en 99,5 % daarbuiten (niet meegerekend ingepland periodiek onderhoud buiten openstelling).	Bedrijfszekerheidstest
10S	Platform beschikbaarheid is 99,9%.	Audit
11S	Infrastructuur (datacentre/hosting) beschikbaarheid is conform Tier 3 normen, minimaal 99,98% en maximaal 1,6uur downtijd per jaar.	Audit
12S	Een volledige stilstand en weer opstarten van de landelijke voorziening (stop/start) mag maximaal 30 minuten duren (incl. correct afsluiten van sessies).	Rollbacktest/Restoretest

13P	Een volledige stilstand en weer opstarten van een component van de landelijke voorziening (stop/start) mag maximaal 20 minuten duren.	Bedrijfszekerheidstest
14S	De (user-)interfaces bevatten op iedere parameterlijst of scherm-/interfacecontrol validaties om (invoer-)fouten te voorkomen.	Functionele test

(*) % beschikbaarheid is 100% minus de ongeplande niet-beschikbaarheid in uren ten opzichte van de openstellingsuren (=het toegankelijk zijn van de functionaliteit voor een geautoriseerde gebruiker).

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: bedrijfzekerheidstest (failovertest), backup/restore test, rollbacktest.

Opmerkingen/Openstaande vraagstukken

N.B. De Indien een enkelvoudige component Cx een beschikbaarheid p1 heeft (stel p1 is 98%), dan heeft:

- Een keten met 2 serieel geschakelde componenten C1 en C2 met beschikbaarheid p1 en p2 als beschikbaarheid p1 x p2 (dus 98% x 98% = 96%).
- Een keten met 2 parallel geschakelde componenten C1a en C1b met beschikbaarheid p1a en p1b als beschikbaarheid (1-(1-p1a) x (1-p1b)), (dus 1- (100%-98%) x (100%-98%) > 99,9%).
- Een keten van 2 serieel geschakelde parallelle component C1a,b en enkelvoudige component C2 met beschikbaarheid p1a, p1b en p2 (allen 98%) als beschikbaarheid 98% x 99,996% = 97,96% Zijnde afgerond 98%.

12 Beveiligbaarheid (Security)

Principes(s):
DSO9 - Passende beveiliging & privacy op basis van reële risico's.

Onderwerpen:
Vertrouwelijkheid, Integriteit, Onweerlegbaarheid, Verantwoording, Authenticiteit

Kaders:

Wetgeving:
VIR, VIR-BI, BIO, AVG.

Doelarchitectuur:

DSO9	APNORA40	De berichtenuitwisseling is onweerlegbaar.
DSO9	APDSO17	De classificatie van de gegevens bepaalt de sterkte van het authenticatiemiddel.
DSO9	APDSO18	De beveiliging wordt ingericht op basis van afweging van risico's in de keten.
DSO9	APDSO19	De beveiliging wordt ingericht op basis van afweging van bruikbaarheid en beheerbaarheid.
DSO9	APDSO20	Security en privacy by design.

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: pentest (aka penetratietest, hackerstest), secure code review, configuration review.

Eisen / Non-functional requirements

Standaarden en normen

Nr.	NFR	Test
1S	Er is een ISMS conform ISO 27001 ingericht.	Audit
2S	Beveiligingsmaatregelen zijn conform ISO27002 + BIO R-maatregelen opgezet. Privacy maatregelen conform de AVG.	Audit
3SP	Er is een Business Impact Analyse (of vergelijkbaar) met BIV classificatie.	Toets
4P	Er is een Product Risico analyse (of vergelijkbaar) beschikbaar voor ieder stelselonderdeel.	Toets
5P	Ieder architectuur-/(technisch-)ontwerpdocument en zeker OGAS, GAS, PSA (evt. SA) heeft een sectie waarin Beveiliging en privacy is uitgewerkt (conform best practices).	Toets

Technische normen

Nr.	NFR	Test
1SP	Externe communicatie op netwerkniveau is geheel TLS / HTTPS (exacte versies op de standaardenlijst).	Test / Pentest
2SE	Webfacing stelselcomponenten zijn hackproof conform OWASP normen (of aantoonbaar gelijkwaardig).	Pentest
3P	Softwarecode voldoet aan de secure coding richtlijnen van CIP en NCSC (of aantoonbaar gelijkwaardig).	Secure code review

4P	Hashcodes ten behoeve van onweerlegbaarheid zijn minimaal SHA-256	Toets
5S	Er is een duidelijke scheiding van vertrouwde en niet vertrouwde zones door middel van compartimentering op alle niveau's (netwerk tot applicatie).	Configuration review

Verantwoording (*)

Nr.	**NFR**	**Test**
1SP	Iedere stelselcomponent schrijft mutaties en gebeurtenissen in auditlog (conform H10.10 BIR2017 / BIO H12)	Test
2P	Ieder uitgaand bericht (met rechtsgevolgen) wordt gearchiveerd.	Test
3P	Inkomende berichten (met rechtsgevolgen) die niet slechts leesoperaties zijn worden gearchiveerd.	Test

(*) Zie ook de eisen in het GPvE onder 2.5 en KNP8, 9 en 10.

13 Onderhoudbaarheid (Maintainability)

Principes(s):
DSO8

Onderwerpen:
Modulariteit, Herbruikbaarheid, Analyseerbaarheid, Wijzigbaarheid, Testbaarheid.

Kaders:

Wetgeving:
Geen

Doelarchitectuur:

Eisen / Non-functional requirements

Nr.	NFR	Test
1P	Codekwaliteit voldoet minimaal aan SIG 3,5* of aantoonbaar vergelijkbaar.	Audit/codescan
2P	Unittest coverage is minimaal 80% (*)	Audit/codescan
3S	Een prio2 incident conform de prioriteitsincident indeling dient door een medior applicatie/systeembeheerder binnen 1 dag geanalyseerd te kunnen worden tot een juist oplossingsvoorstel. Hiervoor zijn adequate loggegevens beschikbaar.	Exploitatietest
4S	Eenvoudige storingen moeten binnen 1 uur technisch geanalyseerd kunnen worden qua systeemopzet (**).Hiervoor zijn adequate loggegevens beschikbaar.	Exploitatietest
5SP	Bij aanbrengen van wijzigingen dient 99,9% van de niet gewijzigde onderdelen onveranderd gedrag te vertonen.	Regressietest

(*) Alle broncode moet met unit tests worden getest, tenzij de broncode op een andere manier automatisch getests wordt (bv in systeem test). Elke unit test moet controles uitvoeren op juist gedrag na uitvoeren van de unit onder test. Een indicator van goede coverage is een waarde van 80% of hoger.
(**) Eenvoudig is hier niet smart gedefinieerd maar moet worden geïnterpreteerd als een storing in 1 component die bijvoorbeeld veroorzaakt wordt door een enkele bug of configuratiefout. Analyse

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: codekwaliteitstest/scan, testcoverage analyse, exploitatietest.

14 Overdraagbaarheid (Portability)

Principes(s):
DSO5, 8

Onderwerpen:
Aanpasbaarheid, Installeerbaarheid, Vervangbaarheid

Kaders:

Wetgeving:
Geen

Doelarchitectuur:

Eisen / Non-functional requirements

Nr.	NFR	Test
1P	Een nieuwe installatie/deployment in een 'schone' omgeving van een software-/standaardcomponent dient binnen 4 uur te kunnen geschieden.	Installatietest
2P	Testscripts voor één component ten behoeve van geautomatiseerd testen zijn overdraagbaar over de omgevingen van een OTAP straat.	Sanitytest
3S	Componenten dienen binnen 5 werkdagen naar een identiek cloudplatform (PAAS) in een ander rekencentrum te kunnen worden gemigreerd.	Audit / Regressietest
4S	Componenten zonder containerondersteuning dienen binnen 3 maanden naar een alternatief cloudplatform te kunnen worden gemigreerd.	Audit / Architecture review / Regressietest
5S	Componenten gebruiken herbruikbare bouwblokken die binnen DSO ter beschikking worden gesteld (*)	Architecture review
6S	Er wordt gebruik gemaakt van volwassen en gangbare ontwikkeltechnologie met een breed ontwikkelaarsdraagvlak.	Architecture review
7S	Software componenten die een frontend functionaliteit implementeren kunnen middels een standaard browser op een werkstation of mobiel apparaat worden uitgevoerd zonder dat de gebruiker hiervoor add-ons/plug-ins hoeft te installeren.	Architecture review

(*) 1) Het copyright van een herbruikbaar component ligt altijd bij een overheidsinstelling.
2) De herbruikbare componten worden vrijgegeven onder een (open source) licentie die aansluit bij het licentie gebruik van de gebruikers van de componenten.

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: installatietest, sanitytest.

15 Functionele geschiktheid (functional suitability)

Principes(s):
DSO1

Onderwerpen:
Functionele compleetheid, -correctheid en toepasbaarheid

Kaders:

Wetgeving:
Omgevingswet, wet Digitale Overheid

Doelarchitectuur:

Eisen / Non-functional requirements

Nr.	NFR	Test
1S	De functionele acceptatietest (FAT) verifieert dat de eindgebruiker alle handelingen die nodig worden geacht voor alle in het GPvE beschreven functionele requirements kan uitvoeren zonder blokkades of work-arounds.	FAT / Ketentest
2S	De gebruikersacceptatietest (GAT) is geslaagd indien alle, samen met de gebruikers, opgestelde testgevallen zonder kritische (prio-1,2) bevindingen zijn doorlopen.	GAT

Toetsmethoden

Algemeen: audit, toets, (functionele-) test, (architecture) review.
Specifiek: functionele acceptatie test, gebruikers acceptatie test, usability test.

16 Bijlage A: ISO 25010 Toelichting

Onderstaand een overzicht van de ISO25010 kwaliteitsatributen:

16.1 Productkwaliteit (Product quality)

16.1.1 Functionele geschiktheid (Functional suitability)

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

- Functionele compleetheid (Functional completeness)
  De mate waarin de set van functies alle gespecificeerde taken en gebruikersdoelen afdekt.
- Functionele correctheid (Functional correctness)
  De mate waarin een product of systeem de correcte resultaten met de gewenste mate van nauwkeurigheid levert.
- Functionele toepasbaarheid (Functional appropriateness)
  De mate waarin de functies het bereiken van gespecificeerde taken en doelen mogelijk maken.

16.1.2 Prestatie-efficiëntie (Performance efficiency)

De prestaties in verhouding tot de hoeveelheid middelen gebruikt onder genoemde condities.

- Snelheid (Time-behaviour)
  De mate waarin antwoord- en verwerkingstijden en doorvoersnelheid van een product of systeem, tijdens de uitvoer van zijn functies, voldoet aan de wensen.
- Middelenbeslag (Resource utilization)
  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.
- Capaciteit (Capacity)
  De mate waarin de maximale limieten van een product- of systeemparameter voldoet aan de wensen.

16.1.3 Uitwisselbaarheid (Compatibility)

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.

- Beïnvloedbaarheid (Co-existence)
  De mate waarin een product zijn gewenste functies efficiënt kan uitvoeren terwijl het een gemeenschappelijke omgeving en middelen deelt met andere producten, zonder nadelige invloed op enig ander product.
- Koppelbaarheid (Interoperability)
  De mate waarin twee of meer systemen, producten of componenten informatie kunnen uitwisselen en de uitgewisselde informatie kunnen gebruiken.

16.1.4 Bruikbaarheid (Usability)

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.

- Herkenbaarheid van geschiktheid (Appropriateness recognisability)
  De mate waarin gebruikers kunnen herkennen of een product of systeem geschikt is voor hun behoeften.
- Leerbaarheid (Learnability)
  De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om gespecificeerde leerdoelen te bereiken met betrekking tot het gebruik van het product of systeem met effectiviteit, efficiëntie, vrijheid van risico en voldoening, in een gespecificeerde gebruikscontext.

- Bedienbaarheid (Operability)
  De mate waarin een product of systeem attributen heeft die het makkelijk maken om het te bedienen en beheersen.
- Voorkomen gebruikersfouten (User error protection)
  De mate waarin het systeem gebruikers beschermt tegen het maken van fouten.
- Volmaaktheid gebruikersinteractie (User interface aesthetics)
  De mate waarin een gebruikersinterface het de gebruiker mogelijk maakt om een plezierige en voldoening gevende interactie te hebben.
- Toegankelijkheid (Accessibility)
  De mate waarin een product of systeem gebruikt kan worden door mensen met de meest uiteenlopende eigenschappen en mogelijkheden om een gespecificeerd doel te bereiken in een gespecificeerde gebruikscontext

16.1.5 Betrouwbaarheid (Reliability)

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

- Volwassenheid (Maturity)
  De mate waarin een systeem, product of component aan betrouwbaarheidsbehoeften voldoet onder normale werkomstandigheden.
- Beschikbaarheid (Availability)
  De mate waarin een systeem, product of component operationeel en toegankelijk is wanneer men het wil gebruiken.
- Foutbestendigheid (Fault tolerance)
  De mate waarin een systeem, product of component werkt zoals bedoeld ondanks de aanwezigheid van hard- of softwarefouten.
- Herstelbaarheid (Recoverability)
  De mate waarin het product of 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.

16.1.6 Beveiligbaarheid (Security)

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.

- Vertrouwelijkheid (Confidentiality)
  De mate waarin een product of systeem er voor zorgt dat gegevens alleen toegankelijk zijn voor diegenen die geautoriseerd zijn.
- Integriteit (Integrity)
  De mate waarin een systeem, product of component ongeautoriseerde toegang tot of aanpassing van computerprogramma's of gegevens verhindert.
- Onweerlegbaarheid (Non-repudiation)
  De mate waarin kan worden bewezen dat acties of gebeurtenissen plaats hebben gevonden, zodat later deze acties of gebeurtenissen niet ontkend kunnen worden.
- Verantwoording (Accountability)
  De mate waarin acties van een entiteit getraceerd kunnen worden naar die specifieke entiteit.
- Authenticiteit (Authenticity)
  De mate waarin bewezen kan worden dat de identiteit van een onderwerp of bron is zoals wordt beweerd.
- De mate waarin een claim over de oorsprong of de auteur van de informatie verifieerbaar is, bijvoorbeeld aan handschrift.

16.1.7 Onderhoudbaarheid (Maintainability)

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

- Modulariteit (Modularity)
  De mate waarin een systeem of computerprogramma opgebouwd is in losstaande componenten zodat wijzigingen van een component minimale impact heeft op andere componenten.

- Herbruikbaarheid (Reusability)
  De mate waarin een bestaand onderdeel gebruikt kan worden in meer dan één systeem of bij het bouwen van een nieuw onderdeel.
- Analyseerbaarheid (Analysability)
  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.
- Wijzigbaarheid (Modifiability)
  De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden zonder fouten of kwaliteitsvermindering tot gevolg.
- Testbaarheid (Testability)
  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.

16.1.8 Overdraagbaarheid (Portability)

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.

- Aanpasbaarheid (Adaptability)
  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.
- Installeerbaarheid (Installability)
  De mate waarin het product of het systeem effectief en efficiënt geïnstalleerd of verwijderd kan worden in een gespecificeerde omgeving.
- Vervangbaarheid (Replaceability)
  De mate waarin een product een ander specifiek softwareproduct, met hetzelfde doel in de zelfde omgeving, kan vervangen.

16.2 Kwaliteit tijdens gebruik (Quality in use)

16.2.1 Effectiviteit (Effectiveness)

De nauwkeurigheid en volledigheid waarmee gebruikers gespecificeerde doelen behalen.

16.2.2 Efficiëntie (Efficiency)

De benodigde hulpbronnen die gebruikt zijn in verhouding tot de nauwkeurigheid en volledigheid waarmee gebruikers doelen behalen.

16.2.3 Voldoening (Satisfaction)

De mate waarin gebruikersbehoeften vervuld worden als het product of systeem gebruikt wordt in een gespecificeerde gebruikscontext.

- Bruikbaarheid (Usefullness)
  De mate waarin een gebruiker tevreden is met de voor de gebruiker waargenomen behaalde doelen, inclusief de resultaten van het gebruik van het systeem en de consequenties van het gebruik van het systeem.
- Vertrouwen (Trust)
  De mate waarin een gebruiker of andere betrokkene vertrouwen heeft dat het product of systeem zich zal gedragen zoals bedoeld.
- Tevredenheid (Pleasure)
  De mate waarin een gebruiker tevreden is bij het verwezenlijken van zijn persoonlijke wensen.
- Welzijn (Comfort)
  De mate waarin een gebruiker tevreden is met zijn fysiek welzijn.

16.2.4 Vrijheid van risico (Freedom from risk)

De mate waarin een product of systeem het potentiële risico beperkt met betrekking tot economische status, mensenlevens, gezondheid of de omgeving.

- Economisch risico beperking (Economic risk mitigation)
  De mate waarin een product of systeem de potentiële risico's beperkt met betrekking tot financiële status, efficiënte werking, commerciële eigendommen, reputatie of andere middelen in de beoogde gebruikscontexten.
- Gezond- en veiligheidsrisico beperking (Health and safety risk mitigation)
  De mate waarin een product of systeem de potentiële risico's met betrekking tot personen beperkt in de beoogde gebruikscontexten.
- Omgevingsrisico beperking (Environmental risk mitigation)
  De mate waarin een product of systeem de potentiële risico's met betrekking tot eigendommen of de omgeving beperkt in de beoogde gebruikscontexten.

16.2.5 Context dekking (Context coverage)

De mate waarin een product of systeem gebruikt kan worden met effectiviteit, efficiëntie, vrijheid van risico en voldoening zowel in de gespecificeerde gebruikscontexten als in niet initieel gespecificeerde gebruikscontexten.

- Context compleetheid (Context completeness)
  De mate waarin een product of systeem gebruikt kan worden met effectiviteit, efficiëntie, vrijheid van risico en voldoening in alle gespecificeerde gebruikscontexten.
- Flexibiliteit (Flexibility)
  De mate waarin een product of systeem gebruikt kan worden met effectiviteit, efficiëntie, vrijheid van risico en voldoening in gebruikscontexten die niet initieel gespecificeerd zijn in de requirements.