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

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

###### Goedkeuring

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

###### Revisiehistorie

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

###### Betrokkenen bij dit document

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

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

###### Template versie

Versie wip, 02-04-2025

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

# Managementsamenvatting

{het product} heeft de volgende functies (PSA, {documentreferentie}):

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

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

Omdat {het product} {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 {het product} aan de wettelijke verplichting voor toegankelijkheid (de A en AA-eisen uit WCAG v2.2).

# Inleiding

## Over dit document

Dit document beschrijft de niet-functionele eisen aan {het product}. Basis voor de niet-functionele eisen zijn de kwaliteitsattributen zoals gedefinieerd in de standaard NEN-ISO/IEC 25010:2023. De 2023 versie van de standaard is nog niet in het Nederlands vertaald en daarom gebruikt dit document de engelstalige terminologie. De standaard bevat een "product quality model" dat productkwaliteit in negen hoofdeigenschappen onderverdeelt: functional suitability, performance efficiency, compatibility, interaction capability, reliability, security, maintainability, flexibility en safety.

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 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), product backlog en testplannen.

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 | WCAG2.2 (Web Content Accessibility Guidelines) voor eisen met betrekking tot toegankelijkheid |
| K06 | NEN-ISO/IEC 25010:2023 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 analyse (BIA),
* Data protection impact assessment (DPIA),
* 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 3 tot en met 11 hebben elk betrekking op een hoofdeigenschap. De hoofdstukken zijn verder onderverdeeld in paragrafen conform de kwaliteitseigenschappen uit NEN-ISO/IEC 25010:2023.

In het hoofdstuk Interaction capability 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 25010:2023. En in het hoofdstuk Security 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.

# Functional suitability

Capability of a product to provide functions that meet stated and implied needs of intended users when it is used under specified conditions.

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

## Functional completeness

Capability of a product to provide a set of functions that covers all the specified tasks and intended users’ objectives.

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

## Functional correctness

Capability of a product to provide accurate results when used by intended users.

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

## Functional appropriateness

Capability of a product to provide functions that facilitate the accomplishment of specified tasks and objectives.

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

# Performance-efficiency

Capability of a product to perform its functions within specified time and throughput parameters and be efficient in the use of resources under specified conditions.

## Time behavior

Capability of a product to perform its specified function under specified conditions so that the response time and throughput rates meet the requirements.

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

## Resource utilization

Capability of a product to use no more than the specified amount of resources to perform its function under specified conditions.

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

## Capacity

Capability of a product to meet requirements for the maximum limits of a product parameter.

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

# Compatability

Capability of a product to exchange information with other products, and/or to perform its required functions while sharing the same common environment and resources.

## Co-existence

Capability of a product to perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product.

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

## Interoperability

Capability of a product to exchange information with other products and mutually use the information that has been exchanged.

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

# Interaction capability

Capability of a product to be interacted with by specified users to exchange information between a user and a system via the user interface to complete the intended task.

## Appropriateness recognizability

Capability of a product to be recognized by users as appropriate for their needs.

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

## Learnability

Capability of a product to have specified users learn to use specified product functions within a specified amount of time.

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

## Operability

Capability of a product to have functions and attributes that it easy to operate and control.

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

## User error protection

Capability of a product to prevent operation errors.

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

## User engagement

Capability of a product to present functions and information in an inviting and motivating manner encouraging continued interaction.

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

## Inclusivity

Capability of a product to be utilised by people of various backgrounds.

Als standaard voor toegankelijkheid hanteert de Nederlandse overheid de Web Content Accessibility Guidelines (WCAG), zie <https://www.w3.org/TR/WCAG22/>. Officieel gebruikt de Nederlandse Overheid versie 2.1, maar het gebruik van versie 2.2 wordt [aangeraden](https://www.digitaleoverheid.nl/nieuws/nieuwe-aanbevolen-standaard-digitale-toegankelijkheid/).

Van WCAG versie 2.2 is op het moment nog geen Nederlandse vertaling, wel van versie 2.1, zie [https://www.w3.org/Translations/WCAG22-nl/](https://www.w3.org/Translations/WCAG21-nl/).

Conform de EN 301 549, hanteert {opdrachtgevende organisatie} de succescriteria voor niveau A en AA als eisen.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Eis | Prio | Rationale | Realisatie in | Realisatie door | Bewijs |
| 1 | De applicatie voldoet aan de WCAG2.2 succescriteria, niveau A en AA | {prio} | Wettelijke verplichting | {software} | ICTU | Axe-core rapportage |

Onderstaande tabel bevat de WCAG2.2 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 4.10.3 regels |
| Principe 1 | [Perceivable](https://www.w3.org/TR/WCAG22/#perceivable) |  |  |
| Richtlijn 1.1 | [Text Alternatives](https://www.w3.org/TR/WCAG22/#text-alternatives) |  |  |
| Succes criterium 1.1.1 | [Non-text Content](https://www.w3.org/TR/WCAG22/#non-text-content) | A | [aria-meter-name](https://dequeuniversity.com/rules/axe/4.10/aria-meter-name?application=axeAPI), [aria-progressbar-name](https://dequeuniversity.com/rules/axe/4.10/aria-progressbar-name?application=axeAPI), [image-alt](https://dequeuniversity.com/rules/axe/4.10/image-alt?application=axeAPI), [input-image-alt](https://dequeuniversity.com/rules/axe/4.10/input-image-alt?application=axeAPI), [object-alt](https://dequeuniversity.com/rules/axe/4.10/object-alt?application=axeAPI), [role-img-alt](https://dequeuniversity.com/rules/axe/4.10/role-img-alt?application=axeAPI), [svg-img-alt](https://dequeuniversity.com/rules/axe/4.10/svg-img-alt?application=axeAPI) |
| Richtlijn 1.2 | [Time-based Media](https://www.w3.org/TR/WCAG22/#time-based-media) |  |  |
| Succes criterium 1.2.1 | [Audio-only and Video-only (Prerecorded)](https://www.w3.org/TR/WCAG22/#audio-only-and-video-only-prerecorded) | A | [audio-caption](https://dequeuniversity.com/rules/axe/4.10/audio-caption?application=axeAPI) |
| Succes criterium 1.2.2 | [Captions (Prerecorded)](https://www.w3.org/TR/WCAG22/#captions-prerecorded) | A | [video-caption](https://dequeuniversity.com/rules/axe/4.10/video-caption?application=axeAPI) |
| Succes criterium 1.2.3 | [Audio Description or Media Alternative (Prerecorded)](https://www.w3.org/TR/WCAG22/#audio-description-or-media-alternative-prerecorded) | A | geen |
| Succes criterium 1.2.4 | [Captions (Live)](https://www.w3.org/TR/WCAG22/#captions-live) | AA | geen |
| Succes criterium 1.2.5 | [Audio Description (Prerecorded)](https://www.w3.org/TR/WCAG22/#audio-description-prerecorded) | AA | geen |
| Succes criterium 1.2.6 | [Sign Language (Prerecorded)](https://www.w3.org/TR/WCAG22/#sign-language-prerecorded) | AAA | geen |
| Succes criterium 1.2.7 | [Extended Audio Description (Prerecorded)](https://www.w3.org/TR/WCAG22/#extended-audio-description-prerecorded) | AAA | geen |
| Succes criterium 1.2.8 | [Media Alternative (Prerecorded)](https://www.w3.org/TR/WCAG22/#media-alternative-prerecorded) | AAA | geen |
| Succes criterium 1.2.9 | [Audio-only (Live)](https://www.w3.org/TR/WCAG22/#audio-only-live) | AAA | geen |
| Richtlijn 1.3 | [Adaptable](https://www.w3.org/TR/WCAG22/#adaptable) |  |  |
| Succes criterium 1.3.1 | [Info and Relationships](https://www.w3.org/TR/WCAG22/#info-and-relationships) | A | [aria-hidden-body](https://dequeuniversity.com/rules/axe/4.10/aria-hidden-body?application=axeAPI), [aria-required-children](https://dequeuniversity.com/rules/axe/4.10/aria-required-children?application=axeAPI), [aria-required-parent](https://dequeuniversity.com/rules/axe/4.10/aria-required-parent?application=axeAPI), [definition-list](https://dequeuniversity.com/rules/axe/4.10/definition-list?application=axeAPI), [dlitem](https://dequeuniversity.com/rules/axe/4.10/dlitem?application=axeAPI), [list](https://dequeuniversity.com/rules/axe/4.10/list?application=axeAPI), [listitem](https://dequeuniversity.com/rules/axe/4.10/listitem?application=axeAPI), [p-as-heading](https://dequeuniversity.com/rules/axe/4.10/p-as-heading?application=axeAPI) (experimenteel), [table-fake-caption](https://dequeuniversity.com/rules/axe/4.10/table-fake-caption?application=axeAPI) (experimenteel), [td-has-header](https://dequeuniversity.com/rules/axe/4.10/td-has-header?application=axeAPI) (experimenteel), [td-headers-attr](https://dequeuniversity.com/rules/axe/4.10/td-headers-attr?application=axeAPI), [th-has-data-cells](https://dequeuniversity.com/rules/axe/4.10/th-has-data-cells?application=axeAPI) |
| Succes criterium 1.3.2 | [Meaningful Sequence](https://www.w3.org/TR/WCAG22/#meaningful-sequence) | A | geen |
| Succes criterium 1.3.3 | [Sensory Characteristics](https://www.w3.org/TR/WCAG22/#sensory-characteristics) | A | geen |
| Succes criterium 1.3.4 | [Orientation](https://www.w3.org/TR/WCAG22/#orientation) | AA | [css-orientation-lock](https://dequeuniversity.com/rules/axe/4.10/css-orientation-lock?application=axeAPI) (experimenteel) |
| Succes criterium 1.3.5 | [Identify Input Purpose](https://www.w3.org/TR/WCAG22/#identify-input-purpose) | AA | [autocomplete-valid](https://dequeuniversity.com/rules/axe/4.10/autocomplete-valid?application=axeAPI) |
| Succes criterium 1.3.6 | [Identify Purpose](https://www.w3.org/TR/WCAG22/#identify-purpose) | AAA | geen |
| Richtlijn 1.4 | [Distinguishable](https://www.w3.org/TR/WCAG22/#distinguishable) |  |  |
| Succes criterium 1.4.1 | [Use of Color](https://www.w3.org/TR/WCAG22/#use-of-color) | A | [link-in-text-block](https://dequeuniversity.com/rules/axe/4.10/link-in-text-block?application=axeAPI) |
| Succes criterium 1.4.2 | [Audio Control](https://www.w3.org/TR/WCAG22/#audio-control) | A | [no-autoplay-audio](https://dequeuniversity.com/rules/axe/4.10/no-autoplay-audio?application=axeAPI) |
| Succes criterium 1.4.3 | [Contrast (Minimum)](https://www.w3.org/TR/WCAG22/#contrast-minimum) | AA | [color-contrast](https://dequeuniversity.com/rules/axe/4.10/color-contrast?application=axeAPI) |
| Succes criterium 1.4.4 | [Resize Text](https://www.w3.org/TR/WCAG22/#resize-text) | AA | [meta-viewport](https://dequeuniversity.com/rules/axe/4.10/meta-viewport?application=axeAPI) |
| Succes criterium 1.4.5 | [Images of Text](https://www.w3.org/TR/WCAG22/#images-of-text) | AA | geen |
| Succes criterium 1.4.6 | [Contrast (Enhanced)](https://www.w3.org/TR/WCAG22/#contrast-enhanced) | AAA | [color-contrast-enhanced](https://dequeuniversity.com/rules/axe/4.10/color-contrast-enhanced?application=axeAPI) |
| Succes criterium 1.4.7 | [Low or No Background Audio](https://www.w3.org/TR/WCAG22/#low-or-no-background-audio) | AAA | geen |
| Succes criterium 1.4.8 | [Visual Presentation](https://www.w3.org/TR/WCAG22/#visual-presentation) | AAA | geen |
| Succes criterium 1.4.9 | [Images of Text (No Exception)](https://www.w3.org/TR/WCAG22/#images-of-text-no-exception) | AAA | geen |
| Succes criterium 1.4.10 | [Reflow](https://www.w3.org/TR/WCAG22/#reflow) | AA | geen |
| Succes criterium 1.4.11 | [Non-text Contrast](https://www.w3.org/TR/WCAG22/#non-text-contrast) | AA | geen |
| Succes criterium 1.4.12 | [Text Spacing](https://www.w3.org/TR/WCAG22/#text-spacing) | AA | [avoid-inline-spacing](https://dequeuniversity.com/rules/axe/4.10/avoid-inline-spacing?application=axeAPI) |
| Succes criterium 1.4.13 | [Content on Hover or Focus](https://www.w3.org/TR/WCAG22/#content-on-hover-or-focus) | AA | geen |
| Principe 2 | [Operable](https://www.w3.org/TR/WCAG22/#operable) |  |  |
| Richtlijn 2.1 | [Keyboard Accessible](https://www.w3.org/TR/WCAG22/#keyboard-accessible) |  |  |
| Succes criterium 2.1.1 | [Keyboard](https://www.w3.org/TR/WCAG22/#keyboard) | A | [frame-focusable-content](https://dequeuniversity.com/rules/axe/4.10/frame-focusable-content?application=axeAPI), [scrollable-region-focusable](https://dequeuniversity.com/rules/axe/4.10/scrollable-region-focusable?application=axeAPI), [server-side-image-map](https://dequeuniversity.com/rules/axe/4.10/server-side-image-map?application=axeAPI) |
| Succes criterium 2.1.2 | [No Keyboard Trap](https://www.w3.org/TR/WCAG22/#no-keyboard-trap) | A | geen |
| Succes criterium 2.1.3 | [Keyboard (No Exception)](https://www.w3.org/TR/WCAG22/#keyboard-no-exception) | AAA | [scrollable-region-focusable](https://dequeuniversity.com/rules/axe/4.10/scrollable-region-focusable?application=axeAPI) |
| Succes criterium 2.1.4 | [Character Key Shortcuts](https://www.w3.org/TR/WCAG22/#character-key-shortcuts) | A | geen |
| Richtlijn 2.2 | [Enough Time](https://www.w3.org/TR/WCAG22/#enough-time) |  |  |
| Succes criterium 2.2.1 | [Timing Adjustable](https://www.w3.org/TR/WCAG22/#timing-adjustable) | A | [meta-refresh](https://dequeuniversity.com/rules/axe/4.10/meta-refresh?application=axeAPI) |
| Succes criterium 2.2.2 | [Pause, Stop, Hide](https://www.w3.org/TR/WCAG22/#pause-stop-hide) | A | [blink](https://dequeuniversity.com/rules/axe/4.10/blink?application=axeAPI), [marquee](https://dequeuniversity.com/rules/axe/4.10/marquee?application=axeAPI) |
| Succes criterium 2.2.3 | [No Timing](https://www.w3.org/TR/WCAG22/#no-timing) | AAA | geen |
| Succes criterium 2.2.4 | [Interruptions](https://www.w3.org/TR/WCAG22/#interruptions) | AAA | [meta-refresh-no-exceptions](https://dequeuniversity.com/rules/axe/4.10/meta-refresh-no-exceptions?application=axeAPI) |
| Succes criterium 2.2.5 | [Re-authenticating](https://www.w3.org/TR/WCAG22/#re-authenticating) | AAA | geen |
| Succes criterium 2.2.6 | [Timeouts](https://www.w3.org/TR/WCAG22/#timeouts) | AAA | geen |
| Richtlijn 2.3 | [Seizures and Physical Reactions](https://www.w3.org/TR/WCAG22/#seizures-and-physical-reactions) |  |  |
| Succes criterium 2.3.1 | [Three Flashes or Below Threshold](https://www.w3.org/TR/WCAG22/#three-flashes-or-below-threshold) | A | geen |
| Succes criterium 2.3.2 | [Three Flashes](https://www.w3.org/TR/WCAG22/#three-flashes) | AAA | geen |
| Succes criterium 2.3.3 | [Animation from Interactions](https://www.w3.org/TR/WCAG22/#animation-from-interactions) | AAA | geen |
| Richtlijn 2.4 | [Navigable](https://www.w3.org/TR/WCAG22/#navigable) |  |  |
| Succes criterium 2.4.1 | [Bypass Blocks](https://www.w3.org/TR/WCAG22/#bypass-blocks) | A | [bypass](https://dequeuniversity.com/rules/axe/4.10/bypass?application=axeAPI) |
| Succes criterium 2.4.2 | [Page Titled](https://www.w3.org/TR/WCAG22/#page-titled) | A | [document-title](https://dequeuniversity.com/rules/axe/4.10/document-title?application=axeAPI) |
| Succes criterium 2.4.3 | [Focus Order](https://www.w3.org/TR/WCAG22/#focus-order) | A | geen |
| Succes criterium 2.4.4 | [Link Purpose (In Context)](https://www.w3.org/TR/WCAG22/#link-purpose-in-context) | A | [area-alt](https://dequeuniversity.com/rules/axe/4.10/area-alt?application=axeAPI), [link-name](https://dequeuniversity.com/rules/axe/4.10/link-name?application=axeAPI) |
| Succes criterium 2.4.5 | [Multiple Ways](https://www.w3.org/TR/WCAG22/#multiple-ways) | AA | geen |
| Succes criterium 2.4.6 | [Headings and Labels](https://www.w3.org/TR/WCAG22/#headings-and-labels) | AA | geen |
| Succes criterium 2.4.7 | [Focus Visible](https://www.w3.org/TR/WCAG22/#focus-visible) | AA | geen |
| Succes criterium 2.4.8 | [Location](https://www.w3.org/TR/WCAG22/#location) | AAA | geen |
| Succes criterium 2.4.9 | [Link Purpose (Link Only)](https://www.w3.org/TR/WCAG22/#link-purpose-link-only) | AAA | [identical-links-same-purpose](https://dequeuniversity.com/rules/axe/4.10/identical-links-same-purpose?application=axeAPI) |
| Succes criterium 2.4.10 | [Section Headings](https://www.w3.org/TR/WCAG22/#section-headings) | AAA | geen |
| Succes criterium 2.4.11 | [Focus Not Obscured (Minimum)](https://www.w3.org/TR/WCAG22/#focus-not-obscured-minimum) | AA | geen |
| Succes criterium 2.4.12 | [Focus Not Obscured (Enhanced)](https://www.w3.org/TR/WCAG22/#focus-not-obscured-enhanced) | AAA | geen |
| Succes criterium 2.4.13 | [Focus Appearance](https://www.w3.org/TR/WCAG22/#focus-appearance) | AAA | geen |
| Richtlijn 2.5 | [Input Modalities](https://www.w3.org/TR/WCAG22/#input-modalities) |  |  |
| Succes criterium 2.5.1 | [Pointer Gestures](https://www.w3.org/TR/WCAG22/#pointer-gestures) | A | geen |
| Succes criterium 2.5.2 | [Pointer Cancellation](https://www.w3.org/TR/WCAG22/#pointer-cancellation) | A | geen |
| Succes criterium 2.5.3 | [Label in Name](https://www.w3.org/TR/WCAG22/#label-in-name) | A | [label-content-name-mismatch](https://dequeuniversity.com/rules/axe/4.10/label-content-name-mismatch?application=axeAPI) (experimenteel) |
| Succes criterium 2.5.4 | [Motion Actuation](https://www.w3.org/TR/WCAG22/#motion-actuation) | A | geen |
| Succes criterium 2.5.5 | [Target Size (Enhanced)](https://www.w3.org/TR/WCAG22/#target-size-enhanced) | AAA | geen |
| Succes criterium 2.5.6 | [Concurrent Input Mechanisms](https://www.w3.org/TR/WCAG22/#concurrent-input-mechanisms) | AAA | geen |
| Succes criterium 2.5.7 | [Dragging Movements](https://www.w3.org/TR/WCAG22/#dragging-movements) | AA | geen |
| Succes criterium 2.5.8 | [Target Size (Minimum)](https://www.w3.org/TR/WCAG22/#target-size-minimum) | AA | [target-size](https://dequeuniversity.com/rules/axe/4.10/target-size?application=axeAPI) |
| Principe 3 | [Understandable](https://www.w3.org/TR/WCAG22/#understandable) |  |  |
| Richtlijn 3.1 | [Readable](https://www.w3.org/TR/WCAG22/#readable) |  |  |
| Succes criterium 3.1.1 | [Language of Page](https://www.w3.org/TR/WCAG22/#language-of-page) | A | [html-has-lang](https://dequeuniversity.com/rules/axe/4.10/html-has-lang?application=axeAPI), [html-lang-valid](https://dequeuniversity.com/rules/axe/4.10/html-lang-valid?application=axeAPI), [html-xml-lang-mismatch](https://dequeuniversity.com/rules/axe/4.10/html-xml-lang-mismatch?application=axeAPI) |
| Succes criterium 3.1.2 | [Language of Parts](https://www.w3.org/TR/WCAG22/#language-of-parts) | AA | [valid-lang](https://dequeuniversity.com/rules/axe/4.10/valid-lang?application=axeAPI) |
| Succes criterium 3.1.3 | [Unusual Words](https://www.w3.org/TR/WCAG22/#unusual-words) | AAA | geen |
| Succes criterium 3.1.4 | [Abbreviations](https://www.w3.org/TR/WCAG22/#abbreviations) | AAA | geen |
| Succes criterium 3.1.5 | [Reading Level](https://www.w3.org/TR/WCAG22/#reading-level) | AAA | geen |
| Succes criterium 3.1.6 | [Pronunciation](https://www.w3.org/TR/WCAG22/#pronunciation) | AAA | geen |
| Richtlijn 3.2 | [Predictable](https://www.w3.org/TR/WCAG22/#predictable) |  |  |
| Succes criterium 3.2.1 | [On Focus](https://www.w3.org/TR/WCAG22/#on-focus) | A | geen |
| Succes criterium 3.2.2 | [On Input](https://www.w3.org/TR/WCAG22/#on-input) | A | geen |
| Succes criterium 3.2.3 | [Consistent Navigation](https://www.w3.org/TR/WCAG22/#consistent-navigation) | AA | geen |
| Succes criterium 3.2.4 | [Consistent Identification](https://www.w3.org/TR/WCAG22/#consistent-identification) | AA | geen |
| Succes criterium 3.2.5 | [Change on Request](https://www.w3.org/TR/WCAG22/#change-on-request) | AAA | [meta-refresh-no-exceptions](https://dequeuniversity.com/rules/axe/4.10/meta-refresh-no-exceptions?application=axeAPI) |
| Succes criterium 3.2.6 | [Consistent Help](https://www.w3.org/TR/WCAG22/#consistent-help) | A | geen |
| Richtlijn 3.3 | [Input Assistance](https://www.w3.org/TR/WCAG22/#input-assistance) |  |  |
| Succes criterium 3.3.1 | [Error Identification](https://www.w3.org/TR/WCAG22/#error-identification) | A | geen |
| Succes criterium 3.3.2 | [Labels or Instructions](https://www.w3.org/TR/WCAG22/#labels-or-instructions) | A | [form-field-multiple-labels](https://dequeuniversity.com/rules/axe/4.10/form-field-multiple-labels?application=axeAPI) |
| Succes criterium 3.3.3 | [Error Suggestion](https://www.w3.org/TR/WCAG22/#error-suggestion) | AA | geen |
| Succes criterium 3.3.4 | [Error Prevention (Legal, Financial, Data)](https://www.w3.org/TR/WCAG22/#error-prevention-legal-financial-data) | AA | geen |
| Succes criterium 3.3.5 | [Help](https://www.w3.org/TR/WCAG22/#help) | AAA | geen |
| Succes criterium 3.3.6 | [Error Prevention (All)](https://www.w3.org/TR/WCAG22/#error-prevention-all) | AAA | geen |
| Succes criterium 3.3.7 | [Redundant Entry](https://www.w3.org/TR/WCAG22/#redundant-entry) | A | geen |
| Succes criterium 3.3.8 | [Accessible Authentication (Minimum)](https://www.w3.org/TR/WCAG22/#accessible-authentication-minimum) | AA | geen |
| Succes criterium 3.3.9 | [Accessible Authentication (Enhanced)](https://www.w3.org/TR/WCAG22/#accessible-authentication-enhanced) | AAA | geen |
| Principe 4 | [Robust](https://www.w3.org/TR/WCAG22/#robust) |  |  |
| Richtlijn 4.1 | [Compatible](https://www.w3.org/TR/WCAG22/#compatible) |  |  |
| Succes criterium 4.1.1 | [Parsing](https://www.w3.org/TR/WCAG22/#parsing) | A | [duplicate-id-active](https://dequeuniversity.com/rules/axe/4.10/duplicate-id-active?application=axeAPI), [duplicate-id](https://dequeuniversity.com/rules/axe/4.10/duplicate-id?application=axeAPI) |
| Succes criterium 4.1.2 | [Name, Role, Value](https://www.w3.org/TR/WCAG22/#name-role-value) | A | [area-alt](https://dequeuniversity.com/rules/axe/4.10/area-alt?application=axeAPI), [aria-allowed-attr](https://dequeuniversity.com/rules/axe/4.10/aria-allowed-attr?application=axeAPI), [aria-braille-equivalent](https://dequeuniversity.com/rules/axe/4.10/aria-braille-equivalent?application=axeAPI), [aria-command-name](https://dequeuniversity.com/rules/axe/4.10/aria-command-name?application=axeAPI), [aria-conditional-attr](https://dequeuniversity.com/rules/axe/4.10/aria-conditional-attr?application=axeAPI), [aria-deprecated-role](https://dequeuniversity.com/rules/axe/4.10/aria-deprecated-role?application=axeAPI), [aria-hidden-body](https://dequeuniversity.com/rules/axe/4.10/aria-hidden-body?application=axeAPI), [aria-hidden-focus](https://dequeuniversity.com/rules/axe/4.10/aria-hidden-focus?application=axeAPI), [aria-input-field-name](https://dequeuniversity.com/rules/axe/4.10/aria-input-field-name?application=axeAPI), [aria-prohibited-attr](https://dequeuniversity.com/rules/axe/4.10/aria-prohibited-attr?application=axeAPI), [aria-required-attr](https://dequeuniversity.com/rules/axe/4.10/aria-required-attr?application=axeAPI), [aria-roledescription](https://dequeuniversity.com/rules/axe/4.10/aria-roledescription?application=axeAPI), [aria-roles](https://dequeuniversity.com/rules/axe/4.10/aria-roles?application=axeAPI), [aria-toggle-field-name](https://dequeuniversity.com/rules/axe/4.10/aria-toggle-field-name?application=axeAPI), [aria-tooltip-name](https://dequeuniversity.com/rules/axe/4.10/aria-tooltip-name?application=axeAPI), [aria-valid-attr-value](https://dequeuniversity.com/rules/axe/4.10/aria-valid-attr-value?application=axeAPI), [aria-valid-attr](https://dequeuniversity.com/rules/axe/4.10/aria-valid-attr?application=axeAPI), [button-name](https://dequeuniversity.com/rules/axe/4.10/button-name?application=axeAPI), [duplicate-id-aria](https://dequeuniversity.com/rules/axe/4.10/duplicate-id-aria?application=axeAPI), [frame-title-unique](https://dequeuniversity.com/rules/axe/4.10/frame-title-unique?application=axeAPI), [frame-title](https://dequeuniversity.com/rules/axe/4.10/frame-title?application=axeAPI), [input-button-name](https://dequeuniversity.com/rules/axe/4.10/input-button-name?application=axeAPI), [input-image-alt](https://dequeuniversity.com/rules/axe/4.10/input-image-alt?application=axeAPI), [label](https://dequeuniversity.com/rules/axe/4.10/label?application=axeAPI), [link-name](https://dequeuniversity.com/rules/axe/4.10/link-name?application=axeAPI), [nested-interactive](https://dequeuniversity.com/rules/axe/4.10/nested-interactive?application=axeAPI), [select-name](https://dequeuniversity.com/rules/axe/4.10/select-name?application=axeAPI), [summary-name](https://dequeuniversity.com/rules/axe/4.10/summary-name?application=axeAPI) |
| Succes criterium 4.1.3 | [Status Messages](https://www.w3.org/TR/WCAG22/#status-messages) | AA | geen |

## User assistance

Capability of a product to be used by people with the widest range of characteristics and capabilities to achieve specified goals in a specified context of use.

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

## Self-descriptiveness

Capability of a product to present appropriate information, where needed by the user, to make its capabilities and use immediately obvious to the user without excessive interactions with a product or other resources.

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

## Taal en leesbaarheid

Naast de aan NEN-ISO/IEC 25010:2023 ontleende hoofdeigenschap bruikbaarheid zijn voor de gebruikskwaliteit van {het product} 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 | Realisatie in | Realisatie door | Bewijs |
| 1 | De applicatie gebruikt maximaal taalniveau B1 | {prio} | [Aanbevolen richtlijn](https://www.communicatierijk.nl/vakkennis/rijkswebsites/aanbevolen-richtlijnen/taalniveau-b1) | {software} | {partij} | {bewijs} |
| 2 | De applicatie ondersteunt {ondersteunde talen} | {prio} | {rationale} | {software} | ICTU | {bewijs} |

# Reliability

Capability of a product to perform specified functions under specified conditions for a specified period of time without interruptions and failures.

## Faultlessness

Capability of a product to perform specified functions without fault under normal operation.

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

## Availability

Capability of a product to be operational and accessible when required for use.

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

## Fault tolerance

Capability of a product to operate as intented despite the presence of hardware or software faults.

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

## Recoverability

Capability of a product in the event of an interruption or a failure to recover the data directly affected and re-establish the desired state of the system.

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

# Security

Capability of a product to protect information and data so that persons or other products have the degree of data access appropriate to their types and levels of authorization, and to defend against attack patterns by malicious actors.

## 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 | Realisatie in | Realisatie door | 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 | {software, hardware, combinatie} | {partij} | {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 | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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 | {software, hardware, combinatie} | {partij} | {bewijs} |
| 5a | In de applicatie zijn de autorisaties op een beheersbare wijze geordend. De applicatie maakt daartoe gebruik van autorisatiegroepen | {prio} |  | {software, hardware, combinatie} | {partij} | {bewijs} |
| 5b | Op basis van taken, verantwoordelijkheden en bevoegdheden zijn de niet te verenigen taken en autorisaties geïdentificeerd | {prio} |  | {software, hardware, combinatie} | {partij} | {bewijs} |
| 5c | Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol | {prio} |  | {software, hardware, combinatie} | {partij} | {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} |  | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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 | {software, hardware, combinatie} | {partij} | {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. | {software, hardware, combinatie} | {partij} | {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 | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {bewijs} |
| 15 | (Web)applicaties 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} | {software, hardware, combinatie} | {partij} | {bewijs} |
| 16 | Applicaties hebben geen run-time afhankelijkheid van externe codebronnen | {prio} | {rationale} | {software, hardware, combinatie} | {partij} | {bewijs} |
| 17 | Applicaties zijn gemaakt met de op het moment van uitleveren meest recente en/of door de leverancier (lees in het geval van open source: de community) aanbevolen versies van externe bibliotheken, raamwerken of andersoortige bouwblokken. Applicaties gebruiken alleen externe bibliotheken, raamwerken of andersoortige bouwblokken waarvoor de leverancier beveiligingsupdates uitbrengt. Applicaties ondersteunen alleen besturingssystemen of browsers waarvoor de leverancier beveiligingsupdates uitbrengt | {prio} | {rationale} | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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 | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {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} |  | {software, hardware, combinatie} | {partij} | {bewijs} |
| 20b | De webapplicatie toont alleen noodzakelijke informatie in HTTP-headers die van belang is voor het functioneren van HTTP | {prio} |  | {software, hardware, combinatie} | {partij} | {bewijs} |
| 20c | De webserver gebruikt alleen de HTTP-functionaliteiten die nodig zijn voor het functioneren van de webapplicatie | {prio} |  | {software, hardware, combinatie} | {partij} | {bewijs} |
| 21 | De aan de gebruiker aangeboden scripts / code bevat geen commentaar | {prio} | Voorkomt misbruik van het commentaar | {software, hardware, combinatie} | {partij} | {bewijs} |
| 22 | De aan de gebruiker getoonde informatie bevat geen directory listings | {prio} | Voorkomt misbruik van de directory listing | {software, hardware, combinatie} | {partij} | {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} | {software, hardware, combinatie} | {partij} | {bewijs} |
| 24 | In de (web)applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht | {prio} | {rationale}{software, hardware, combinatie} | {partij} |  | {bewijs} |
| {nr} | {eis} | {prio} | {rationale} | {software, hardware, combinatie} | {partij} | {software, hardware, combinatie} |

## Confidentiality

Capability of a product to ensure that data are accessible only to those authorized to have access.

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

## Integrity

Capability of a product to ensure that the state of its system and data are protected from unauthorized modification or deletion either by malicious action or computer error.

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

## Non-repudiation

Capability of a product to prove that actions or events have taken place, so that the events or actions cannot be repudiated later.

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

## Accountability

Capability of a product to enable actions of an entity to be traced uniquely to the entity.

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

## Authenticity

Capability of a product to prove that the identity of a subject or resource is the one claimed.

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

## Resistance

Capability of a product to sustain operations while under attack from a malicious actor.

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

# Maintainability

Capability of a product to be modified by the intended maintainers with effectiveness and efficiency.

## Modularity

Capability of a product to limit changes to one component from affecting other components.

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

## Reusability

Capability of a product to be used as assets in more than one system, or in building other assets.

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

## Analysability

Capability of a product to be effectively and efficiently assessed regarding the impact of an intended change to one or more of its parts, to diagnose it for deficiencies or causes of failures, or to identify parts to be modified.

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

## Modifiability

Capability of a product to be effectively and efficiently modified without introducing defects or degrading existing product quality.

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

## Testability

Capability of a product to enable an objective and feasible test to be designed and performed to determine whether a requirement is met.

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

# Flexibility

Capability of a product to be adapted to changes in its requirements, contexts of use, or system environment.

## Adaptability

Capability of a product to be effectively and efficiently adapted for or transferred to different hardware, software or other operational or usage environments.

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

## Scalability

Capability of a product to handle growing or shrinking workloads or to adapt its capacity to handle variability.

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

## Installability

Capability of a product to be effectively and efficiently installed successfully and/or uninstalled in a specified environment.

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

## Replaceability

Capability of a product to replace another specified product for the same purpose in the same environment.

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

# Safety

Capability of a product under defined conditions to avoid a state in which human life, health, property, or the environment is endangered.

## Operational constraint

Capability of a product to constrain its operation to within safe parameters or states when encountering operational hazard.

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

## Risk identification

Capability of a product to identify a course of events or operations that can expose life, property or environment to unacceptable risk.

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

## Fail safe

Capability of a product to automatically place itself in a safe operating mode, or to revert to a safe condition in the event of a failure.

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

## Hazard warning

Capability of a product to provide warnings of unacceptable risks to operations or internal controls so that they can react in sufficient time to sustain safe operations.

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

## Safe integration

Capability of a product to maintain safety during and after integration with one or more components.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 verrichte handelingen |
| **authenticatie** | het vaststellen van de identiteit van een **actor** |
| **autorisatie** | aan een **actor** toegekende rechten |
| **beheerorganisatie** | een (samenwerkingsverband van) organisatie(s) die in opdracht van een **opdrachtgevende organisatie** het **operationeel beheer**, applicatief beheer en/of functioneel beheer van **software** uitvoert |
| **BIA** | Een business impact analyse is een methode om de mogelijke bedrijfsimpact te bepalen die een organisatie zou kunnen ervaren door een incident, dat de functionaliteit van of de informatie in een applicatie in gevaar brengt [NORA] |
| **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 |
| **DPIA** | Een data protection impact assessment is een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen zodat de organisatie maatregelen kan nemen om deze risico’s te verkleinen |
| **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** | Een globaal functioneel ontwerp beschrijft de functionele werking van een product op hoofdlijnen, voor specifieke use cases |
| **IB-plan** | Een informatiebeveiligingsplan beschrijft binnen welke kaders bescherming geleverd wordt tegen welke dreigingen en met welke maatregelen die bescherming vorm krijgt |
| **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** | De infrastructuurarchitectuur beschrijft de technische infrastructuur van een product op hoofdlijnen, in termen van hardwareonderdelen en -relaties (housing, hardware, virtuals, standaard software en middleware) |
| **interactie-ontwerp** | Een interactie-ontwerp beschrijft de interacties tussen gebruikers en het systeem en de user experience daarbij |
| **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** | Een minimum viable product is een eerste versie van een product, die zo vroeg mogelijk wordt uitgerold naar de gebruikers, met net voldoende functionaliteit om het gestelde doel te behalen en niet meer dan dat |
| **MTP** | Een mastertestplan beschrijft de aanpak van het testen van een product op hoofdlijnen, in termen van strategie, activiteiten, afhankelijkheden en de op te leveren resultaten |
| **MVP** | **minimum viable product** |
| **NFE** | Niet-functionele eisen specificeren criteria om de kwaliteit van de software te beoordelen |
| **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** |
| **PKI** | public key infrastructure |
| **PRA** | Een productrisicoanalyse is een analyse van het te testen product die resulteert in een overzicht van wat de meer of minder risicovolle kenmerken en delen van het te testen product zijn, zodat de grondigheid van testen hieraan gerelateerd kan worden |
| **product backlog** | De product backlog is een levende, geordende lijst van wat nodig is om het product te verbeteren. Het is de enige bron van het werk dat door het **Scrumteam** gedaan wordt [Scrumgids] |
| **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 [NORA] |
| **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** | Een software-architectuurdocument beschrijft de technische werking van een product op hoofdlijnen, in termen van softwarecomponenten, hun functies en hun onderlinge interacties en samenhang voor specifieke use cases |
| **Scrum** | Scrum is een lichtgewicht raamwerk dat mensen, teams en organisaties helpt om waarde te creёren door middel van adaptieve oplossingen voor complexe problemen [Scrumgids] |
| **Scrummaster** | De Scrummaster is verantwoordelijk voor het opzetten van **Scrum**, zoals staat beschreven in de Scrumgids [Scrumgids] |
| **Scrumteam** | Een Scrumteam bestaat uit één **Scrummaster**, één **product owner** en **ontwikkelaars** (*developers* in de Scrumgids) [Scrumgids] |
| **softwarearchitectuur** | een **architectuur** die vooral de softwareonderdelen en -relaties (processen, modules, interfaces, datamodel) van een systeem beschrijft |
| **software delivery manager** | organiseert het ontwikkelen en opleveren van **software** conform de vastgestelde eisen en de Kwaliteitsaanpak en rapporteert aan de **projectleider** |
| **software** | software is de verzameling instructies die bepalen wat een computer uitvoert en is uiteindelijk wat de gebruiker ziet, ervaart en waarmee hij interacteert |
| **softwareontwikkeling** | een activiteit die nieuwe **software** maakt en/of bestaande software aanpast |
| **softwareontwikkelproject** | een **project** dat de oplevering van **software** als enige of voornaamste projectresultaat heeft |
| **solution architectuur** | beschrijving van de gewenste oplossing van een specifiek probleem, of het eindresultaat van een **project** [NORA] |
| **technische schuld** | eigenschappen van de **software** die de lange-termijninzetbaarheid en onderhoudbaarheid bedreigen |
| **TVA** | Een threat and vulnerability assessment inventariseert de betrouwbaarheidseisen die aan de bedrijfsprocessen en dientengevolge aan het product worden gesteld, gevolgd door identificatie en analyse van bedreigingen |
| **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 25010:2023](https://www.nen.nl/nen-iso-iec-25010-2023-en-318088) | 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.