Niet-Functionele Eisen

**{Productnaam, versie}**

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 {opdrachtgevende organisatie} | {naam} | {datum} | {versie} |
| Kwaliteitsmanager {beheerorganisatie} | {naam} | {datum} | {versie} |
| Kwaliteitsmanager ICTU | {naam} | {datum} | {versie} |

###### Vereiste goedkeuringen

|  |  |  |  |
| --- | --- | --- | --- |
| Functie/rol | Naam | Datum | Versie |
| Projectleider {opdrachtgevende organisatie} | {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} | {opdrachtgevende organisatie} | Projectleider |
| {naam} | {opdrachtgevende organisatie} | Product owner |
| {naam} | {beheerorganisatie} | Projectleider |
| {naam} | ICTU | Projectleider |
| {naam} | ICTU | Software delivery manager |

###### Template versie

Versie wip, 20-02-2024

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

# Managementsamenvatting

{De applicatie} heeft de volgende functies (PSA, {documentreferentie}):

* {Functie 1}
* {Functie 2}
* {Functie 3}

Deze functies realiseren gezamenlijk het doel van {de applicatie}, namelijk {het doel}.

Omdat {de applicatie} {rationale} is {kwaliteitsaspect 1} de belangrijkste niet-functionele eigenschap. Dat betekent dat {belangrijkste concrete niet-functionele eis voor kwaliteitsaspect 1}. Daarnaast {volgende niet-functionele eis voor kwaliteitsaspect 1}.

Naast {kwaliteitsaspect 1} is ook {kwaliteitsaspect 2} van groot belang omdat {rationale}. Er geldt dat {belangrijkste concrete niet-functionele eis voor kwaliteitsaspect 2}. Ook geldt dat {volgende niet-functionele eis voor kwaliteitsaspect 2}.

Omdat {rationale} is ook {kwaliteitsaspect 3} van belang. Daarom {belangrijkste concrete niet-functionele eis voor kwaliteitsaspect 3}. Ook zal {volgende niet-functionele eis voor kwaliteitsaspect 3}.

Uiteraard voldoet {de applicatie} aan de wettelijke verplichting voor toegankelijkheid (de A en AA-eisen uit WCAG v2.1).

# Inleiding

## 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 standaard NEN-ISO/IEC 25010. Deze standaard onderscheidt een "Product Quality model" en een "Quality-in-Use model". Dit document richt zich op het Product Quality model.

NEN-ISO/IEC 25010 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 kenmerken van een softwareproduct hanteerbaar, realiseerbaar en testbaar te maken; een hoofdeigenschap wordt dan ook weer onderverdeeld in eigenschappen. Deze eigenschappen vormen de basis voor de structurering van de niet-functionele eisen.

De opzet, formulering en inhoud van de niet-functionele eisen voldoen aan algemeen erkende kwaliteitskenmerken: een eis gaat over één onderwerp en is toe te wijzen aan één partij. Daarnaast is de eis compleet, consistent met andere eisen, herleidbaar naar organisatie-eisen, van erkend belang voor de organisatie, actueel, ondubbelzinnig en verifieerbaar. De belangrijke niet-functionele eisen zijn identificeerbaar tot een zodanig niveau dat het mogelijk is:

1. de realisatiefase te begroten met voldoende zekerheid over de benodigde expertise, doorlooptijd en kosten, en
2. op controleerbare wijze te verwerken in software-architectuurdocument (SAD), backlog en testplannen.

In totaal zijn de volgende 31 eigenschappen onderkend:

|  |  |
| --- | --- |
| Hoofdeigenschap | Eigenschap |
| Functionele geschiktheid | Functionele compleetheid |
| Functionele geschiktheid | Functionele correctheid |
| Functionele geschiktheid | Functionele toepasbaarheid |
| Efficiëntie | Snelheid |
| Efficiëntie | Middelenbeslag |
| Efficiëntie | Capaciteit |
| Uitwisselbaarheid | Beïnvloedbaarheid |
| Uitwisselbaarheid | Koppelbaarheid |
| Bruikbaarheid | Herkenbaarheid van geschiktheid |
| Bruikbaarheid | Leerbaarheid |
| Bruikbaarheid | Bedienbaarheid |
| Bruikbaarheid | Voorkomen gebruikersfouten |
| Bruikbaarheid | Volmaaktheid gebruikersinterface |
| Bruikbaarheid | Toegankelijkheid |
| Betrouwbaarheid | Volwassenheid |
| Betrouwbaarheid | Beschikbaarheid |
| Betrouwbaarheid | Foutbestendigheid |
| Betrouwbaarheid | Herstelbaarheid |
| Beveiligbaarheid | Vertrouwelijkheid |
| Beveiligbaarheid | Integriteit |
| Beveiligbaarheid | Onweerlegbaarheid |
| Beveiligbaarheid | Verantwoording |
| Beveiligbaarheid | Authenticiteit |
| Onderhoudbaarheid | Modulariteit |
| Onderhoudbaarheid | Herbruikbaarheid |
| Onderhoudbaarheid | Analyseerbaarheid |
| Onderhoudbaarheid | Wijzigbaarheid |
| Onderhoudbaarheid | Testbaarheid |
| Overdraagbaarheid | Aanpasbaarheid |
| Overdraagbaarheid | Installeerbaarheid |
| Overdraagbaarheid | Vervangbaarheid |

Dit document is als volgt tot stand gekomen:

* De volgende belanghebbenden zijn betrokken bij het opstellen van de eisen door middel van een {workshop} op {datum}: {belanghebbenden}.
* De niet-functionele eisen zijn ontleend aan bestaande documenten: zie paragraaf 2.5.
* Daarnaast zijn de kaders uit paragraaf 2.4 verwerkt.

## 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).

## Kaders

De volgende kaders zijn van toepassing op het projectresultaat:

|  |  |
| --- | --- |
| Volgnummer | Kader |
| K01 | NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017, VIR 2007, VIRBI 2013 en BIO voor het inrichten en beheren van informatiebeveiliging in brede zin. |
| K02 | NCSC ICT-beveiligingsrichtlijnen voor webapplicaties |
| K03 | OWASP Top-10 |
| K04 | ISO 9241-210:2019 Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems |
| K05 | WCAG2.1 (Web Content Accessibility Guidelines) voor eisen met betrekking tot toegankelijkheid |
| K06 | NEN-ISO/IEC 25010:2011 voor het specificeren van productkwaliteit |
| K07 | NORA - Referentiearchitectuur voor de Nederlandse Overheid |

## Uitgangspunten

De volgende uitgangspunten zijn van toepassing op dit document:

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

## Relatie met andere documenten

De volgende documenten waren input voor de niet-functionele eisen:

* Business impact analysis (BIA),
* Privacy impact assessment (PIA),
* Projectstartarchitectuur (PSA) en referentiearchitecturen,
* {En verder, bijvoorbeeld protocollen en samenwerkingsafspraken}.

De niet-functionele eisen zelf zijn input voor:

* Software-architectuurdocument (SAD),
* User stories op de product backlog, voor de eisen die door middel van functionaliteit worden ingevuld (denk aan beveiligingseisen die vereisen dat er bepaalde logging plaatsvindt),
* Kwaliteitsplan, voor de wijze waarop de invulling van de niet-functionele eisen wordt beheerst,
* Mastertestplan (MTP) en detailtestplannen,
* Informatiebeveiligingsplan.

## Leeswijzer

Hoofdstukken 2 tot en met 9 hebben elk betrekking op een hoofdeigenschap. De hoofdstukken zijn verder onderverdeeld in paragrafen conform de kwaliteitseigenschappen uit NEN-ISO/IEC 25010.

In het hoofdstuk Bruikbaarheid is een paragraaf toegevoegd voor de aspecten taal en leesbaarheid. Aspecten die van belang zijn voor gebruikskwaliteit, maar geen onderdeel zijn van NEN-ISO/IEC 25010. En in het hoofdstuk Beveiligbaarheid is een paragraaf toegevoegd met betrekking tot eisen en richtlijnen die volgen uit de Baseline Informatiebeveiliging Overheid (BIO) en Secure Software Development (SSD).

Per eis is een identificatie toegekend (“Nr.”), een beschrijving van de eis (“Eis”), wat de prioritering is (“Prio”) en waarom deze eis is opgenomen met deze prioriteit ("Rationale"). Daarnaast is per eis aangegeven ("Realisatie in") of de eis primair door de software, door de infastructuur of een combinatie daarvan wordt gerealiseerd in het uiteindelijke systeem. De kolom "Realisatie door" geeft aan welke betrokken partij primair verantwoordelijk is voor het realiseren van de eis. De kolom "Bewijs" geeft aan welk document de bewijslast bevat van de invulling van de eis. Waar mogelijk en relevant wordt verwezen naar de overige documentatie.

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.

# 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.

## Functionele compleetheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Functionele correctheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Functionele toepasbaarheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

# Prestatie-efficiëntie

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

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Capaciteit

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

# 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.

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Koppelbaarheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

# 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.

## Herkenbaarheid van geschiktheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Bedienbaarheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Voorkomen gebruikersfouten

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Volmaaktheid gebruikersinterface

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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/> (Engels) en <https://www.w3.org/Translations/WCAG21-nl/> (Nederlands). Conform de EN 301 549, hanteert ICTU de succescriteria voor niveau A en AA als eisen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Bewijs |
| 1 | De applicatie voldoet aan de WCAG2.1 succescriteria, niveau A en AA | {prio} | Wettelijke verplichting | Axe-core rapportage |

Onderstaande tabel bevat de WCAG2.1 succescriteria. {Verwijder de AAA-succescriteria indien gewenst.} Per succescriterium is aangegeven of Axe-core, en zo ja met welke regels, het criterium geautomatiseerd kan controleren. {Geef aan of de succescriteria die Axe-core niet geautomatiseerd kan controleren wel of niet met de hand zullen worden gecontroleerd.}

Merk op dat de [Axe-core regels die als "experimenteel" zijn gemarkeerd](https://github.com/dequelabs/axe-core/blob/develop/doc/rule-descriptions.md#experimental-rules) niet standaard door Axe-core worden getest. Zie de [Axe-core API-documentatie](https://www.deque.com/axe/core-documentation/api-documentation/#options-parameter) voor instructies hoe dit aan te passen.

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Omschrijving | Niveau | Axe-core 4.8.4 regels |
| Principe 1 | [Perceivable](https://www.w3.org/TR/WCAG21/#perceivable) |  |  |
| Richtlijn 1.1 | [Text Alternatives](https://www.w3.org/TR/WCAG21/#text-alternatives) |  |  |
| Succes criterium 1.1.1 | [Non-text Content](https://www.w3.org/TR/WCAG21/#non-text-content) | A | [aria-meter-name](https://dequeuniversity.com/rules/axe/4.8/aria-meter-name?application=axeAPI), [aria-progressbar-name](https://dequeuniversity.com/rules/axe/4.8/aria-progressbar-name?application=axeAPI), [image-alt](https://dequeuniversity.com/rules/axe/4.8/image-alt?application=axeAPI), [input-image-alt](https://dequeuniversity.com/rules/axe/4.8/input-image-alt?application=axeAPI), [object-alt](https://dequeuniversity.com/rules/axe/4.8/object-alt?application=axeAPI), [role-img-alt](https://dequeuniversity.com/rules/axe/4.8/role-img-alt?application=axeAPI), [svg-img-alt](https://dequeuniversity.com/rules/axe/4.8/svg-img-alt?application=axeAPI) |
| Richtlijn 1.2 | [Time-based Media](https://www.w3.org/TR/WCAG21/#time-based-media) |  |  |
| Succes criterium 1.2.1 | [Audio-only and Video-only (Prerecorded)](https://www.w3.org/TR/WCAG21/#audio-only-and-video-only-prerecorded) | A | [audio-caption](https://dequeuniversity.com/rules/axe/4.8/audio-caption?application=axeAPI) |
| Succes criterium 1.2.2 | [Captions (Prerecorded)](https://www.w3.org/TR/WCAG21/#captions-prerecorded) | A | [video-caption](https://dequeuniversity.com/rules/axe/4.8/video-caption?application=axeAPI) |
| Succes criterium 1.2.3 | [Audio Description or Media Alternative (Prerecorded)](https://www.w3.org/TR/WCAG21/#audio-description-or-media-alternative-prerecorded) | A | geen |
| Succes criterium 1.2.4 | [Captions (Live)](https://www.w3.org/TR/WCAG21/#captions-live) | AA | geen |
| Succes criterium 1.2.5 | [Audio Description (Prerecorded)](https://www.w3.org/TR/WCAG21/#audio-description-prerecorded) | AA | geen |
| Succes criterium 1.2.6 | [Sign Language (Prerecorded)](https://www.w3.org/TR/WCAG21/#sign-language-prerecorded) | AAA | geen |
| Succes criterium 1.2.7 | [Extended Audio Description (Prerecorded)](https://www.w3.org/TR/WCAG21/#extended-audio-description-prerecorded) | AAA | geen |
| Succes criterium 1.2.8 | [Media Alternative (Prerecorded)](https://www.w3.org/TR/WCAG21/#media-alternative-prerecorded) | AAA | geen |
| Succes criterium 1.2.9 | [Audio-only (Live)](https://www.w3.org/TR/WCAG21/#audio-only-live) | AAA | geen |
| Richtlijn 1.3 | [Adaptable](https://www.w3.org/TR/WCAG21/#adaptable) |  |  |
| Succes criterium 1.3.1 | [Info and Relationships](https://www.w3.org/TR/WCAG21/#info-and-relationships) | A | [aria-required-children](https://dequeuniversity.com/rules/axe/4.8/aria-required-children?application=axeAPI), [aria-required-parent](https://dequeuniversity.com/rules/axe/4.8/aria-required-parent?application=axeAPI), [definition-list](https://dequeuniversity.com/rules/axe/4.8/definition-list?application=axeAPI), [dlitem](https://dequeuniversity.com/rules/axe/4.8/dlitem?application=axeAPI), [list](https://dequeuniversity.com/rules/axe/4.8/list?application=axeAPI), [listitem](https://dequeuniversity.com/rules/axe/4.8/listitem?application=axeAPI), [p-as-heading](https://dequeuniversity.com/rules/axe/4.8/p-as-heading?application=axeAPI) (experimenteel), [table-fake-caption](https://dequeuniversity.com/rules/axe/4.8/table-fake-caption?application=axeAPI) (experimenteel), [td-has-header](https://dequeuniversity.com/rules/axe/4.8/td-has-header?application=axeAPI) (experimenteel), [td-headers-attr](https://dequeuniversity.com/rules/axe/4.8/td-headers-attr?application=axeAPI), [th-has-data-cells](https://dequeuniversity.com/rules/axe/4.8/th-has-data-cells?application=axeAPI) |
| Succes criterium 1.3.2 | [Meaningful Sequence](https://www.w3.org/TR/WCAG21/#meaningful-sequence) | A | geen |
| Succes criterium 1.3.3 | [Sensory Characteristics](https://www.w3.org/TR/WCAG21/#sensory-characteristics) | A | geen |
| Succes criterium 1.3.4 | [Orientation](https://www.w3.org/TR/WCAG21/#orientation) | AA | [css-orientation-lock](https://dequeuniversity.com/rules/axe/4.8/css-orientation-lock?application=axeAPI) (experimenteel) |
| Succes criterium 1.3.5 | [Identify Input Purpose](https://www.w3.org/TR/WCAG21/#identify-input-purpose) | AA | [autocomplete-valid](https://dequeuniversity.com/rules/axe/4.8/autocomplete-valid?application=axeAPI) |
| Succes criterium 1.3.6 | [Identify Purpose](https://www.w3.org/TR/WCAG21/#identify-purpose) | AAA | geen |
| Richtlijn 1.4 | [Distinguishable](https://www.w3.org/TR/WCAG21/#distinguishable) |  |  |
| Succes criterium 1.4.1 | [Use of Color](https://www.w3.org/TR/WCAG21/#use-of-color) | A | [link-in-text-block](https://dequeuniversity.com/rules/axe/4.8/link-in-text-block?application=axeAPI) |
| Succes criterium 1.4.2 | [Audio Control](https://www.w3.org/TR/WCAG21/#audio-control) | A | [no-autoplay-audio](https://dequeuniversity.com/rules/axe/4.8/no-autoplay-audio?application=axeAPI) |
| Succes criterium 1.4.3 | [Contrast (Minimum)](https://www.w3.org/TR/WCAG21/#contrast-minimum) | AA | [color-contrast](https://dequeuniversity.com/rules/axe/4.8/color-contrast?application=axeAPI) |
| Succes criterium 1.4.4 | [Resize text](https://www.w3.org/TR/WCAG21/#resize-text) | AA | [meta-viewport](https://dequeuniversity.com/rules/axe/4.8/meta-viewport?application=axeAPI) |
| Succes criterium 1.4.5 | [Images of Text](https://www.w3.org/TR/WCAG21/#images-of-text) | AA | geen |
| Succes criterium 1.4.6 | [Contrast (Enhanced)](https://www.w3.org/TR/WCAG21/#contrast-enhanced) | AAA | [color-contrast-enhanced](https://dequeuniversity.com/rules/axe/4.8/color-contrast-enhanced?application=axeAPI) |
| Succes criterium 1.4.7 | [Low or No Background Audio](https://www.w3.org/TR/WCAG21/#low-or-no-background-audio) | AAA | geen |
| Succes criterium 1.4.8 | [Visual Presentation](https://www.w3.org/TR/WCAG21/#visual-presentation) | AAA | geen |
| Succes criterium 1.4.9 | [Images of Text (No Exception)](https://www.w3.org/TR/WCAG21/#images-of-text-no-exception) | AAA | geen |
| Succes criterium 1.4.10 | [Reflow](https://www.w3.org/TR/WCAG21/#reflow) | AA | geen |
| Succes criterium 1.4.11 | [Non-text Contrast](https://www.w3.org/TR/WCAG21/#non-text-contrast) | AA | geen |
| Succes criterium 1.4.12 | [Text Spacing](https://www.w3.org/TR/WCAG21/#text-spacing) | AA | [avoid-inline-spacing](https://dequeuniversity.com/rules/axe/4.8/avoid-inline-spacing?application=axeAPI) |
| Succes criterium 1.4.13 | [Content on Hover or Focus](https://www.w3.org/TR/WCAG21/#content-on-hover-or-focus) | AA | geen |
| Principe 2 | [Operable](https://www.w3.org/TR/WCAG21/#operable) |  |  |
| Richtlijn 2.1 | [Keyboard Accessible](https://www.w3.org/TR/WCAG21/#keyboard-accessible) |  |  |
| Succes criterium 2.1.1 | [Keyboard](https://www.w3.org/TR/WCAG21/#keyboard) | A | [frame-focusable-content](https://dequeuniversity.com/rules/axe/4.8/frame-focusable-content?application=axeAPI), [scrollable-region-focusable](https://dequeuniversity.com/rules/axe/4.8/scrollable-region-focusable?application=axeAPI), [server-side-image-map](https://dequeuniversity.com/rules/axe/4.8/server-side-image-map?application=axeAPI) |
| Succes criterium 2.1.2 | [No Keyboard Trap](https://www.w3.org/TR/WCAG21/#no-keyboard-trap) | A | geen |
| Succes criterium 2.1.3 | [Keyboard (No Exception)](https://www.w3.org/TR/WCAG21/#keyboard-no-exception) | AAA | geen |
| Succes criterium 2.1.4 | [Character Key Shortcuts](https://www.w3.org/TR/WCAG21/#character-key-shortcuts) | A | geen |
| Richtlijn 2.2 | [Enough Time](https://www.w3.org/TR/WCAG21/#enough-time) |  |  |
| Succes criterium 2.2.1 | [Timing Adjustable](https://www.w3.org/TR/WCAG21/#timing-adjustable) | A | [meta-refresh](https://dequeuniversity.com/rules/axe/4.8/meta-refresh?application=axeAPI) |
| Succes criterium 2.2.2 | [Pause, Stop, Hide](https://www.w3.org/TR/WCAG21/#pause-stop-hide) | A | [blink](https://dequeuniversity.com/rules/axe/4.8/blink?application=axeAPI), [marquee](https://dequeuniversity.com/rules/axe/4.8/marquee?application=axeAPI) |
| Succes criterium 2.2.3 | [No Timing](https://www.w3.org/TR/WCAG21/#no-timing) | AAA | geen |
| Succes criterium 2.2.4 | [Interruptions](https://www.w3.org/TR/WCAG21/#interruptions) | AAA | [meta-refresh-no-exceptions](https://dequeuniversity.com/rules/axe/4.8/meta-refresh-no-exceptions?application=axeAPI) |
| Succes criterium 2.2.5 | [Re-authenticating](https://www.w3.org/TR/WCAG21/#re-authenticating) | AAA | geen |
| Succes criterium 2.2.6 | [Timeouts](https://www.w3.org/TR/WCAG21/#timeouts) | AAA | geen |
| Richtlijn 2.3 | [Seizures and Physical Reactions](https://www.w3.org/TR/WCAG21/#seizures-and-physical-reactions) |  |  |
| Succes criterium 2.3.1 | [Three Flashes or Below Threshold](https://www.w3.org/TR/WCAG21/#three-flashes-or-below-threshold) | A | geen |
| Succes criterium 2.3.2 | [Three Flashes](https://www.w3.org/TR/WCAG21/#three-flashes) | AAA | geen |
| Succes criterium 2.3.3 | [Animation from Interactions](https://www.w3.org/TR/WCAG21/#animation-from-interactions) | AAA | geen |
| Richtlijn 2.4 | [Navigable](https://www.w3.org/TR/WCAG21/#navigable) |  |  |
| Succes criterium 2.4.1 | [Bypass Blocks](https://www.w3.org/TR/WCAG21/#bypass-blocks) | A | [bypass](https://dequeuniversity.com/rules/axe/4.8/bypass?application=axeAPI) |
| Succes criterium 2.4.2 | [Page Titled](https://www.w3.org/TR/WCAG21/#page-titled) | A | [document-title](https://dequeuniversity.com/rules/axe/4.8/document-title?application=axeAPI) |
| Succes criterium 2.4.3 | [Focus Order](https://www.w3.org/TR/WCAG21/#focus-order) | A | geen |
| Succes criterium 2.4.4 | [Link Purpose (In Context)](https://www.w3.org/TR/WCAG21/#link-purpose-in-context) | A | [area-alt](https://dequeuniversity.com/rules/axe/4.8/area-alt?application=axeAPI), [link-name](https://dequeuniversity.com/rules/axe/4.8/link-name?application=axeAPI) |
| Succes criterium 2.4.5 | [Multiple Ways](https://www.w3.org/TR/WCAG21/#multiple-ways) | AA | geen |
| Succes criterium 2.4.6 | [Headings and Labels](https://www.w3.org/TR/WCAG21/#headings-and-labels) | AA | geen |
| Succes criterium 2.4.7 | [Focus Visible](https://www.w3.org/TR/WCAG21/#focus-visible) | AA | geen |
| Succes criterium 2.4.8 | [Location](https://www.w3.org/TR/WCAG21/#location) | AAA | geen |
| Succes criterium 2.4.9 | [Link Purpose (Link Only)](https://www.w3.org/TR/WCAG21/#link-purpose-link-only) | AAA | [identical-links-same-purpose](https://dequeuniversity.com/rules/axe/4.8/identical-links-same-purpose?application=axeAPI) |
| Succes criterium 2.4.10 | [Section Headings](https://www.w3.org/TR/WCAG21/#section-headings) | AAA | geen |
| Richtlijn 2.5 | [Input Modalities](https://www.w3.org/TR/WCAG21/#input-modalities) |  |  |
| Succes criterium 2.5.1 | [Pointer Gestures](https://www.w3.org/TR/WCAG21/#pointer-gestures) | A | geen |
| Succes criterium 2.5.2 | [Pointer Cancellation](https://www.w3.org/TR/WCAG21/#pointer-cancellation) | A | geen |
| Succes criterium 2.5.3 | [Label in Name](https://www.w3.org/TR/WCAG21/#label-in-name) | A | [label-content-name-mismatch](https://dequeuniversity.com/rules/axe/4.8/label-content-name-mismatch?application=axeAPI) (experimenteel) |
| Succes criterium 2.5.4 | [Motion Actuation](https://www.w3.org/TR/WCAG21/#motion-actuation) | A | geen |
| Succes criterium 2.5.5 | [Target Size](https://www.w3.org/TR/WCAG21/#target-size) | AAA | geen |
| Succes criterium 2.5.6 | [Concurrent Input Mechanisms](https://www.w3.org/TR/WCAG21/#concurrent-input-mechanisms) | AAA | geen |
| Principe 3 | [Understandable](https://www.w3.org/TR/WCAG21/#understandable) |  |  |
| Richtlijn 3.1 | [Readable](https://www.w3.org/TR/WCAG21/#readable) |  |  |
| Succes criterium 3.1.1 | [Language of Page](https://www.w3.org/TR/WCAG21/#language-of-page) | A | [html-has-lang](https://dequeuniversity.com/rules/axe/4.8/html-has-lang?application=axeAPI), [html-lang-valid](https://dequeuniversity.com/rules/axe/4.8/html-lang-valid?application=axeAPI), [html-xml-lang-mismatch](https://dequeuniversity.com/rules/axe/4.8/html-xml-lang-mismatch?application=axeAPI) |
| Succes criterium 3.1.2 | [Language of Parts](https://www.w3.org/TR/WCAG21/#language-of-parts) | AA | [valid-lang](https://dequeuniversity.com/rules/axe/4.8/valid-lang?application=axeAPI) |
| Succes criterium 3.1.3 | [Unusual Words](https://www.w3.org/TR/WCAG21/#unusual-words) | AAA | geen |
| Succes criterium 3.1.4 | [Abbreviations](https://www.w3.org/TR/WCAG21/#abbreviations) | AAA | geen |
| Succes criterium 3.1.5 | [Reading Level](https://www.w3.org/TR/WCAG21/#reading-level) | AAA | geen |
| Succes criterium 3.1.6 | [Pronunciation](https://www.w3.org/TR/WCAG21/#pronunciation) | AAA | geen |
| Richtlijn 3.2 | [Predictable](https://www.w3.org/TR/WCAG21/#predictable) |  |  |
| Succes criterium 3.2.1 | [On Focus](https://www.w3.org/TR/WCAG21/#on-focus) | A | geen |
| Succes criterium 3.2.2 | [On Input](https://www.w3.org/TR/WCAG21/#on-input) | A | geen |
| Succes criterium 3.2.3 | [Consistent Navigation](https://www.w3.org/TR/WCAG21/#consistent-navigation) | AA | geen |
| Succes criterium 3.2.4 | [Consistent Identification](https://www.w3.org/TR/WCAG21/#consistent-identification) | AA | geen |
| Succes criterium 3.2.5 | [Change on Request](https://www.w3.org/TR/WCAG21/#change-on-request) | AAA | [meta-refresh-no-exceptions](https://dequeuniversity.com/rules/axe/4.8/meta-refresh-no-exceptions?application=axeAPI) |
| Richtlijn 3.3 | [Input Assistance](https://www.w3.org/TR/WCAG21/#input-assistance) |  |  |
| Succes criterium 3.3.1 | [Error Identification](https://www.w3.org/TR/WCAG21/#error-identification) | A | geen |
| Succes criterium 3.3.2 | [Labels or Instructions](https://www.w3.org/TR/WCAG21/#labels-or-instructions) | A | [form-field-multiple-labels](https://dequeuniversity.com/rules/axe/4.8/form-field-multiple-labels?application=axeAPI) |
| Succes criterium 3.3.3 | [Error Suggestion](https://www.w3.org/TR/WCAG21/#error-suggestion) | AA | geen |
| Succes criterium 3.3.4 | [Error Prevention (Legal, Financial, Data)](https://www.w3.org/TR/WCAG21/#error-prevention-legal-financial-data) | AA | geen |
| Succes criterium 3.3.5 | [Help](https://www.w3.org/TR/WCAG21/#help) | AAA | geen |
| Succes criterium 3.3.6 | [Error Prevention (All)](https://www.w3.org/TR/WCAG21/#error-prevention-all) | AAA | geen |
| Principe 4 | [Robust](https://www.w3.org/TR/WCAG21/#robust) |  |  |
| Richtlijn 4.1 | [Compatible](https://www.w3.org/TR/WCAG21/#compatible) |  |  |
| Succes criterium 4.1.1 | [Parsing](https://www.w3.org/TR/WCAG21/#parsing) | A | [duplicate-id-active](https://dequeuniversity.com/rules/axe/4.8/duplicate-id-active?application=axeAPI), [duplicate-id](https://dequeuniversity.com/rules/axe/4.8/duplicate-id?application=axeAPI) |
| Succes criterium 4.1.2 | [Name, Role, Value](https://www.w3.org/TR/WCAG21/#name-role-value) | A | [area-alt](https://dequeuniversity.com/rules/axe/4.8/area-alt?application=axeAPI), [aria-allowed-attr](https://dequeuniversity.com/rules/axe/4.8/aria-allowed-attr?application=axeAPI), [aria-braille-equivalent](https://dequeuniversity.com/rules/axe/4.8/aria-braille-equivalent?application=axeAPI), [aria-command-name](https://dequeuniversity.com/rules/axe/4.8/aria-command-name?application=axeAPI), [aria-conditional-attr](https://dequeuniversity.com/rules/axe/4.8/aria-conditional-attr?application=axeAPI), [aria-deprecated-role](https://dequeuniversity.com/rules/axe/4.8/aria-deprecated-role?application=axeAPI), [aria-hidden-body](https://dequeuniversity.com/rules/axe/4.8/aria-hidden-body?application=axeAPI), [aria-hidden-focus](https://dequeuniversity.com/rules/axe/4.8/aria-hidden-focus?application=axeAPI), [aria-input-field-name](https://dequeuniversity.com/rules/axe/4.8/aria-input-field-name?application=axeAPI), [aria-prohibited-attr](https://dequeuniversity.com/rules/axe/4.8/aria-prohibited-attr?application=axeAPI), [aria-required-attr](https://dequeuniversity.com/rules/axe/4.8/aria-required-attr?application=axeAPI), [aria-roledescription](https://dequeuniversity.com/rules/axe/4.8/aria-roledescription?application=axeAPI), [aria-roles](https://dequeuniversity.com/rules/axe/4.8/aria-roles?application=axeAPI), [aria-toggle-field-name](https://dequeuniversity.com/rules/axe/4.8/aria-toggle-field-name?application=axeAPI), [aria-tooltip-name](https://dequeuniversity.com/rules/axe/4.8/aria-tooltip-name?application=axeAPI), [aria-valid-attr-value](https://dequeuniversity.com/rules/axe/4.8/aria-valid-attr-value?application=axeAPI), [aria-valid-attr](https://dequeuniversity.com/rules/axe/4.8/aria-valid-attr?application=axeAPI), [button-name](https://dequeuniversity.com/rules/axe/4.8/button-name?application=axeAPI), [duplicate-id-aria](https://dequeuniversity.com/rules/axe/4.8/duplicate-id-aria?application=axeAPI), [frame-title-unique](https://dequeuniversity.com/rules/axe/4.8/frame-title-unique?application=axeAPI), [frame-title](https://dequeuniversity.com/rules/axe/4.8/frame-title?application=axeAPI), [input-button-name](https://dequeuniversity.com/rules/axe/4.8/input-button-name?application=axeAPI), [input-image-alt](https://dequeuniversity.com/rules/axe/4.8/input-image-alt?application=axeAPI), [label](https://dequeuniversity.com/rules/axe/4.8/label?application=axeAPI), [link-name](https://dequeuniversity.com/rules/axe/4.8/link-name?application=axeAPI), [nested-interactive](https://dequeuniversity.com/rules/axe/4.8/nested-interactive?application=axeAPI), [select-name](https://dequeuniversity.com/rules/axe/4.8/select-name?application=axeAPI) |
| Succes criterium 4.1.3 | [Status Messages](https://www.w3.org/TR/WCAG21/#status-messages) | AA | geen |

## Taal en leesbaarheid

Naast de aan NEN-ISO/IEC 25010 ontleende hoofdeigenschap bruikbaarheid zijn voor de gebruikskwaliteit van {de applicatie} van belang:

* Taal: welke talen dienen te worden ondersteund.
* Leesbaarheid: teksten moeten makkelijk te lezen zijn. Korte zinnen hebben de voorkeur. Hoe gemakkelijker de zin en de woorden, hoe beter de leesbaarheid.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Bewijs |
| 1 | De applicatie gebruikt maximaal taalniveau B1 | {prio} | [Aanbevolen richtlijn](https://www.communicatierijk.nl/vakkennis/rijkswebsites/aanbevolen-richtlijnen/taalniveau-b1) | {bewijs} |
| 2 | De applicatie ondersteunt {ondersteunde talen} | {prio} | {rationale} | {bewijs} |

# Betrouwbaarheid

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

## Volwassenheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Beschikbaarheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Foutbestendigheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

# 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.

## BIO- en SSD-eisen

De overheid is gebonden aan kaderstelling op het gebied van informatiebeveiliging, zoals de Baseline Informatiebeveiliging Overheid (BIO). 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 BIO ondersteunt. De BIO is een toepassing van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 op het domein van de Nederlandse overheid. Voor de Rijksoverheid zijn in die toepassing het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007) en het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) verwerkt.

BIO 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 | Rationale | Bewijs |
| 1 | Applicaties zijn gebaseerd op een formele, met de beheerorganisatie afgestemde standaard stack | {prio} | Dit maakt integrale beveiliging mogelijk en beperkt het risico op nieuwe en onbekende zwakheden door het gebruik van onbekende componenten of services | {bewijs} |
| 2 | De architectuur van een (web)applicatie is gebaseerd op een gelaagde structuur door de presentatielaag, de applicatielaag en de gegevens te scheiden | {prio} | Hierdoor kunnen de lagen beschermd worden binnen de netwerkzones | {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} | {rationale} | {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} | {rationale} | {bewijs} |
| 5 | Inrichting van de autorisaties van gebruikers (inclusief beheerders) binnen een (web)applicatie: | {prio} | Autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet te verenigen autorisaties is mogelijk | {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} |
| 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} | {rationale} | {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 | {prio} | Mogelijk maken van toekomstig onderzoek en toegangscontrole | {bewijs} |
| 8 | Applicaties normaliseren de invoer, valideren de invoer op syntax en semantiek en normaliseren uitvoer waar dit toepasbaar is | {prio} | 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. | {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 gelogd | {prio} | Onbeschikbaarheid van de applicatie voorkomen en tegelijkertijd analyse van de opgetreden situatie mogelijk maken | {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} | {rationale} | {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} | {rationale} | {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} | {rationale} | {bewijs} |
| 13 | De maximale sessieduur en maximale inactiviteit zijn door (of namens) de opdrachtgevende organisatie in te stellen. De instelbare waarden zijn per default begrenst op 10 uur (sessieduur) en 15 minuten (inactiviteit). Alleen op expliciet aangeven van de opdrachtgevede organisatie kan hiervan worden afgeweken | {prio} | {rationale} | {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} | {rationale} | {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} | {rationale} | {bewijs} |
| 16 | Applicaties hebben geen run-time afhankelijkheid van externe codebronnen | {prio} | {rationale} | {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} | {rationale} | {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} | {rationale} | {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 | {prio} | De logging zorgt voor traceerbaarheid van gebeurtenissen en activiteiten in relatie tot ten minste personen, systemen, applicaties en tijd | {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} | {rationale} | {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 | {prio} | Voorkomt misbruik van het commentaar | {bewijs} |
| 22 | De aan de gebruiker getoonde informatie bevat geen directory listings | {prio} | Voorkomt misbruik van de directory listing | {bewijs} |
| 23 | Wanneer toegang tot (de inhoud van) het filesysteem nodig is, gebeurt dit altijd onder expliciete autorisatie en controle door de applicatie | {prio} | {rationale} | {bewijs} |
| 24 | In de (web)applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht | {prio} | {rationale} | {bewijs} |
| {nr} | {eis} | {prio} | {rationale} | {bewijs} |

## Vertrouwelijkheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Integriteit

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Verantwoording

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Authenticiteit

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

# Onderhoudbaarheid

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

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Wijzigbaarheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

# 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.

## 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 | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Installeerbaarheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

## Vervangbaarheid

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| {nr} | {eis} | {prio} | {rationale} | {software/hardware/combinatie} | {partij} | {bewijs} |

Bijlagen

1. Terminologie en afkortingen

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

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

1. Bronnen

De onderstaande tabel verwijst naar regelmatig gebruikte bronnen.

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

1. De ICTU Kwaliteitsaanpak Softwareontwikkeling

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

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

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

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

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

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

De ICTU Kwaliteitsaanpak Softwareontwikkeling heeft drie doelstellingen:

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

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

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

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

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