ICTU Kwaliteitsaanpak Softwareontwikkeling

Versie 2.5.0-rc.1, 10-02-2023

Inhoudsopgave

1 Inleiding

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: "De Rijksoverheid heeft haar ICT (Informatie- en communicatietechnologie)-projecten niet onder controle". Eén van de fundamentele problemen is dat de risico's, die inherent zijn aan softwareontwikkeling, door organisaties nog onvoldoende worden herkend, erkend en gemitigeerd. Dit terwijl de risico's bij de ontwikkeling van software, binnen het ICT-domein, algemeen bekend zijn en er ook voor veel risico's passende maatregelen bestaan.

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

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

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

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

2 Doelstellingen

De ICTU Kwaliteitsaanpak Softwareontwikkeling heeft drie doelstellingen:

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

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

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

3 Begrippenkader

Deze Kwaliteitsaanpak heeft betrekking op de ICTU-projecten waarin software ontwikkeld wordt. De terminologie in dit document is daarop afgestemd en sluit, waar relevant, aan op andere begrippenkaders.

De bijlage Terminologie en afkortingen bevat een lijst met veel gebruikte begrippen en afkortingen. Een aantal begrippen speelt echter een zodanig prominente rol bij het begrip en het gebruik van de Kwaliteitsaanpak, dat ze hieronder nader zijn toegelicht.

Een **informatiesysteem** is "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" (bron: VIR 2007, NORA).

Software is de verzameling instructies die bepalen wat een computer uitvoert en is uiteindelijk wat de gebruiker ziet, ervaart en waarmee hij interacteert. In de dagelijkse praktijk en communicatie van ICTU wordt "programmatuur", uit de vorige definitie, aangeduid met "software".

Vaak kunnen de termen "broncode" en "software" onderling uitgewisseld worden, maar soms is het van belang onderscheid te maken. **Broncode** is leesbaar voor mensen en drukt de intentie van een programmeur uit. Om een computer broncode te laten "uitvoeren", is een vertaalslag nodig naar voor een computer begrijpelijke instructies. Broncode bij ICTU is bijvoorbeeld geschreven in de programmeertalen Java of C#.

Een **softwareontwikkelproject** is een project dat de oplevering van software als enige of voornaamste projectresultaat heeft.

4 Leeswijzer

Dit document "ICTU Kwaliteitsaanpak Softwareontwikkeling", verder ook aangeduid met 'de Kwaliteitsaanpak', is bedoeld voor software en gerelateerde producten, voor processen waarmee die producten worden gerealiseerd en voor de overkoepelende organisatie waarin op projectbasis wordt gewerkt (ICTU). Dit betekent dat deze Kwaliteitsaanpak betrekking heeft op de drie aspecten van softwareontwikkeling:

1. Producten - Het eerste deel van de Kwaliteitsaanpak betreft de eigenschappen van de ontwikkelde producten. De broncode valt hieronder, maar ook alle andere producten, zoals eisen, ontwerpen en testscripts.
2. Processen - Het tweede deel gaat over het ontwikkelproces; werkwijze, gebruik van hulpmiddelen en projectaanpak.
3. Organisatie - Het derde deel betreft de organisatie waarbinnen projecten worden uitgevoerd: ICTU; dit gaat over de samenhang tussen projecten en de faciliteiten die projecten ter beschikking moeten hebben.

De drie aspecten komen hieronder in meer detail aan bod in de vorm van maatregelen die ICTU heeft getroffen om de risico's die samenhangen met softwareontwikkeling te mitigeren. De praktijkrichtlijn “Risicobeheersing bij ontwikkeling en onderhoud van maatwerksoftware” (NPR 5326:2019) beschrijft veelvoorkomende risico's van maatwerksoftwareontwikkeling en adviseert bijbehorende risicobeheersmaatregelen. Bijlage Relatie met NEN NPR 5326 beschrijft hoe de maatregelen in deze Kwaliteitsaanpak samenhangen met de maatregelen die de NPR 5326 adviseert.

De beschrijving van elke maatregel is voorzien van een rationale: waarom behoort de maatregel tot de Kwaliteitsaanpak? Waar mogelijk verwijst de rationale naar maatregelen uit standaarden en richtlijnen die overeenkomen met de door ICTU getroffen maatregelen.

Bij de omschrijving van de maatregelen is gebruik gemaakt van de volgende rollen om aan te geven wie verantwoordelijkheid draagt voor het uitvoeren van de maatregelen:

- Project: de tijdelijke organisatie die de software ontwikkelt en onderhoudt. Het project bestaat uit medewerkers van ICTU, van de opdrachtgever en mogelijk ook van de beheerorganisatie of andere partijen. De softwareontwikkeling binnen het project gebeurt door één of meer Scrumteams, bestaande uit een product owner, ontwikkelaars en een Scrummaster. De product owner is altijd een medewerker van de opdrachtgevende organisatie.
- Projectleider: de ICTU-medewerker verantwoordelijk voor uitvoering van het project,
- Software delivery manager: organiseert het ontwikkelen en opleveren van software conform de vastgestelde eisen en de Kwaliteitsaanpak, rapporteert aan de projectleider,
- Kwaliteitsmanager: controleert en borgt de kwaliteit van software conform de vastgestelde eisen en de Kwaliteitsaanpak, rapporteert aan de projectleider.

Projecten bij ICTU die software ontwikkelen en/of onderhouden volgens deze Kwaliteitsaanpak, kunnen ondersteuning krijgen van de afdelingen ICTU Software Diensten (ISD) en ICTU Software Expertise (ISE). ISD levert ontwikkel- en

testomgevingen, tools en ondersteunende diensten. ISE levert expertise in de vorm van software delivery managers, kwaliteitsmanagers en software-ontwikkelaars. ISE onderhoudt tevens deze Kwaliteitsaanpak. ISD en ISE zijn niet verantwoordelijk voor de projectuitvoering, maar voor het bieden van expertise en diensten om projecten in staat te stellen efficiënt en effectief volgens de Kwaliteitsaanpak te werken.

De Kwaliteitsaanpak is een evoluerende aanpak, gebaseerd op de ervaringen die ICTU continu opdoet in de projecten waarin ICTU samen met opdrachtgevers maatwerksoftware ontwikkelt en onderhoudt. ICTU hanteert daarbij de vuistregel dat als tenminste 80% van de projecten minstens 80% van de tijd een bepaalde werkwijze hanteren, voor die werkwijze een maatregel in de Kwaliteitsaanpak wordt opgenomen. Maar het kan ook voorkomen dat maatregelen om andere redenen landen in de Kwaliteitsaanpak; denk aan het toegankelijk maken van software dat wettelijk verplicht is.

De maatregelen vormen het startpunt voor de aanpak van ieder ICTU-softwareproject, maar bieden daarbij ruimte voor variatie of alternatieve invulling. Bijvoorbeeld stelt de Kwaliteitsaanpak: software wordt minimaal bij iedere grote release of tenminste twee keer per jaar onderworpen aan een beveiligingstest door beveiligingsexperts die ICTU daarvoor inhuurt (zie M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen). Een alternatief is dat de opdrachtgever de verantwoordelijkheid neemt voor het laten uitvoeren van beveiligingstests. Hierover maakt de projectleider nadere afspraken met de opdrachtgever. De Kwaliteitsaanpak is dus zowel voorschrijvend als beschrijvend. Voorschrijvend omdat ICTU verwacht dat projecten die maatwerksoftware ontwikkelen en onderhouden de aanpak toepassen, en alleen aanpassen als daar een goede reden voor is, en mits dat wettelijk is toegestaan. Tegelijkertijd is de aanpak beschrijvend omdat de meeste maatregelen voor de meeste projecten de meeste tijd van toepassing zijn en worden toegepast. Zoals blijkt uit de self-assessment die ICTU regelmatig uitvoert op de toepassing van de Kwaliteitsaanpak.

5 Producten

5.1 M31: Het project beschikt over vastgestelde informatie

M31: Het project beschikt over vastgestelde informatie
Voor een goede uitvoering van het project is specifieke informatie nodig. De opdrachtgever zorgt dat het project bij de start van de voorfase inzicht heeft in de informatie die typisch wordt vastgelegd in een projectstartarchitectuur, business impact analysis en privacy impact assessment. Waar nodig werkt de opdrachtgever de informatie bij tijdens de voorfase en realisatiefase.

De opdrachtgever zorgt dat het project vanaf de start van de voorfase beschikt over:

1. Projectstartarchitectuur,
2. Business impact analysis,
3. Privacy impact assessment.

Als de benodigde informatie niet gereed is bij de start van de voorfase dan maken opdrachtgever en ICTU nadere afspraken over de manier waarop de benodigde informatie nog tijdens de voorfase beschikbaar komt voor het project.

Projectstartarchitectuur

Een projectstartarchitectuur (PSA) is bedoeld om te borgen dat nieuwe ontwikkelingen en veranderingen in samenhang worden gerealiseerd en passen binnen de toekomstig gewenste informatievoorziening. Een PSA bevat in ieder geval de volgende onderwerpen:

- Een beschrijving van de doelen en ambities waaraan het project bijdraagt en invulling geeft. Dus niet de projectdoelen en -ambitie.
- Een afbakening van het project en de context van de voorziening/oplossing die het project gaat realiseren gezien als een 'black box'. Denk o.a. ook aan relaties met andere projecten en generieke en specifieke diensten (services).
- De belangrijkste functies van de door het project te realiseren voorziening, informatiestromen en koppelvlakken.
- Een beschrijving van de belangrijkste belanghebbenden en/of betrokken ketenpartijen.
- Een concretisering van kaders en randvoorwaarden die van toepassing zijn.
- Beleidsuitgangspunten (drijfveren en doelen), zowel voor het specifieke project als algemeen voor de organisatie en visie (oplossingsrichting).
- Standaarden en normen (open standaarden van het Forum Standaardisatie en domeinspecifieke standaarden).

Zie http://www.noraonline.nl/wiki/PSA.

Business impact analysis

In een business impact analysis (BIA) legt de opdrachtgevende organisatie vast hoe belangrijk informatiebeveiliging is voor de eigen bedrijfsvoering/processen. Naast de gevoeligheid voor incidenten komt hierin ook de 'risk appetite' van de organisatie tot uiting. Alleen de organisatie zelf kan hierover een uitspraak doen.

Privacy impact assessment

In een privacy impact assessment (PIA) legt de vragende organisatie vast wat de privacy-gevoeligheid is van de gegevens die in een proces of informatiesysteem worden verzameld en verwerkt. De rechtmatigheid van de verwerking wordt beoordeeld. En de PIA stelt grenzen aan de gegevens die mogen worden verzameld en verwerkt. Zicht op privacygevoelige gegevens en het (laten) treffen van adequate en afdoende beschermingsmaatregelen is een wettelijke plicht die een organisatie niet aan een andere partij kan overdragen.

Indien een PIA niet nodig is, is een verklaring daaromtrent vereist.

Aanvullende informatie

Waar mogelijk stelt de opdrachtgever ook andere relevante informatie ter beschikking aan het project zoals een eventueel programma van eisen, procesbeschrijvingen van te ondersteunen bedrijfsprocessen, documentatie van te koppelen systemen, documentatie van de te gebruiken voorzieningen voor bijvoorbeeld authenticatie en autorisatie, beveiligingsbeleid, beheeracceptatiecriteria en verder te hanteren kaders en richtlijnen.

Rationale

De genoemde producten hebben tot doel om de benodigde omvang, kosten en doorlooptijd van de voorfase te kunnen schatten. De projectstartarchitectuur vormt input voor de tijdens de voorfase te ontwikkelen producten zoals functionele en niet-functionele eisen, functioneel ontwerp en softwarearchitectuur. Een BIA en eventuele PIA zijn richtinggevend voor de in de voorfase te selecteren beveiligingsmaatregelen.

Als deze producten er niet zijn, dan moeten ze alsnog worden gemaakt. Dat vereist grote betrokkenheid van de organisatie van de opdrachtgever, en duurt in de regel lang. De aanwezigheid en compleetheid van deze producten is dus belangrijke informatie voor de raming van de voorfase.

5.2 M01: Het project levert in elke fase vastgestelde producten en informatie op

M01: Het project levert in elke fase vastgestelde producten en informatie op
Iedere projectfase levert specifieke informatie op. De voorfase levert inzicht in de functionele en niet-functionele eisen, ontwerp en architectuur, testplannen, operationele risico's, en benodigde kwaliteitsmaatregelen. Deze informatie wordt tijdens de realisatiefase waar nodig bijgewerkt. De realisatiefase levert één of meerdere werkende versies van de software met regressietests, aangevuld met een vrijgaveadvies, release notes en installatiedocumentatie.

Opdrachtgever, ICTU, beheerpartij en andere meewerkende partijen, leveren samen de volgende informatie op:

Plan van aanpak

Het plan van aanpak voor de voorfase en het plan van aanpak voor de realisatiefase beschrijven de in deze fasen te realiseren producten, en de planning, werkwijze en verantwoordelijkheden voor de totstandkoming van die producten.

Beschrijving van functionele eisen

De beschrijving van functionele eisen bestaat uit epics en/of user stories, eventueel aangevuld met use cases. De beschrijving bevat tevens eisen voor ondersteuning van beheerfuncties, die door de beoogd beheerder gesteld worden, en voor logging, inclusief de globale inhoud van te loggen business events (gebeurtenissen op procesniveau) en de daarvoor geldende bewaartermijnen.

Bronnen van de opdrachtgever zoals de projectstartarchitectuur, een programma van eisen en procesbeschrijvingen vormen het startpunt voor de functionele eisen. Tijdens het project worden use cases in samenwerking met de product owner vertaald naar user stories.

Beschrijving van niet-functionele eisen

Niet-functionele eisen specificeren criteria om het functioneren van de software te beoordelen, maar beschrijven niet het specifieke gedrag zelf. Voor de beschrijving en onderverdeling van niet-functionele eisen gebruikt ICTU:

- NEN-ISO/IEC 25010,
- Wet beveiliging netwerk- en informatiesystemen (Wbni),
- Baseline Informatiebeveiliging Overheid (BIO),
- methode Grip op SDD (Secure Software Development) van het Centrum Informatiebeveiliging en Privacybescherming (CIP),
- Algemene verordening gegevensbescherming (AVG),
- ISO 9241-210:2019 Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems,
- hoofdstuk 9 van de Europese Standaard EN 301 549 — dit is gelijk aan de Web Content Accessibility Guidelines versie 2.1, niveau A en AA.

De beschrijving van niet-functionele eisen moet expliciet aandacht besteden aan de

door de beoogd beheerder gewenste ondersteuning van beheerfuncties. Bepaalde niet-functionele eisen kunnen aanleiding zijn tot het treffen van beveiligingsmaatregelen. Door deze eisen expliciet in de voorfase te benoemen, wordt voorkomen dat de bijbehorende beveiligingsmaatregelen achteraf moeten worden toegevoegd.

Overheidsorganisaties moeten een toegankelijkheidsverklaring op hun websites plaatsen. Indien gewenst ondersteunt ICTU bij het opstellen van de toegankelijkheidsverklaring.

Bronnen van de opdrachtgever zoals procesbeschrijvingen, privacy impact assessment (PIA), beheeracceptatiecriteria, beveiligingsbeleid en projectstartarchitectuur vormen het startpunt voor de niet-functionele eisen.

Product backlog

De product backlog is een geprioriteerd overzicht van alle nog te realiseren functionele en niet-functionele eigenschappen van de software. De product owner is de eigenaar van de product backlog. De zaken op de lijst zijn normaal gesproken in de vorm van een epic of user story. Hierin staat:

- *Wat* er gemaakt moet worden,
- *Waarom*,
- en voor *wie*.

De product owner is verantwoordelijk voor de inhoud en bepaalt de prioritering van de eisen. Er staan ook ruwe schattingen bij van de waarde voor de organisatie en van de ontwikkelkosten.

Zie http://www.scrumguides.org/scrum-guide.html#artifacts-productbacklog.

Ontwerp- en architectuurdocumentatie (software, interactie, infrastructuur)

De ontwerp- en architectuurdocumentatie beschrijft de opzet van de te bouwen software in de context waarbinnen het moet opereren en de ontwerpkeuzes en -principes die zijn gevolgd. Die documentatie laat tevens zien hoe de software aan de gestelde functionele en niet-functionele eisen voldoet.

Het project legt ontwerp- en architectuurinformatie vast in verschillende documenten en producten, zoals een softwarearchitectuurdocument (SAD), een infrastructuurarchitectuur (IA), een globaal functioneel ontwerp (GFO) en een prototype en/of interactieontwerp.

Het softwarearchitectuurdocument verschaft een compleet overzicht van en rationale voor de architectuur van de te ontwikkelen software, waarbij diverse relevante views diverse aspecten van de software belichten. Zie bijvoorbeeld http://www.win.tue.nl/~wstomv/edu/2ip30/references/Kruchten-4+1-view.pdf; andere manieren van architectuurbeschrijving zijn ook toegestaan.

De infrastructuurarchitectuur beschrijft de topologie van de implementatie-omgeving waaronder protocollen, beveiligingsniveaus en services. Deze architectuur biedt een logische afbeelding van de eisen naar de implementatie-omgeving en geeft onderbouwing voor de gemaakte keuzes.

Een prototype is een eerste, ruwe versie van de applicatie. Het prototype illustreert waar men uiteindelijk met de toepassing naar toe wil. Het maakt ideeën tastbaar en creëert een eerste indruk van structuur, ontwerp en functionaliteit.

Testdocumentatie

De testplannen bestaan uit een mastertestplan (MTP), gemaakt op basis van een productrisicoanalyse (PRA), en detailtestplannen. Het doel van een mastertestplan is om betrokkenen bij het testproces te informeren over de strategie, aanpak, activiteiten, inclusief de onderlinge relaties en afhankelijkheden, en de op te leveren producten met betrekking tot het testtraject. Het mastertestplan beschrijft deze strategie, aanpak, activiteiten en eindproducten, die in de detailtestplannen verder worden gedetailleerd.

Opdrachtgever is verantwoordelijk voor het mastertestplan. Het project maakt een detailtestplan voor de testsoorten die tijdens de realisatiefase door het project worden uitgevoerd. Voor testen die onder verantwoordelijkheid van het project door een derde partij worden uitgevoerd, denk aan penetratietesten en evaluaties van gebruikskwaliteit, worden aparte detailtestplannen gemaakt.

Logische testgevallen worden vastgelegd en gekoppeld met use cases en user stories. Fysieke testgevallen worden vastgelegd in het formaat van de gebruikte tooling en gekoppeld met de logische testgevallen. Op basis hiervan worden testrapportages gegenereerd die laten zien dat alle use cases en user stories zijn getest en dat die tests zijn geslaagd.

Informatiebeveiligingsplan

Het informatiebeveiligingsplan vormt een handzaam document dat uitlegt binnen welke kaders bescherming geleverd wordt tegen welke dreigingen en hoe die bescherming vorm krijgt. Mogelijke bronnen voor het informatiebeveiligingsplan zijn de business impact analysis (BIA), privacy impact assessment (PIA) en de threat and vulnerability assessment (TVA). De TVA wordt tijdens de voorfase opgesteld op basis van de resultaten van de BIA, de eventuele PIA en inhoud van de ontwerp- en architectuurdocumentatie. Een TVA levert een deel van een traceerbare onderbouwing voor de te treffen beveiligingsmaatregelen.

Het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007) bevat een methode om te komen tot een systematische aanpak van informatiebeveiliging. Eén van de vereisten van het VIR 2007 is dat voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied een afhankelijkheids- en kwetsbaarheidsanalyse (A&K-analyse) wordt uitgevoerd. Bij ICTU wordt daarvoor een TVA gebruikt. De betrouwbaarheidseisen, die aan de bedrijfsprocessen en dientengevolge aan het informatiesysteem of verantwoordelijkheidsgebied worden gesteld, worden tijdens een afhankelijkheidsanalyse geïnventariseerd. Vervolgens worden de bedreigingen geïdentificeerd en geanalyseerd.

Kwaliteitsplan

Het kwaliteitsplan beschrijft de standaard kwaliteitsmaatregelen die ICTU-projecten treffen om goede kwaliteit software te realiseren. Als er bijzondere of hoge niet-functionele eisen zijn, beschrijft het kwaliteitsplan ook de extra projectspecifieke kwaliteitsmaatregelen die het project treft om deze eisen te realiseren.

Deploybare versie van de software

Het project levert deploybare versies van de software in een formaat dat is afgestemd met de beheerpartij.

Broncode, inclusief de benodigdheden voor het bouwen van de software

Het project levert de broncode, inclusief configuratiebestanden en buildscripts, nodig voor het bouwen van de software.

Regressietests, inclusief de benodigdheden voor het uitvoeren van de tests

Het project levert de regressietests, inclusief configuratiebestanden en scripts nodig voor het uitvoeren van de tests.

Deploymentdocumentatie

De deploymentdocumentatie bevat informatie over de eisen die een applicatie stelt aan een omgeving en de stappen die nodig zijn om de applicatie in die omgeving veilig te installeren en configureren. De documentatie bevat daartoe onder meer aanwijzingen voor de HTTP-header en -request-configuratie van de webserver en voor het verwijderen van overbodige header-informatie zoals de 'Server'-header. Ook zijn er aanwijzingen voor veilige configuratie(s) van (externe) toegang tot de beheerinterface. De documentatie bevat daarnaast in ieder geval een beschrijving van de protocollen en services die de applicatie aanbiedt, de protocollen, services en accounts die het product gebruikt en de protocollen, services en accounts die de applicatie gebruikt voor beheer.

Software bill of materials

Voor elke release stelt het project een "software bill of materials" op: een overzicht van de gebruikte libraries, frameworks, componenten en andere software(deel)producten in de release. Software draagt inherent het risico in zich van verborgen fouten. Deze fouten kunnen mogelijk misbruikt worden, waardoor (beveiligings)problemen ontstaan. Met dit overzicht heeft de opdrachtgever of diens beheerpartij informatie over de gebruikte software(deel)producten, die geraadpleegd kan worden wanneer fouten in software bekend wordt, zodat een risico-inschatting gemaakt kan worden en eventueel actie kan worden ondernomen.

Release notes

Voor elke release stelt het project release notes op: een overzicht van de wijzigingen in de release. Software delivery manager en opdrachtgever maken afspraken over de opzet van de release notes.

Vrijgaveadvies

Voor elke release stelt het project een vrijgaveadvies op. Het vrijgaveadvies bevat tenminste alle nog openstaande testbevindingen en geconstateerde beveiligingsbevindingen; zie ook M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen en M16: Het project gebruikt tools voor vastgestelde taken. Als er issues zijn, bijvoorbeeld rondom kwaliteit of beveiliging, zijn deze voorzien van een beschreven voorziene impact.

Software delivery manager en opdrachtgever maken afspraken over de opzet van het vrijgaveadvies en de verantwoordelijkheden van betrokken partijen bij de

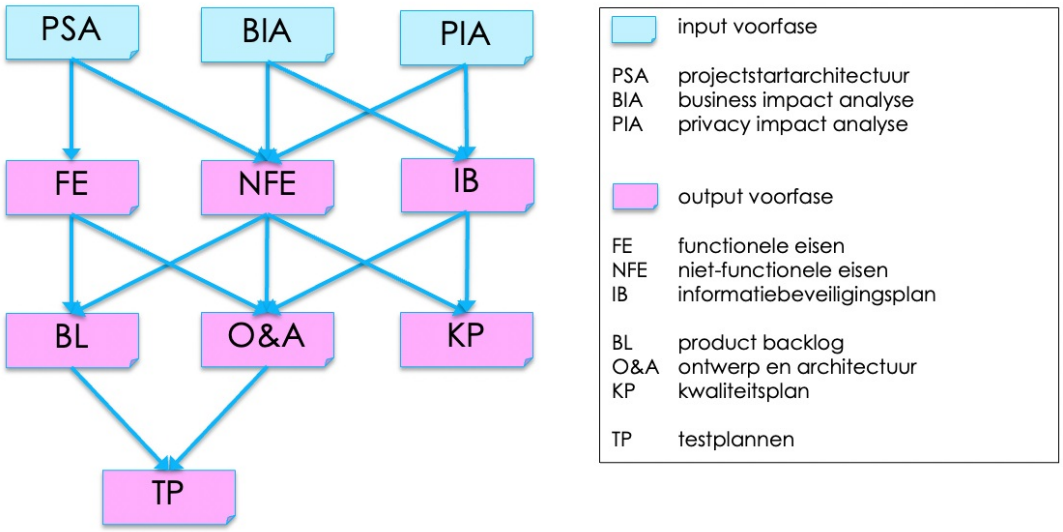
totstandkoming ervan, waaronder ook de beheerpartij.

Due diligence

Als tijdens een project bestaande software dient te worden afgebouwd, onderhouden en/of herbouwd, vindt een onderzoek plaats naar de compleetheid en consistentie van de bestaande softwareproducten aan de hand van de onderstaande tabel (inclusief de deliverables in de kolom 'Realisatiefase') en wordt de kwaliteit van de bestaande softwareproducten getoetst. Dit onderzoek, dat bij ICTU een "due diligence" heet, is onderdeel van de voorfase en wordt uitgevoerd door vertegenwoordigers van ICTU en medewerkers van het desbetreffende project, samen met vertegenwoordigers van de opdrachtgever.

De uitkomsten van het onderzoek bestaan uit een rapportage met tenminste de bevindingen, risico's voor opdrachtgever en ICTU, en mitigerende maatregelen. Daarnaast maakt het project een transitieplan dat de activiteiten beschrijft die nodig zijn om de software af te bouwen of te herbouwen en te onderhouden. Als er significante technische schuld aanwezig is de bestaande software maakt het project een plan voor het aflossen van deze schuld.

Samenhang voorfaseproducten



Bovenstaande figuur laat de belangrijkste relaties zien tussen de verschillende producten die de input en output van de voorfase vormen. Naast de informatiestromen zoals door de pijlen weergegeven zijn er in de praktijk nog meer verbanden tussen de producten. Zo kan de gekozen oplossing in de architectuur van invloed zijn op de maatregelen in het informatiebeveiligingsplan of leiden niet-functionele eisen tot extra functionele eisen.

Overzicht

De onderstaande tabel bevat de hierboven genoemde producten. Het ✔ geeft aan in welke fase ze van belang zijn en worden opgeleverd, ook als ze zijn opgesteld door externe auteurs.

Product	Voorfase	Realisatiefase
Plan van aanpak	✔	✔
Beschrijving van functionele eisen	✔	✔
Beschrijving van niet-functionele eisen	✔	✔
Product backlog	✔	✔
Ontwerp- en architectuurdocumentatie (software, interactie, infrastructuur)	✔	✔
Testdocumentatie: testplannen	✔	✔
Testdocumentatie: testgevallen, rapportages		✔
Informatiebeveiligingsplan	✔	✔
Kwaliteitsplan	✔	✔
Deploybare versie van de software		✔
Broncode, inclusief de benodigdheden voor het bouwen van de software		✔
Regressietests, inclusief de benodigdheden voor het uitvoeren van de tests		✔
Deploymentdocumentatie		✔
Software bill of materials		✔
Release notes		✔
Vrijgaveadvies		✔
Bij due diligence: uitkomsten onderzoek (bevindingen, risico's, mitigerende maatregelen)	✔	
Bij due diligence: transitieplan voor af te bouwen, te onderhouden en/of te herbouwen softwareproducten	✔	
Bij due diligence: plan voor aflossen technische schuld, indien van toepassing	✔	

Verantwoordelijkheden

De opdrachtgever is primair verantwoordelijk voor het beschrijven van de functionele en niet-functionele eisen, de geprioriteerde backlog, het mastertestplan en het informatiebeveiligingsplan.

ICTU is primair verantwoordelijk voor plan van aanpak, softwarearchitectuurdocumentatie, globaal functioneel ontwerp, prototype, detailtestplannen en testrapportages voor bouwtesten, kwaliteitsplan, deploybare versie van de software, broncode, regressietests, deploymentdocumentatie, release notes en vrijgaveadvies. Als er een due diligence plaatsvindt, levert ICTU de onderzoeksresultaten en maakt een transitieplan, en indien van toepassing, een plan voor het aflossen van technische schuld.

De beheerpartij is primair verantwoordelijk voor de infrastructuurarchitectuur en -ontwerp en detailtestplannen en testrapportages voor infrastructuurtesten.

Rationale

Het uniformeren van op te leveren producten biedt voordelen voor planning (het is bekend welke producten gemaakt moeten worden), voor bemensing (het is bekend welke expertise nodig is) en voor het uitwisselen van medewerkers.

De voorgeschreven producten stellen de beheerpartij in staat om de opgeleverde software uit te rollen, te beheren en eventueel te onderhouden. Daarnaast is duidelijk welke eventueel openstaande punten er nog zijn. De voorgeschreven producten bieden voldoende verantwoording richting de ontvanger voor uitgevoerde werkzaamheden.

De genoemde producten uit de voorfase hebben tot doel om enerzijds de omvang, kosten en doorlooptijd van de realisatiefase te kunnen schatten en anderzijds om de kaders voor de realisatiefase te bepalen, zodat de scope, aanpak en oplossingsrichting in grote lijnen bekend zijn.

5.3 M02: Het project zorgt dat het product continu aan de kwaliteitsnormen voldoet

M02: Het project zorgt dat het product continu aan de kwaliteitsnormen voldoet
Producten voldoen zo snel mogelijk vanaf de start van een project aan de door het project en ICTU vastgestelde kwaliteitsnormen en blijven daar zo veel mogelijk aan voldoen. De kwaliteit van producten, die nog niet zijn afgerond of nog niet aan de normen voldoen, wordt door het project bewaakt. Het voldoen aan de kwaliteitsnormen is onderdeel van de Definition of Done en herstel van de kwaliteit wordt planmatig opgepakt.

De kwaliteitsnormen voor het project zijn beschreven in de niet-functionele eisen, het informatiebeveiligingsplan, het kwaliteitsplan en deze Kwaliteitsaanpak, zie M01: Het project levert in elke fase vastgestelde producten en informatie op.

Tijdens de voorfase wordt het voldoen aan de kwaliteitsnormen met behulp van reviews gecontroleerd. Als onderdeel van het op te stellen kwaliteitsplan wordt tijdens de voorfase bepaald hoe het project de kwaliteit tijdens realisatie gaat controleren; voor producten die niet geautomatiseerd kunnen worden gecontroleerd, beschrijft het kwaliteitsplan een alternatieve aanpak. Als bijvoorbeeld door de gekozen technologie geen ondersteuning van het kwaliteitssysteem mogelijk is, kunnen periodieke, handmatige controles als alternatief ingezet worden.

Tijdens de realisatiefase wordt de kwaliteit diverse malen per uur gemeten door een geautomatiseerd kwaliteitssysteem, genaamd Quality-time. Het Scrumteam kijkt dagelijks of er afwijkingen van de normen zijn en onderneemt actie, indien nodig. Ook de kwaliteitsmanager signaleert afwijkingen en meldt deze bij het Scrumteam.

Kwaliteitseigenschappen van de software die niet (volledig) geautomatiseerd kunnen worden gemeten, worden tijdens de realisatiefase periodiek handmatig geëvalueerd. Minimaal betreft dit de beveiliging van de software, zie M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen. Ook zorgt het project dat de performance van de software regelmatig wordt getest. Voor kwaliteitsaspecten als toegankelijkheid en gebruikskwaliteit organiseert het project handmatige testen en/of

evaluaties in een vorm en met een frequentie die aansluit bij de aard van de applicatie en de door de opdrachtgever gestelde eisen. De kwaliteitsmanager houdt in het kwaliteitssysteem bij wanneer de laatste test of evaluatie is uitgevoerd en wanneer het tijd is voor de volgende.

Documenten, die onderdeel uitmaken van het op te leveren projectresultaat, zijn zo veel mogelijk geactualiseerd; eventuele achterstand wordt planmatig weggewerkt. De kwaliteitscontrole van documenten gebeurt op basis van reviews. De auteur van een document en de software delivery manager zorgen dat de juiste reviewers benoemd zijn; hiertoe behoort in ieder geval de kwaliteitsmanager. De auteur van het document zorgt voor een correct versiebeheer van het document. De auteur koppelt aan de reviewers terug of en hoe het ontvangen commentaar is verwerkt in de volgende versie van het betreffende document.

Als de kwaliteitsnormen langdurig niet worden behaald heeft de kwaliteitsmanager de volgende escalatielijn:

1. De kwaliteitsmanager bespreekt de situatie met de software delivery manager.
2. Indien dat niet tot resultaat leidt, escaleert de kwaliteitsmanager de situatie naar de projectleider.
3. Indien 2. niet tot resultaat leidt, escaleert de kwaliteitsmanager de situatie naar het hoofd van de afdeling ICTU Software Expertise (ISE).

Rationale

Het zo snel mogelijk en continu voldoen aan de kwaliteitsnormen beperkt toekomstige hersteltijd. Het dwingt tevens een systematische kwaliteitscontrole af.

5.4 M03: Het project zorgt dat het product traceerbaar aan eisen voldoet

M03: Het project zorgt dat het product traceerbaar aan eisen voldoet
Eisen zijn wederzijds traceerbaar naar bewijsmateriaal, zoals logische testgevallen, dat de eis gerealiseerd is; dat wil zeggen dat geadministreerd is bij welke eis bewijsmateriaal hoort en vice versa. Dit wordt waar mogelijk met tooling ondersteund.

Functionele eisen in de vorm van user stories zijn gekoppeld aan logische testgevallen. Ontwerpdocumentatie in de vorm van use cases is gekoppeld aan logische testgevallen. ICTU gebruikt hiervoor Jira. Logische testgevallen zijn gekoppeld aan fysieke testgevallen. De fysieke testgevallen worden geannoteerd met een identifier van de logische testgevallen. Het project is verantwoordelijk voor het traceerbaar voldoen aan de eisen.

Niet-functionele eisen zijn gekoppeld aan onder andere softwarearchitectuurdocument, mastertestplan en detailtestplannen. De traceerbaarheid hiervan is (nog) niet geadministreerd met behulp van tooling.

Rationale

Door eisen en testgevallen te koppelen en traceerbaar te maken, is het mogelijk de dekking van tests ten opzichte van eisen te bepalen. Logische testgevallen worden gekoppeld aan use cases om zo aan te tonen dat alle ontworpen en geïmplementeerde functionaliteit getest wordt. Logische testgevallen worden gekoppeld aan user stories om aan te tonen dat alle wijzigingen die in een sprint zijn gemaakt ook getest zijn.

5.5 M13: Het project gebruikt ISO-25010 voor de specificatie van productkwaliteitseisen

M13: Het project gebruikt ISO-25010 voor de specificatie van productkwaliteitseisen
Voor specificatie en documentatie van vereiste en gewenste kwaliteitseigenschappen, de niet-functionele eisen, maken projecten gebruik van de terminologie uit NEN-ISO/IEC 25010. Projecten gebruiken NEN-ISO/IEC 25010 om te controleren of alle relevante kwaliteitseigenschappen van het op te leveren eindproduct worden meegenomen in de ontwikkeling en/of onderhoud van het product.

De standaard NEN-ISO/IEC 25010:2011, kortweg "ISO-25010", biedt een model voor het beschrijven van productkwaliteit. Kwaliteitseigenschappen zijn voorzien van een naam, definitie en classificatie. ISO-25010 dekt een breed spectrum van kwaliteitseigenschappen af.

Rationale

ISO-25010 biedt een model voor productkwaliteit. De standaard biedt geen concrete maatregelen, maar biedt wel een begrippenkader en dekt het volledige spectrum van mogelijk relevante kwaliteitseigenschappen af. Het gebruiken van een standaard voor specificatie van kwaliteit voorkomt miscommunicatie over kwaliteitseigenschappen en de breedte van de standaard zorgt ervoor dat alle relevante aspecten aan bod komen.

5.6 M04: Het project borgt de correcte werking van het product met geautomatiseerde regressietests

M04: Het project borgt de correcte werking van het product met geautomatiseerde regressietests
Regressietests - tests die verifiëren of eerder ontwikkelde software nog steeds correct werkt na wijzigingen in de software of aansluiting op andere externe koppelvlakken - zijn geautomatiseerd.

Het project hanteert een norm voor de dekking van regressietests en bewaakt deze.

Rationale

Handmatig uitgevoerde regressietests zijn arbeidsintensief, foutgevoelig en afhankelijk van de aanwezigheid van specifieke medewerkers. Gelet op de vrijwel continue metingen op en leveringen van de software, zijn de nadelen van handmatige regressietests niet acceptabel. Door ze te automatiseren zijn ze herhaalbaar en kunnen ze onderdeel uitmaken van de continuous delivery pipeline.

5.7 M07: Het project gebruikt een continuous delivery pipeline om het product te bouwen, testen en op te leveren

M07: Het project gebruikt een continuous delivery pipeline om het product te bouwen, testen en op te leveren
Er is een geautomatiseerde continuous delivery pipeline die aantoonbaar correct werkt en de software bouwt, installeert in testomgevingen, test op functionele en niet-functionele eigenschappen en oplevert.

De geautomatiseerde continuous delivery pipeline voert ten minste de volgende activiteiten uit:

1. Bouw van de software,
2. Unit tests,
3. Regressietests,
4. Beveiligingstests,
5. Performancetests,
6. Toegankelijkheidstests,
7. Broncodekwaliteitscontroles,
8. Installatie van de software,
9. Oplevering van het totale product, dus inclusief alle deliverables, in de vorm zoals bruikbaar voor en afgesproken met de opdrachtgever.

Performance- en beveiligingstests zijn ook onderdeel van de continuous delivery pipeline, maar vanwege doorlooptijden en licenties is dat niet altijd haalbaar; in dat geval vinden de performance- en beveiligingstests zo veel mogelijk, en bij voorkeur dagelijks, plaats.

Niet alle testen en controles kunnen altijd geautomatiseerd worden uitgevoerd. Denk aan kwaliteitscontroles op architectuurbeslissingen of het testen van toegankelijkheidseisen. Waar mogelijk wordt wel een zo groot mogelijk deel van de testen en controles geautomatiseerd en als onderdeel van de pipeline uitgevoerd.

De afdeling ICTU Software Diensten (ISD) voorziet in tools en ondersteuning, zodat projecten deze pipeline kunnen toepassen. Projecten zijn verantwoordelijk voor de correcte werking van de pipeline.

ICTU gebruikt Jenkins, GitLab CI of Azure DevOps als tool voor de implementatie van de continuous delivery pipeline. ISD biedt de projecten een voorziening om releases van het totale product veilig op te leveren aan opdrachtgevers en beheerpartijen.

Rationale

Software incrementeel opleveren vereist dat de software frequent gebouwd, getest en opgeleverd kan worden. Om dit efficiënt en foutvrij te doen, dient het proces van bouwen, testen en opleveren geautomatiseerd te zijn; een continuous delivery pipeline faciliteert dit.

5.8 M08: Het project maakt technische schuld inzichtelijk en lost deze planmatig op

M08: Het project maakt technische schuld inzichtelijk en lost deze planmatig op
Technische schuld is inzichtelijk en wordt planmatig aangepakt. De kwaliteitsmanager is verantwoordelijk voor het inzichtelijk maken van de technische schuld. De software delivery manager is verantwoordelijk voor het planmatig aanpakken van de technische schuld en zorgt dat het Scrumteam regelmatig en voldoende tijd heeft om technische schuld te voorkomen en op te lossen. Het Scrumteam is verantwoordelijk voor het zoveel mogelijk voorkomen van technische schuld en voor het identificeren van technische schuld die toch optreedt.

De kwaliteitsmanager maakt de technische schuld inzichtelijk met behulp van een geautomatiseerd kwaliteitssysteem. Technische schuld die niet geautomatiseerd kan worden gemeten legt de kwaliteitsmanager handmatig vast.

Als het Scrumteam of de kwaliteitsmanager constateert dat er technische schuld is, markeert de kwaliteitsmanager deze technische schuld in het kwaliteitssysteem om te voorkomen dat de technische schuld ongemerkt verder toeneemt. Vervolgens vraagt de kwaliteitsmanager het Scrumteam, in overleg met de software delivery manager, om de omvang van de technische schuld in te schatten in user-story-punten. Vervolgens wordt een plan gemaakt om de technische schuld in een beheerst tempo weg te werken; uitgangspunt is ongeveer 10% van de punten die het Scrumteam normaal in een sprint doet. Dit kan in principe zonder overleg met de opdrachtgever omdat het leveren van kwaliteit onderdeel van het werk is.

ICTU gebruikt Quality-time om bestaande technische schuld inzichtelijk te maken en de planning van het aflossen van de schuld vast te leggen, voor zover het technische schuld betreft van kwaliteitseigenschappen die Quality-time kan meten. Technische schuld die niet geautomatiseerd kan worden gemeten legt de kwaliteitsmanager vast als issues in Jira.

Quality-time is een door ICTU ontwikkeld, open source, geautomatiseerd kwaliteitssysteem.

ICTU-projecten reserveren per sprint tijd die het Scrumteam kan besteden aan het oplossen van technische schuld.

Rationale

Technische schuld zijn eigenschappen van de software die de lange termijn inzetbaarheid en onderhoudbaarheid van de software bedreigen. Denk hierbij aan hoge complexiteit, lage testdekking, ontbrekende testsoorten en ontbrekende documentatie.

De aanwezigheid van technische schuld heeft nadelige invloed op de kwaliteit van de eindproducten. Anderzijds is het ontstaan van technische schuld gedurende een project vaak onvermijdelijk. Het is daarnaast ook mogelijk dat een deel van de technische schuld bij aanvang van het project al bestond en mogelijk niet wordt opgelost. In alle gevallen is het verstandig om te weten welke technische schuld bestaat. Om te voorkomen dat technische schuld niet wordt opgelost en uitsluitend toeneemt, is het zaak om het verminderen van technische schuld planmatig aan te pakken.

5.9 M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen

M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen
Projecten laten periodiek de beveiliging van de ontwikkelde software beoordelen. Een beveiligingsexpert onderzoekt de code zowel geautomatiseerd als handmatig op veelvoorkomende kwetsbaarheden en op het voldoen aan voorgeschreven beveiligingsnormen. Overheidsspecifieke beveiligingsnormen of -raamwerken, zoals de BIO (Baseline Informatiebeveiliging Overheid), bieden een basis voor de beoordeling. Bevindingen uit de beveiligingstest worden vastgelegd als onderdeel van de werkvoorraad voor het ontwikkelproces.

Software wordt minimaal bij iedere grote release of ten minste twee keer per jaar onderworpen aan een beveiligingstest door beveiligingsexperts die ICTU daarvoor inhuurt. Op basis van documentatie en architectuurstudie, crystalbox security audits (broncodescan) en penetratieaudits beoordelen deze experts of de software voldoet aan de projectspecifieke niet-functionele eisen met betrekking tot beveiliging, of bekende kwetsbaarheden (zoals bijvoorbeeld in de OWASP Top 10 genoemd) vermeden zijn en of voldoende invulling gegeven is aan de normen die vanuit BIO en SSD gelden.

ICTU zorgt ervoor dat de benodigde expertise op afroep beschikbaar gesteld kan worden aan projecten.

Opdrachtgever kan een derde partij opdracht geven beveiligingstesten uit te voeren in een daarvoor door de opdrachtgever beschikbaar gestelde omgeving. Dit kan zowel incidenteel als structureel worden ingericht. Als de opdrachtgever dit structureel inricht en als deze beveiligingstesten voldoen aan dezelfde eisen als de beveiligingstesten die in opdracht van ICTU worden uitgevoerd kunnen opdrachtgever en het project besluiten dat het project zelf geen beveiligingstesten laat uitvoeren. Afspraken hierover worden bij voorkeur al in de voorfase gemaakt, inclusief een controle dat de opdrachtgever de benodigde contractuele mogelijkheden heeft beveiligingstesten uit te besteden. Uiteraard ontvangt ICTU in dat geval de beveiligingstestrapportages.

De beveiligingstesten vinden altijd plaats in aanvulling op de door tools uitgevoerde continue beveiligingsanalyse van de gerealiseerde software. Bevindingen uit beveiligingstesten en de continue analyse die niet direct worden opgelost, worden in Jira als issue vastgelegd op de backlog van het project.

De kwaliteitsmanager van het project bewaakt de opvolging van de kritische

beveiligingsissues. De kwaliteitsmanager bewaakt tevens of de beveiligingstesten voldoende frequent plaatsvinden, bij voorkeur door Quality-time te laten waarschuwen als het tijd is voor de volgende beveiligingstest.

Rationale

Door het inschakelen van actuele, specifieke expertise wordt de kans vergroot dat eventuele kwetsbaarheden in de gerealiseerde software tijdig herkend worden.

6 Processen

6.1 M14: Het project bereidt samen met opdrachtgever en belanghebbenden de realisatie voor

M14: Het project bereidt samen met opdrachtgever en belanghebbenden de realisatie voor
Projecten hebben een voorbereidingsfase, "voorfase" genoemd, voorafgaand aan de realisatiefase. Voor het uitvoeren van de voorfase zijn vertegenwoordigers van de opdrachtgever, de beoogde beheerpartij en andere belanghebbenden betrokken die meewerken aan het realiseren van een deel van de op te leveren producten. Het doel van de voorfase is beeld krijgen van de te realiseren oplossing, van de risico's die zich tijdens realisatie kunnen voordoen en van de kaders waarbinnen de oplossing moet passen; tijdens de realisatiefase vinden bouw en onderhoud van de software en actualiseren en afronden van documentatie plaats.

Bij voorkeur zijn dezelfde deskundigen in zowel de voorfase als in de realisatiefase betrokken.

In de realisatiefase wordt de prioriteit van werk van het Scrumteam bepaald door een product owner van de opdrachtgever. Bij aanvang van de voorfase is deze beoogde product owner bekend en werkt deze ook mee in de voorfase.

Rationale

Het doel van de voorfase is ten eerste om uitgangspunten, risico's en randvoorwaarden voor verdere projectuitvoering te bepalen en ten tweede om te zorgen dat aan de randvoorwaarden wordt voldaan en voor zoveel mogelijk projectspecifieke risico's maatregelen genomen zijn. Het doel van de realisatiefase is het daadwerkelijk bouwen en onderhouden van de software. Een expliciete splitsing zorgt ervoor dat projecten doordacht van start gaan.

Al tijdens de voorfase moeten keuzes gemaakt worden die invloed hebben op de beveiligingsmaatregelen. Aanwezigheid van een voldoende gemandateerde vertegenwoordiger van de opdrachtgever zorgt dat deze keuzes gemaakt en bekrachtigd kunnen worden. De keuzes komen onder meer tot uitdrukking in de ontwerp- en architectuurdocumentatie, zie M01: Het project levert in elke fase vastgestelde producten en informatie op. De infrastructuur gerelateerde documentatie wordt opgesteld door de beoogd beheerder en dekt een deel van de totale beveiligingsmaatregelen af. Aanwezigheid van de beoogd beheerder in de voorfase zorgt dat dekking van dit deel van de beveiligingsmaatregelen geborgd blijft gedurende de realisatie en exploitatie.

6.2 M21: Het project selecteert medewerkers op basis van kwaliteit

M21: Het project selecteert medewerkers op basis van kwaliteit
Bij de inzet van medewerkers gaat kwaliteit boven andere aspecten, zoals beschikbaarheid, prijs en doorlooptijd.

Rationale

Goede kwaliteit van producten ontstaat primair door het werk van mensen; standaardisatie, kwaliteitsnormen en monitoring zijn hulpmiddelen. De kans dat kwalitatief goede medewerkers ook goede producten maken, is groter dan bij minder goede medewerkers.

6.3 M23: Het project zorgt voor de aanwezigheid van ervaring met de Kwaliteitsaanpak

M23: Het project zorgt voor de aanwezigheid van ervaring met de Kwaliteitsaanpak
De software delivery manager zorgt ervoor dat bij nieuwe projecten wordt gestart met ten minste twee projectleden die bekend zijn met de Kwaliteitsaanpak.

Rationale

Het inzetten van teamleden die bekend zijn met de Kwaliteitsaanpak zorgt voor een soepeler start van een nieuw project omdat zij bekend zijn met de inhoud van de Kwaliteitsaanpak, zoals kwaliteitsnormen en tools, en omdat zij al doende nieuwe teamleden bekend kunnen maken met de Kwaliteitsaanpak.

6.4 M05: Het project hanteert een iteratief en incrementeel ontwikkelproces

M05: Het project hanteert een iteratief en incrementeel ontwikkelproces
Projecten werken iteratief en incrementeel; dit betekent dat een project in korte iteraties werkt, waarbij elke iteratie een werkende versie van de software oplevert die extra waarde vertegenwoordigd voor de opdrachtgever. Behalve de software levert het project iedere iteratie telkens ook alle andere producten bijgewerkt op. Elke iteratie worden verwachtingen en werkelijke resultaten vergeleken en de werkwijze aangescherpt op basis van inzichten en bevindingen.

ICTU gebruikt hiervoor Scrum, een raamwerk voor agile productontwikkeling. ICTU propageert de kernwaarden van Scrum en vereist de volgende onderdelen van Scrum:

1. Scrumteam bestaand uit product owner, ontwikkelaars (zoals programmeurs, testers en ontwerpers) en Scrummaster,
2. Proces met daily scrum, sprints, sprint planning, sprint review, sprint retrospective en sprint refinement,

3. Definition of Ready en Definition of Done,
4. Product backlog en sprint backlog.

Vast onderdeel van de Definition of Done is dat producten actueel en onderling consistent zijn en voldoen aan de door ICTU vastgestelde kwaliteitsnormen.

Rationale

De incrementele oplevering levert vrijwel iedere iteratie toegevoegde waarde en stelt opdrachtgevers, gebruikers en anderen in staat om gaandeweg ervaring op te doen en bij te sturen. Verder dwingt het vroegtijdige tests en kwaliteitscontroles af, die daarmee verankerd worden in het ontwikkel- en onderhoudsproces. Door naast de software telkens ook alle andere producten bij te werken en op te leveren, wordt bereikt dat het product als geheel consistent blijft en dat er geen achterstallig onderhoud ontstaat. Dit leidt tot een zich continu verbeterend proces.

6.5 M06: Het project meet kwaliteitsnormen geautomatiseerd en frequent

M06: Het project meet kwaliteitsnormen geautomatiseerd en frequent
Het voldoen aan de kwaliteitsnormen die geautomatiseerd gemeten kunnen worden, wordt frequent en minimaal één keer per dag gemeten.

ICTU faciliteert dit met mensen en middelen. Het kwaliteitssysteem van ICTU meet het voldoen aan de normen meermaals per uur. De daaruit voortvloeiende kwaliteitsrapportage wordt besproken tijdens de Daily Scrum en/of tijdens het projectoverleg.

Rationale

Vaak meten maakt een vrijwel actueel inzicht op elk moment mogelijk. Projectleden kunnen snel reageren op afwijkingen, die in de regel ook pas recent zijn ontstaan en dus meestal gerelateerd zijn aan huidige activiteiten. Met name afwijkingen van de normen op het vlak van informatiebeveiliging en onderhoudbaarheid komen zo snel aan het licht en kunnen dan ook snel worden beoordeeld en - indien nodig en mogelijk - opgelost.

6.6 M10: Het project kent een wekelijks projectoverleg

M10: Het project kent een wekelijks projectoverleg
De projectleider organiseert een periodiek projectoverleg. Dit overleg vindt wekelijks plaats en duurt niet langer dan een uur. Vereiste aanwezigen zijn de projectleider, de software delivery manager, de Scrummaster, een vertegenwoordiger uit elk van de Scrumteams en de kwaliteitsmanager van het project; andere aanwezigen kunnen zijn: de projectarchitect en de product owner. De agenda voor dit overleg bestaat ten minste uit de volgende onderwerpen: mededelingen, actie- en besluitenlijst, personele zaken, planning en voortgang, kwaliteit en architectuur, risico's en aandachtspunten.

Het periodiek projectoverleg heet bij ICTU het "Intern Projectoverleg" of "IPO".

Bij dit IPO is de aanwezigheid van de volgende rollen vereist:

- projectleider,
- software delivery manager,
- kwaliteitsmanager,
- Scrummaster,
- vertegenwoordiger uit elk Scrumteam.

Nadere toelichting op de agenda:

- Mededelingen: betrokkenen proactief informeren over voor het project relevante ontwikkelingen.
- Actie- en besluitenlijst: de software delivery manager houdt de actie- en besluitenlijst bij.
- Personele zaken: bespreking van samenwerking binnen het project, in- en uitstroom, op- en afschalen.
- Planning en voortgang: bespreking van voortgang ten opzichte van voorspelling en daaraan gerelateerde afwijkingen en knelpunten, leidend tot acties.
- Kwaliteit en architectuur: bespreking van kwaliteit, bijvoorbeeld naar aanleiding van de self-assessment, architectuur voor borging van inhoudelijke koers, eventuele afwijkingen en benodigde acties.
- Risico's en aandachtspunten: de software delivery manager houdt het risicolog bij.

Het kwaliteitssysteem bewaakt de actualiteit van de actie- en besluitenlijst en het risicolog.

Rationale

Het doel van het periodiek projectoverleg is alle betrokkenen op hetzelfde informatieniveau te brengen en te houden. Het overleg is intern om vrijuit te kunnen praten over personele zaken en risico's voor het project.

6.7 M16: Het project gebruikt tools voor vastgestelde taken

M16: Het project gebruikt tools voor vastgestelde taken
ICTU stelt het gebruik van tools verplicht voor:

1. backlog management en agile werken,
2. inrichten en uitvoeren van een continuous delivery pipeline,
3. monitoren van de kwaliteit van broncode,
4. versiebeheer van op te leveren producten,
5. release van software,
6. maken van testrapportages,
7. maken van kwaliteitsrapportages,
8. controleren van de configuratie op aanwezigheid van bekende kwetsbaarheden,
9. controleren van door de applicatie gebruikte versies van externe software op aanwezigheid van bekende kwetsbaarheden,
10. controleren van de software op aanwezigheid van kwetsbare constructies,
11. testen van performance en schaalbaarheid,
12. testen op toegankelijkheid van de applicatie en
    13) produceren van een "software bill of materials" (SBoM).

Onder het ondersteunen van "agile werken" vallen het opvoeren van eisen, het opvoeren van logische testgevallen, het koppelen van logische testgevallen aan eisen, het bijhouden van een werkvoorraad, het plannen van iteraties en het toewijzen van eisen aan iteraties. De 'eisen' worden, conform Scrumterminologie, geregistreerd als epics en/of user stories, de werkvoorraad als backlog en de iteraties als sprints.

ICTU adviseert en ondersteunt voor de genoemde taken onderstaande tools. Projecten gebruiken deze tools:

1. Backlogmanagement en agile werken: Azure DevOps of Jira,
2. Continuous delivery pipeline: Jenkins, GitLab CI/CD (Continuous Integration, Delivery, and Deployment) of Azure DevOps,
3. Kwaliteit van broncode: SonarQube,
4. Versiebeheer: GitLab of Azure DevOps,
5. Release van software: Releaseserver in het ontwikkelplatform,
6. Testrapportages: JUnit, Robot Framework, TestNG, of hiermee compatible tools,
7. Kwaliteitsrapportages: Quality-time,
8. Kwetsbaarheden in configuratie: OpenVAS (Vulnerability Assessment System),
9. Kwetsbaarheden in externe software: OWASP (Open Web Application Security Project) Dependency Checker,
10. Kwetsbaarheden in software: GitLab SAST (Static Application Security Testing), SonarQube en/of OWASP ZAP (Zed Attack Proxy),
11. Performancetesten en performancetestrapportages: JMeter en Performancetestrunner,
12. Toegankelijkheid: Axe, en
13. Software bill of materials: tools die een SBoM in CycloneDX-formaat (zie https://cyclonedx.org) genereren.

Rationale

Projecten hebben een redelijke vrijheid bij het kiezen en gebruiken van tools, maar voor een aantal taken is het gebruik verplicht gesteld. Deze tools zijn nodig voor een efficiënte uitvoering van de Kwaliteitsaanpak. Uniform gebruik van deze tools maakt het mogelijk koppeling tussen die tools voor alle projecten te standaardiseren; daarnaast bevordert het de uitwisselbaarheid van medewerkers en neemt het risico op het gebruik van onvolwassen tools af. Tot slot is het gebruik in een aantal gevallen, ten behoeve van informatiebeveiliging bij de overheid, verplicht.

6.8 M09: Het project implementeert nieuwe versies van de Kwaliteitsaanpak binnen de gestelde termijn

M09: Het project implementeert nieuwe versies van de Kwaliteitsaanpak binnen de gestelde termijn
Projecten implementeren nieuwe versies van Kwaliteitsaanpak en kwaliteitsnormen binnen de door ICTU gestelde termijn. De projectleider is verantwoordelijk voor de implementatie.

De software delivery manager is verantwoordelijk voor de implementatie van de Kwaliteitsaanpak. De software delivery manager stemt periodiek de self-assessmentresultaten af met de projectleider.

Rationale

De implementatie van een nieuwe versie van de Kwaliteitsaanpak kost tijd. De introductie en aanpassing van normen en tools, kunnen verschillende consequenties hebben: bestaande broncode blijkt niet meer volledig te voldoen aan de normen, een nieuwe tool moet in de ontwikkelstraat worden toegevoegd, enzovoort.

Anderzijds is het voor de uniformiteit van kwaliteitsmeting en rapportage en de doorontwikkeling van de Kwaliteitsaanpak van belang de implementatieperiode zo kort mogelijk en voorspelbaar te houden. Daarom stemt ICTU met de projecten een implementatiemoment en -periode af.

Omdat implementatie van maatregelen in een project tijd kost is de self-assessment gericht op het in kaart brengen van de belangrijkste verschillen tussen de Kwaliteitsaanpak en de in het project toegepaste werkwijze, maar niet op het uitputtend inventariseren van alle verschillen.

6.9 M28: Het project voert periodiek een self-assessment uit ten aanzien van de Kwaliteitsaanpak

M28: Het project voert periodiek een self-assessment uit ten aanzien van de Kwaliteitsaanpak
De projectleider organiseert periodiek een self-assessment ten aanzien van de Kwaliteitsaanpak.

Deze self-assessment geeft inzicht in de huidige status van het project en kan aanleiding geven tot het nemen van maatregelen binnen het project.

De projectleider identificeert de belangrijkste verschillen tussen Kwaliteitsaanpak en werkwijze in het project en rapporteert hierover aan ICTU. In overleg tussen projectleider en ICTU wordt besloten of het verschil tijdelijk of permanent wordt geaccepteerd. In het geval van tijdelijke acceptatie stelt de projectleider een verbeteractie op. Merk op dat de verbeteractie ook kan bestaan uit het opstellen van een verbetervoorstel voor de Kwaliteitsaanpak.

Voor de belangrijkste verschillen beschrijft de projectleider:

- het geconstateerde verschil,
- reden voor het verschil,
- in geval van acceptatie; waarom het verschil geaccepteerd wordt,
- in geval van verbeteractie; planning om het verschil weg te werken.

De projectleider is verantwoordelijk voor het doen van de self-assessment, die in de regel door de software delivery manager wordt uitgevoerd. De kwaliteitsmanager reviewt de self-assessment, of de software delivery manager en kwaliteitsmanager voeren de self-assessment samen uit.

De self-assessment is een intern product, maar kan gedeeld worden met opdrachtgevers en andere betrokkenen. Voor het doen van de self-assessment stelt ICTU een ondersteunend formulier beschikbaar.

Rationale

Net als bij technische producten is het periodiek meten van de kwaliteit van belang om in controle te blijven. Aangezien veel maatregelen uit de Kwaliteitsaanpak zich niet geautomatiseerd laten meten, is menselijke inbreng nodig.

6.10 M30: Het project identificeert, mitigeert en bewaakt risico's

M30: Het project identificeert, mitigeert en bewaakt risico's
Het project identificeert, mitigeert en bewaakt projectspecifieke risico's voorafgaand aan en tijdens de projectuitvoering. Het project houdt een risicolog bij met geïdentificeerde risico's. De uitkomsten van de "Doordacht-van-Start-sessie" vormen het startpunt van deze risicolog. Risico's die tijdens de voorfase worden geïdentificeerd, bijvoorbeeld bij de productrisicoanalyse, worden toegevoegd aan de risicolog. Tijdens de voorfase en bij de start van de realisatiefase worden risicosessies gehouden met (vertegenwoordigers van) de belanghebbenden om verdere risico's te identificeren. Het project identificeert en implementeert mitigerende maatregelen danwel accepteert expliciet de geïdentificeerde risico's. Het project bewaakt de risicolog en uitvoering van de mitigerende maatregelen tijdens het IPO.

Rationale

Een flink deel van de risico's die komen kijken bij het ontwikkelen van software zijn bekend. NPR 5326 geeft voor een deel van deze generieke risico's beheersmaatregelen. De maatregelen in deze Kwaliteitsaanpak komen grotendeels overeen met de beheersmaatregelen in NPR 5326.

Echter, naast generieke risico's loopt elke project ook projectspecifieke risico's die voortkomen uit de context waarin het project wordt uitgevoerd. Alleen door deze risico's voorafgaand aan en tijdens het project actief te identificeren en te mitigeren kan de potentiële impact ervan beperkt worden.

6.11 M34: Het project draagt software beheerst over

M34: Het project draagt software beheerst over
Als de software op enig moment door een andere partij dan ICTU verder ontwikkeld en/of onderhouden zal worden, draagt het project zorg voor een beheerste overdracht. Beheerdocumentatie, broncode en testmiddelen zijn van dusdanige kwaliteit en compleetheid dat de andere partij de software efficiënt en effectief kan doorontwikkelen en/of onderhouden.

Het project gebruikt NEN NPR 5325 als leidraad voor de overdracht van software aan een andere partij. De paragraafnummers hieronder verwijzen naar de betreffende paragraaf in NPR 5325.

Het project zorgt, bij voorkeur altijd maar in ieder geval bij de overdracht, dat de software, documentatie en testmiddelen aantoonbaar voldoen aan onderstaande criteria.

1. De documentatie beschrijft de ontwikkel- en testomgeving die is toegepast (5.1),
2. De functionele documentatie beschrijft gegevensmodellen, functionele indeling, koppelingen, berichtdefinities en workflows/processen (5.2),
3. In het geval van DevOps: de operationele bedieningsinstructies beschrijven

minimaal back-up/recovery, procedures bij calamiteiten, regelmatig terugkerende beheeractiviteiten en opstart- en afsluitprocedures (5.3),
4. De productbacklog bevat de bekende bugs en wensen (5.4),
5. De broncode kent een gezonde balans tussen isolatie, cohesie en koppeling (6.1),
6. De broncode heeft een beperkte mate van duplicatie (6.2),
7. De broncode heeft een beperkte mate van complexiteit (6.3),
8. De broncode bevat geen of een beperkt aantal niet-afgeronde werkzaamheden ("todo's") (6.4).
9. De tests raken een voldoende groot deel van de broncode (code dekking) (7.1),
10. De tests raken een voldoende groot deel van de functionaliteit (functionele dekking) (7.2),
11. De onderkende productrisico's zijn gedekt (7.3),
12. Er is een regressietest beschikbaar (7.4),
13. Er is traceerbaarheid van eisen naar testgevallen (7.5), en
14. De testset is goed opgebouwd (7.6).

Ten behoeve van de overdracht maakt het project, in afstemming met opdrachtgever en ontvangende partij, een plan voor de voorbereiding van de overdracht, de kennisoverdracht, de overdracht van de software zelf en eventuele nazorg.

6.12 M27: Het project sluit projectfasen en zichzelf expliciet af

M27: Het project sluit projectfasen en zichzelf expliciet af
Afsluiting van een projectfase gebeurt expliciet en gecontroleerd: alle producten, zoals documentatie, broncode, referentiedata en credentials, die in de af te sluiten fase nodig waren of zijn opgeleverd, worden gearchiveerd. Indien er geen volgende fase is voorzien op korte termijn, dienen alle producten van de laptops van de projectmedewerkers verwijderd te worden.

De software delivery manager is verantwoordelijk voor het archiveren. De software delivery manager geeft het Scrumteam opdracht de archivering voor te bereiden en geeft de afdeling ICTU Software Diensten (ISD) de opdracht de archivering uit te voeren.

Alle documentatie, broncode, referentiedata en credentials die tijdens de werkzaamheden nodig waren of zijn opgeleverd, worden gearchiveerd en van werkstations van medewerkers verwijderd.

Rationale

Archiveren faciliteert het eventueel herstarten of overdragen van het project op een later tijdstip. Verwijderen neemt een onnodig risico op inbreuk op vertrouwelijkheid weg en vrijwaart projectmedewerkers en ICTU van verdenking en aansprakelijkheid wanneer een incident optreedt.

Het expliciet afsluiten van het project is conform Maatregel 14: "Archivering" uit de NPR 5326.

7 Organisatie

7.1 M29: ICTU zorgt dat een project verantwoord kan starten

M29: ICTU zorgt dat een project verantwoord kan starten
Voordat een softwareontwikkelproject, dat conform de Kwaliteitsaanpak gaat werken, start, toetst ICTU of het project gebaseerd is op een adequaat projectvoorstel en of zij beschikt over de benodigde kennis, diensten en hulpmiddelen om het project te ondersteunen. Zo niet, dan voert de organisatie ofwel het project niet uit, ofwel past zij het projectvoorstel aan en/of organiseert zij de benodigde kennis, diensten en hulpmiddelen.

Voordat ICTU een project verantwoord kan starten en het door de afdeling ICTU Software Diensten (ISD) ondersteund kan worden, moet aan een aantal randvoorwaarden zijn voldaan:

1. Het project ontwikkelt en/of onderhoudt maatwerksoftware volgens deze Kwaliteitsaanpak.
2. De opdrachtgever heeft kennisgenomen van en commiteert zich aan de Kwaliteitsaanpak.
3. Er is adequaat projectmanagement en -governance ingericht, zowel aan opdrachtgeverszijde als aan ICTU-zijde.
4. De omvang, de snelheid van opschaling, en de behoefte aan ondersteuning van het project is zodanig dat dit samengaat met ongestoorde dienstverlening aan de lopende projecten.
5. Er is een ICTU-projectleider verantwoordelijk voor projectuitvoering, projectresultaat en de geleverde kwaliteit.
6. De projectleider en andere projectmedewerkers met projectmanagementverantwoordelijkheid hebben kennis van en ervaring met de Kwaliteitsaanpak en het ecosysteem.
7. Het project zet een kwaliteitsmanager in met kennis van en ervaring met de Kwaliteitsaanpak en het ecosysteem.
8. Het project doorloopt voorfase en realisatiefase volgens de Kwaliteitsaanpak.
9. De dienstverlening met betrekking tot het ecosysteem is afgestemd tussen project en de afdeling ISD en is onderdeel van het aanbod van ICTU aan de opdrachtgever.

Voorafgaand aan de start van een project organiseert ICTU een "Doordacht-van-Start-sessie", waarin aandacht besteed wordt aan de bovengenoemde punten. Indien een dergelijke sessie onverhoopt niet is voorzien voor het project, vindt de toetsing op een alternatief moment plaats. In alle gevallen heeft de toets plaatsgevonden voordat de opdrachtgever een definitief projectvoorstel ontvangt.

Projectvoorstellen van ICTU voor projecten die door ISD worden ondersteund, hebben ten minste de onderstaande stappen doorlopen. N.B: Input voor een projectvoorstel bestaat niet alleen uit schriftelijke communicatie, maar ook uit gesprekken met opdrachtgever en andere belanghebbenden.

1. De verwachtingen van de opdrachtgever met betrekking tot omvang, doorlooptijd en kosten zijn geïdentificeerd voordat het projectvoorstel wordt geschreven.
2. De schattingen voor doorlooptijd en teambezetting zijn gebaseerd op een expertschatting en optioneel een functiepuntentelling.
3. Zowel de afdeling Relatiemanagement als de afdeling ISD reviewen het projectvoorstel. ISD gebruikt hiervoor de onderstaande checklist.
4. De relatiemanager en de beoogd projectleider en/of software delivery manager nemen het projectvoorstel mondeling door met de opdrachtgever.

Een projectvoorstel bevat ten minste de volgende onderdelen:

- een beknopte en heldere omschrijving van het doel van het project: welk probleem van de opdrachtgever lost het project op;
- een beschrijving van het beoogde resultaat van het project;
- een beschrijving van de deliverables van het project;
- een beschrijving van de aanpak van het project;
- een beschrijving van de planning van het project, inclusief doorlooptijd, aantal sprints, lengte van sprints, eventuele voorbereidingstijd, sprint 0, overdrachtsfase, en nazorg;
- een beschrijving van de rollen in het project, door welke organisatie deze rollen worden ingevuld, hoeveel tijd dat kost en welke eisen aan competenties en/of ervaring worden gesteld;
- een beschrijving van het projectmanagement en de governance op het project, inclusief opdrachtgever (organisatie, naam en functie) en product owner (organisatie, naam en functie) en overzicht rapportages;
- een beschrijving van het kwaliteitsmanagement op het project;
- een beschrijving van het risicomanagement op het project;
- een schatting van de kosten van het project;
- een beschrijving van de randvoorwaarden en aannames die onder het plan liggen;
- een beschrijving van de belangrijkste risico's voor het projectresultaat;
- een beschrijving van relaties en/of afhankelijkheden met andere projecten door ICTU voor deze opdrachtgever, dan wel voor andere opdrachtgevers, dan wel andere projecten bij de opdrachtgever die niet door ICTU worden uitgevoerd;
- een beschrijving van de belanghebbenden en hun belangen bij het project. Mogelijke belanghebbenden zijn bijvoorbeeld eindgebruikers, burgers, afdelingen bij de opdrachtgever, ketenpartners, en beheerorganisaties;
- relevante referenties;
- een distributielijst;
- een versienummer, datum, auteur, status;
- een algemene beschrijving van ICTU.

In het geval van een voorstel voor een voorfase, zijn de volgende aanvullende onderdelen opgenomen:

- hoe, door wie, en wanneer wordt besloten over het vervolg op de voorfase,
- of er mensen beschikbaar worden gehouden, en, zo ja, hoe lang, tussen voorfase en eventuele realisatiefase.

In het geval van een voorstel voor een realisatiefase, zijn de volgende aanvullende onderdelen opgenomen:

- een releaseplanning;
- de data waarop de software voor het eerst naar een acceptatieomgeving wordt opgeleverd en het moment dat de software voor het eerst in productie gaat.

Rationale

Om de Kwaliteitsaanpak succesvol in te zetten, is ondersteuning van het project nodig. Het vooraf toetsen of deze ondersteuning in de juiste mate beschikbaar is, voorkomt dat projecten niet of niet goed volgens de Kwaliteitsaanpak kunnen werken.

7.2 M19: ICTU biedt projecten een afgeschermde digitale omgeving

M19: ICTU biedt projecten een afgeschermde digitale omgeving
ICTU geeft de projecten de beschikking over eigen, afgeschermde digitale omgevingen, waarbinnen ze de door het project ontwikkelde software en tools kunnen installeren en waartoe op een beheerste manier toegang wordt verleend.

ICTU ondersteunt dit met Docker en/of virtuele machines en een VLAN (Virtual local area network) per project. Een nieuwe afgeschermde digitale omgeving is binnen een werkweek na aanvraag beschikbaar.

De software delivery manager is verantwoordelijk voor het autoriseren van personen voor toegang tot de beveiligde projectomgeving. De afdeling ICTU Software Diensten (ISD) beheert de basisconfiguratie van de afgeschermde digitale omgevingen. Projecten wijken alleen in overleg met ISD af van de basisconfiguratie. Als bepaalde afwijkingen vaker voorkomen, kan dit leiden tot het maken van aanpassingen aan de basisconfiguratie.

Rationale

Door het bieden van een afgeschermde digitale omgeving zijn de afhankelijkheden en invloeden tussen projecten minimaal en worden beveiligingsrisico's verkleind.

7.3 M18: ICTU biedt ondersteuning voor verplicht gestelde tools

M18: ICTU biedt ondersteuning voor verplicht gestelde tools
ICTU zorgt voor technische en functionele ondersteuning aan projecten bij het gebruik van alle verplichte tools.

ICTU zorgt voor ondersteuning van de bij M16: Het project gebruikt tools voor vastgestelde taken verplicht gestelde tools. Een team van specialisten met kennis, ervaring en capaciteit is beschikbaar voor ondersteuning aan projecten.

Bij de selectie van tools ter ondersteuning van de projectuitvoering geeft ICTU de voorkeur aan open source tools. Ook tools die ICTU zelf ontwikkelt ter ondersteuning van softwareontwikkelprojecten worden bij voorkeur open source beschikbaar gesteld.

Rationale

De keuze om het gebruik van een aantal tools verplicht te stellen (M16: Het project gebruikt tools voor vastgestelde taken) volgt uit de belangrijke rol die die tools spelen in de ontwikkelstraat en in het kwaliteitssysteem. Met de verplichting komt ook een verantwoordelijkheid: om projecten in staat te stellen snel en effectief met deze tools te werken, moeten die projecten ondersteund worden.

De verplicht gestelde tools zijn beperkt in aantal, bewezen en gangbaar; veel medewerkers zullen deze tools al kennen.

De voorkeur voor open source tools is conform de rationale uit NORA (Nederlandse Overheid Referentiearchitectuur) voor het gebruik van open source tools, zoals beschreven in NORA v3.0 drijfveer "Beleid open standaarden". De voorkeur voor het open source beschikbaar stellen van eigen ontwikkelde tools is conform de "Beleidsbrief vrijgeven van de broncode van overheidssoftware" van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, 17 april 2020.

7.4 M11: ICTU beheert, onderhoudt en implementeert de Kwaliteitsaanpak en kwaliteitsnormen

M11: ICTU beheert, onderhoudt en implementeert de Kwaliteitsaanpak en kwaliteitsnormen
ICTU beheert, onderhoudt en implementeert de Kwaliteitsaanpak en de kwaliteitsnormen. Aanpassingen zijn gebaseerd op praktijkervaring, nieuwe inzichten en nieuwe mogelijkheden voor meting en analyse. Iedere medewerker kan wijzigingsvoorstellen indienen bij ICTU. ICTU behandelt de wijzigingsvoorstellen, kiest de te nemen actie bij elk wijzigingsvoorstel en legt de wijzigingsvoorstellen en besluiten vast.

De Kwaliteitsaanpak wordt voor ICTU onderhouden door de afdeling ICTU Software Expertise (ISE). Iedereen die betrokken is bij softwareontwikkelprojecten kan een wijzigingsvoorstel indienen bij het hoofd van de afdeling ISE; die zorgt voor behandeling van en besluitvorming over het wijzigingsvoorstel. De afdeling zorgt ook zelf voor actualisering van de Kwaliteitsaanpak, op basis van praktijkervaringen en nieuwe inzichten.

Bij een verandering van de Kwaliteitsaanpak zorgt het hoofd van de afdeling ISE voor een passend implementatie- en verandertraject.

Rationale

Expliciet beheer en onderhoud van de ICTU Kwaliteitsaanpak Softwareontwikkeling is nodig om geleerde lessen, nieuwe inzichten uit bijvoorbeeld wetenschappelijke literatuur en nieuwe technische mogelijkheden voor meting en analyse te verwerken in de Kwaliteitsaanpak. De Kwaliteitsaanpak wordt door ICTU - en niet door een project - onderhouden, zodat deze bij meerdere projecten uniform kan worden toegepast.

7.5 M12: ICTU publiceert nieuwe versies van de Kwaliteitsaanpak en normen periodiek en op een vaste locatie

M12: ICTU publiceert nieuwe versies van de Kwaliteitsaanpak en normen periodiek en op een vaste locatie
ICTU publiceert periodiek een nieuwe versie van de Kwaliteitsaanpak en/of de kwaliteitsnormen op een vaste, bekende locatie.

De ICTU Kwaliteitsaanpak Softwareontwikkeling is te vinden op de ICTU-website (https://www.ictu.nl/kwaliteitsaanpak) en, inclusief templates en self-assessment checklist, op het ICTU Portaal (Sharepoint). Publicatie van een nieuwe versie wordt aangekondigd via een e-mail naar belanghebbenden en de 'Zeepkist', een terugkerende informatiebijeenkomst van de afdeling ICTU Software Expertise (ISE).

Rationale

Medewerkers moeten te allen tijde de actuele Kwaliteitsaanpak en -normen kunnen raadplegen. Welke versie actueel is en wanneer een nieuwe versie actueel wordt, is essentiële informatie voor de planning van werkzaamheden binnen de projecten en binnen de afdeling als geheel.

7.6 M33: ICTU organiseert periodiek een gezamenlijke self-assessment ten aanzien van de Kwaliteitsaanpak

M33: ICTU organiseert periodiek een gezamenlijke self-assessment ten aanzien van de Kwaliteitsaanpak
ICTU organiseert periodiek een gezamenlijke self-assessment ten aanzien van de Kwaliteitsaanpak die inzicht geeft in de huidige status van de Kwaliteitsaanpak en aanleiding kan geven tot het nemen van maatregelen om de Kwaliteitsaanpak en de ondersteuning daarvan door ICTU te verbeteren.

Deze gezamenlijke self-assessment geeft inzicht in de huidige status van de Kwaliteitsaanpak en kan aanleiding geven tot het nemen van maatregelen om de Kwaliteitsaanpak en de ondersteuning daarvan door ICTU te verbeteren.

ICTU nodigt de lopende projecten jaarlijks uit om deel te nemen aan de gezamelijke self-assessment. Deelname door projecten is vrijwillig. Voor het doen van de self-assessment stelt ICTU een ondersteunend formulier beschikbaar.

De projecten identificeren aan de hand van het formulier de belangrijkste verschillen tussen Kwaliteitsaanpak en werkwijze in het project en rapporteren hierover aan ICTU.

ICTU voegt de self-assessments van de deelnemende projecten samen en maakt een analyse van de resultaten. De analyse gaat in op:

- Opvallende overeenkomsten en verschillen tussen projecten,
- Opvallende overeenkomsten en verschillen met eerdere gezamenlijke self-assessments,

- Opvallende maatregelen, bijvoorbeeld maatregelen die veel projecten niet of deels toepassen, en
- Gemaakte opmerkingen door de deelnemende projecten.

ICTU organiseert een bespreking van de analyse met de deelnemende projecten. Hieruit vloeiende verbeteracties voor de Kwaliteitsaanpak worden door ICTU geprioriteerd en via de backlog voor de Kwaliteitsaanpak afgehandeld. Bij grotere verbeteracties betrekt ICTU de kwaliteitsmanagers van de belanghebbende projecten.

De gezamenlijke self-assessment is een intern product en de niet-geanonimiseerde resultaten worden alleen gedeeld met de deelnemende projecten. De geanonimiseerde resultaten kunnen worden gedeeld met belanghebbenden en belangstellenden binnen en buiten ICTU.

Rationale

Door een gezamenlijke self-assessment te doen met meerdere projecten tegelijkertijd onstaat er inzicht in de mate waarin maatregelen van de Kwaliteitsaanpak toegepast worden en zinvol zijn. Het gesprek over de uitkomsten van de gezamenlijke self-assessment levert input voor verbetering van de Kwaliteitsaanpak zelf.

Bijlagen

A Terminologie en afkortingen

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

Term/afkorting	Toelichting
actor	een persoon die of een extern informatiesysteem dat een handeling verricht op het informatiesysteem
API	application programming interface
ART	automatische **regressietest**
auditing	Vastlegging van de door een actor verrichtte handelingen.
authenticatie	het vaststellen van de identiteit van een **actor**
autorisatie	aan een **actor** toegekende rechten
BIA	business impact analysis
BIO	Baseline Informatiebeveiliging Overheid
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
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
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)

Term/afkorting	Toelichting
NORA	Nederlandse OverheidsReferentieArchitectuur
NPR	Nederlandse PraktijkRichtlijn
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
PSA	projectstartarchitectuur
PvE	programma van eisen
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
SAD	software-architectuurdocument
softwareontwikkeling	een activiteit die nieuwe software maakt en/of bestaande software aanpast
usability	gebruiksvriendelijkheid
use case	een afgebakende eenheid van interactie tussen een **actor** en het systeem
TVA	threat and vulnerability assessment
UX	user experience
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIRBI	Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie
VM	virtual machine, virtuele machine
vrijgaveadvies	advies om een release vrij te geven, met een testverslag dat tenminste alle nog openstaande testbevindingen en geconstateerde beveiligingsbevindingen bevat

B Bronnen

De onderstaande tabel verwijst naar regelmatig gebruikte bronnen.

Bron	Toelichting
BIO	Baseline Informatiebeveiliging Overheid.
ISO 9241-210:2019	Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems.
NCSC ICT-beveiligingsrichtlijnen voor webapplicaties	De ICT-beveiligingsrichtlijnen voor webapplicaties geven een leidraad voor veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur.

Bron	Toelichting
NEN-ISO/IEC 25010:2011	Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models.
NEN-ISO/IEC 27001:2017	Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen
NEN-ISO/IEC 27002:2017	Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging
NEN 7510:2017	Informatiebeveiliging in de zorg.
NEN NPR 5325:2017	Praktijkrichtlijn voor het overdragen van software.
NEN NPR 5326:2019	Praktijkrichtlijn voor risicobeheersing bij softwareontwikkeling.
NORA	Referentiearchitectuur voor de Nederlandse Overheid.
OWASP Top-10	De OWASP Top-10 is een op consensus gebaseerd overzicht van de meest kritische beveiligingsrisico's voor webapplicaties.
Wbni 2018	Wet Beveiliging Netwerk- en Informatiesystemen. Beschrijft de meldplicht en de zorgplicht die van toepassing zijn op organisaties die vitaal zijn én op digitale dienstverleners.

C Overzicht maatregelen

Hieronder zijn alle maatregeldefinities uit deze Kwaliteitsaanpak opgenomen, op volgorde van maatregelnummer.

M01: Het project levert in elke fase vastgestelde producten en informatie op
Iedere projectfase levert specifieke informatie op. De voorfase levert inzicht in de functionele en niet-functionele eisen, ontwerp en architectuur, testplannen, operationele risico's, en benodigde kwaliteitsmaatregelen. Deze informatie wordt tijdens de realisatiefase waar nodig bijgewerkt. De realisatiefase levert één of meerdere werkende versies van de software met regressietests, aangevuld met een vrijgaveadvies, release notes en installatiedocumentatie.

M02: Het project zorgt dat het product continu aan de kwaliteitsnormen voldoet
Producten voldoen zo snel mogelijk vanaf de start van een project aan de door het project en ICTU vastgestelde kwaliteitsnormen en blijven daar zo veel mogelijk aan voldoen. De kwaliteit van producten, die nog niet zijn afgerond of nog niet aan de normen voldoen, wordt door het project bewaakt. Het voldoen aan de kwaliteitsnormen is onderdeel van de Definition of Done en herstel van de kwaliteit wordt planmatig opgepakt.

M03: Het project zorgt dat het product traceerbaar aan eisen voldoet
Eisen zijn wederzijds traceerbaar naar bewijsmateriaal, zoals logische testgevallen, dat de eis gerealiseerd is; dat wil zeggen dat geadministreerd is bij welke eis bewijsmateriaal hoort en vice versa. Dit wordt waar mogelijk met tooling ondersteund.

M04: Het project borgt de correcte werking van het product met geautomatiseerde regressietests
Regressietests - tests die verifiëren of eerder ontwikkelde software nog steeds correct werkt na wijzigingen in de software of aansluiting op andere externe koppelvlakken - zijn geautomatiseerd.

M05: Het project hanteert een iteratief en incrementeel ontwikkelproces
Projecten werken iteratief en incrementeel; dit betekent dat een project in korte iteraties werkt, waarbij elke iteratie een werkende versie van de software oplevert die extra waarde vertegenwoordigd voor de opdrachtgever. Behalve de software levert het project iedere iteratie telkens ook alle andere producten bijgewerkt op. Elke iteratie worden verwachtingen en werkelijke resultaten vergeleken en de werkwijze aangescherpt op basis van inzichten en bevindingen.

M06: Het project meet kwaliteitsnormen geautomatiseerd en frequent
Het voldoen aan de kwaliteitsnormen die geautomatiseerd gemeten kunnen worden, wordt frequent en minimaal één keer per dag gemeten.

M07: Het project gebruikt een continuous delivery pipeline om het product te bouwen, testen en op te leveren
Er is een geautomatiseerde continuous delivery pipeline die aantoonbaar correct werkt en de software bouwt, installeert in testomgevingen, test op functionele en niet-functionele eigenschappen en oplevert.

M08: Het project maakt technische schuld inzichtelijk en lost deze planmatig op
Technische schuld is inzichtelijk en wordt planmatig aangepakt. De kwaliteitsmanager is verantwoordelijk voor het inzichtelijk maken van de technische schuld. De software delivery manager is verantwoordelijk voor het planmatig aanpakken van de technische schuld en zorgt dat het Scrumteam regelmatig en voldoende tijd heeft om technische schuld te voorkomen en op te lossen. Het Scrumteam is verantwoordelijk voor het zoveel mogelijk voorkomen van technische schuld en voor het identificeren van technische schuld die toch optreedt.

M09: Het project implementeert nieuwe versies van de Kwaliteitsaanpak binnen de gestelde termijn
Projecten implementeren nieuwe versies van Kwaliteitsaanpak en kwaliteitsnormen binnen de door ICTU gestelde termijn. De projectleider is verantwoordelijk voor de implementatie.

M10: Het project kent een wekelijks projectoverleg
De projectleider organiseert een periodiek projectoverleg. Dit overleg vindt wekelijks plaats en duurt niet langer dan een uur. Vereiste aanwezigen zijn de projectleider, de software delivery manager, de Scrummaster, een vertegenwoordiger uit elk van de Scrumteams en de kwaliteitsmanager van het project; andere aanwezigen kunnen zijn: de projectarchitect en de product owner.

De agenda voor dit overleg bestaat ten minste uit de volgende onderwerpen: mededelingen, actie- en besluitenlijst, personele zaken, planning en voortgang, kwaliteit en architectuur, risico's en aandachtspunten.

M11: ICTU beheert, onderhoudt en implementeert de Kwaliteitsaanpak en kwaliteitsnormen
ICTU beheert, onderhoudt en implementeert de Kwaliteitsaanpak en de kwaliteitsnormen. Aanpassingen zijn gebaseerd op praktijkervaring, nieuwe inzichten en nieuwe mogelijkheden voor meting en analyse. Iedere medewerker kan wijzigingsvoorstellen indienen bij ICTU. ICTU behandelt de wijzigingsvoorstellen, kiest de te nemen actie bij elk wijzigingsvoorstel en legt de wijzigingsvoorstellen en besluiten vast.

M12: ICTU publiceert nieuwe versies van de Kwaliteitsaanpak en normen periodiek en op een vaste locatie
ICTU publiceert periodiek een nieuwe versie van de Kwaliteitsaanpak en/of de kwaliteitsnormen op een vaste, bekende locatie.

M13: Het project gebruikt ISO-25010 voor de specificatie van productkwaliteitseisen
Voor specificatie en documentatie van vereiste en gewenste kwaliteitseigenschappen, de niet-functionele eisen, maken projecten gebruik van de terminologie uit NEN-ISO/IEC 25010. Projecten gebruiken NEN-ISO/IEC 25010 om te controleren of alle relevante kwaliteitseigenschappen van het op te leveren eindproduct worden meegenomen in de ontwikkeling en/of onderhoud van het product.

M14: Het project bereidt samen met opdrachtgever en belanghebbenden de realisatie voor
Projecten hebben een voorbereidingsfase, "voorfase" genoemd, voorafgaand aan de realisatiefase. Voor het uitvoeren van de voorfase zijn vertegenwoordigers van de opdrachtgever, de beoogde beheerpartij en andere belanghebbenden betrokken die meewerken aan het realiseren van een deel van de op te leveren producten. Het doel van de voorfase is beeld krijgen van de te realiseren oplossing, van de risico's die zich tijdens realisatie kunnen voordoen en van de kaders waarbinnen de oplossing moet passen; tijdens de realisatiefase vinden bouw en onderhoud van de software en actualiseren en afronden van documentatie plaats.

M16: Het project gebruikt tools voor vastgestelde taken
ICTU stelt het gebruik van tools verplicht voor:
1. backlog management en agile werken,
2. inrichten en uitvoeren van een continuous delivery pipeline,
3. monitoren van de kwaliteit van broncode,
4. versiebeheer van op te leveren producten,
5. release van software,
6. maken van testrapportages,

7. maken van kwaliteitsrapportages,
8. controleren van de configuratie op aanwezigheid van bekende kwetsbaarheden,
9. controleren van door de applicatie gebruikte versies van externe software op aanwezigheid van bekende kwetsbaarheden,
10. controleren van de software op aanwezigheid van kwetsbare constructies,
11. testen van performance en schaalbaarheid,
12. testen op toegankelijkheid van de applicatie en
13) produceren van een "software bill of materials" (SBoM).

M18: ICTU biedt ondersteuning voor verplicht gestelde tools
ICTU zorgt voor technische en functionele ondersteuning aan projecten bij het gebruik van alle verplichte tools.

M19: ICTU biedt projecten een afgeschermde digitale omgeving
ICTU geeft de projecten de beschikking over eigen, afgeschermde digitale omgevingen, waarbinnen ze de door het project ontwikkelde software en tools kunnen installeren en waartoe op een beheerste manier toegang wordt verleend.

M21: Het project selecteert medewerkers op basis van kwaliteit
Bij de inzet van medewerkers gaat kwaliteit boven andere aspecten, zoals beschikbaarheid, prijs en doorlooptijd.

M23: Het project zorgt voor de aanwezigheid van ervaring met de Kwaliteitsaanpak
De software delivery manager zorgt ervoor dat bij nieuwe projecten wordt gestart met ten minste twee projectleden die bekend zijn met de Kwaliteitsaanpak.

M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen
Projecten laten periodiek de beveiliging van de ontwikkelde software beoordelen. Een beveiligingsexpert onderzoekt de code zowel geautomatiseerd als handmatig op veelvoorkomende kwetsbaarheden en op het voldoen aan voorgeschreven beveiligingsnormen. Overheidsspecifieke beveiligingsnormen of -raamwerken, zoals de BIO (Baseline Informatiebeveiliging Overheid), bieden een basis voor de beoordeling. Bevindingen uit de beveiligingstest worden vastgelegd als onderdeel van de werkvoorraad voor het ontwikkelproces.

M27: Het project sluit projectfasen en zichzelf expliciet af
Afsluiting van een projectfase gebeurt expliciet en gecontroleerd: alle producten, zoals documentatie, broncode, referentiedata en credentials, die in de af te sluiten fase nodig waren of zijn opgeleverd, worden gearchiveerd. Indien er geen volgende fase is voorzien op korte termijn, dienen alle producten van de laptops van de projectmedewerkers verwijderd te worden.

M28: Het project voert periodiek een self-assessment uit ten aanzien van de Kwaliteitsaanpak
De projectleider organiseert periodiek een self-assessment ten aanzien van de Kwaliteitsaanpak.

M29: ICTU zorgt dat een project verantwoord kan starten
Voordat een softwareontwikkelproject, dat conform de Kwaliteitsaanpak gaat werken, start, toetst ICTU of het project gebaseerd is op een adequaat projectvoorstel en of zij beschikt over de benodigde kennis, diensten en hulpmiddelen om het project te ondersteunen. Zo niet, dan voert de organisatie ofwel het project niet uit, ofwel past zij het projectvoorstel aan en/of organiseert zij de benodigde kennis, diensten en hulpmiddelen.

M30: Het project identificeert, mitigeert en bewaakt risico's
Het project identificeert, mitigeert en bewaakt projectspecifieke risico's voorafgaand aan en tijdens de projectuitvoering. Het project houdt een risicolog bij met geïdentificeerde risico's. De uitkomsten van de "Doordacht-van-Start-sessie" vormen het startpunt van deze risicolog. Risico's die tijdens de voorfase worden geïdentificeerd, bijvoorbeeld bij de productrisicoanalyse, worden toegevoegd aan de risicolog. Tijdens de voorfase en bij de start van de realisatiefase worden risicosessies gehouden met (vertegenwoordigers van) de belanghebbenden om verdere risico's te identificeren. Het project identificeert en implementeert mitigerende maatregelen danwel accepteert expliciet de geïdentificeerde risico's. Het project bewaakt de risicolog en uitvoering van de mitigerende maatregelen tijdens het IPO.

M31: Het project beschikt over vastgestelde informatie
Voor een goede uitvoering van het project is specifieke informatie nodig. De opdrachtgever zorgt dat het project bij de start van de voorfase inzicht heeft in de informatie die typisch wordt vastgelegd in een projectstartarchitectuur, business impact analysis en privacy impact assessment. Waar nodig werkt de opdrachtgever de informatie bij tijdens de voorfase en realisatiefase.

M33: ICTU organiseert periodiek een gezamenlijke self-assessment ten aanzien van de Kwaliteitsaanpak
ICTU organiseert periodiek een gezamenlijke self-assessment ten aanzien van de Kwaliteitsaanpak die inzicht geeft in de huidige status van de Kwaliteitsaanpak en aanleiding kan geven tot het nemen van maatregelen om de Kwaliteitsaanpak en de ondersteuning daarvan door ICTU te verbeteren.

M34: Het project draagt software beheerst over
Als de software op enig moment door een andere partij dan ICTU verder ontwikkeld en/of onderhouden zal worden, draagt het project zorg voor een beheerste overdracht. Beheerdocumentatie, broncode en testmiddelen zijn van dusdanige kwaliteit en compleetheid dat de andere partij de software efficiënt en effectief kan doorontwikkelen en/of onderhouden.

D Relatie met NEN NPR 5326

De Nederlandse Praktijkrichtlijn "Risicobeheersing bij ontwikkeling en onderhoud van maatwerksoftware" (NPR 5326) beschrijft beheersmaatregelen voor een deel van de risico's die inherent zijn aan softwareontwikkeling op maat. Onderstaande tabel laat de relatie zien tussen de risicobeheersmaatregelen uit de NPR 5326 en de maatregelen uit deze Kwaliteitsaanpak.

NPR 5326 risicobeheersmaatregel	Maatregelen Kwaliteitsaanpak	Toelichting
Maatregel 01: Belanghebbenden identificeren en betrekken	M14: Het project bereidt samen met opdrachtgever en belanghebbenden de realisatie voor	Voorafgaand aan en tijdens de voorfase identificeert en betrekt ICTU de belanghebbenden
Maatregel 02: Belangrijke niet-functionele eisen identificeren	M01: Het project levert in elke fase vastgestelde producten en informatie op	De niet-functionele eisen zijn een van de uitkomsten van de voorfase
Maatregel 03: Belangrijke functionele eisen identificeren	M01: Het project levert in elke fase vastgestelde producten en informatie op	De functionele eisen zijn een van de uitkomsten van de voorfase
Maatregel 04: Productdecompositie in incrementeel opleverbare delen met business-waarde	M01: Het project levert in elke fase vastgestelde producten en informatie op	De product backlog is een van de uitkomsten van de voorfase
Maatregel 05: Technische schuld identificeren, inzichtelijk maken en planmatig oplossen	M08: Het project maakt technische schuld inzichtelijk en lost deze planmatig op	
Maatregel 06: Oplossingsrichtingen verkennen	M01: Het project levert in elke fase vastgestelde producten en informatie op	Tijdens de voorfase worden oplossingsrichtingen verkend, bijvoorbeeld met behulp van een prototype
Maatregel 07: Incrementele oplevering van het product	M05: Het project hanteert een iteratief en incrementeel ontwikkelproces	ICTU hanteert een iteratief en incrementeel ontwikkelproces
Maatregel 08: Iteratieve ontwikkelaanpak	M05: Het project hanteert een iteratief en incrementeel ontwikkelproces	ICTU hanteert een iteratief en incrementeel ontwikkelproces
Maatregel 09: Geautomatiseerde ontwikkelpijplijn inrichten	M07: Het project gebruikt een continuous delivery pipeline om het product te bouwen, testen en op te leveren	

NPR 5326 risicobeheersmaatregel	Maatregelen Kwaliteitsaanpak	Toelichting
Maatregel 10: Voortdurend voldoen aan de eisen met regressietests	M04: Het project borgt de correcte werking van het product met geautomatiseerde regressietests	
Maatregel 11: Voortgangsbewaking met burndown charts	M10: Het project kent een wekelijks projectoverleg	Projecten bespreken de voortgang in het wekelijks projectoverleg aan de hand van backlog informatie uit het backlog management systeem
Maatregel 12: Een officiële producteigenaar met mandaat	M05: Het project hanteert een iteratief en incrementeel ontwikkelproces	ICTU hanteert Scrum, inclusief de rol van de product owner
Maatregel 13: Toepassen van een kwaliteitgedreven ontwikkelmethode		De Kwaliteitsaanpak schrijft geen ontwikkelmethode voor aan de projecten; de borging van kwaliteitsnormen zal echter wel invloed hebben op de gevolgde ontwikkelmethode
Maatregel 14: Archivering	M27: Het project sluit projectfasen en zichzelf expliciet af	
Maatregel 15: Deugdelijke overdracht	M34: Het project draagt software beheerst over	
Maatregel 16: Teams met specialistische kennis en hulpmiddelen ondersteunen	M18: ICTU biedt ondersteuning voor verplicht gestelde tools, M19: ICTU biedt projecten een afgeschermde digitale omgeving	
Maatregel 17: Continu risicomanagement	M02: Het project zorgt dat het product continu aan de kwaliteitsnormen voldoet, M10: Het project kent een wekelijks projectoverleg, M30: Het project identificeert, mitigeert en bewaakt risico's	Projecten voldoen continu aan de kwaliteitsnormen, identificeren en mitigeren projectspecifieke risico's en bespreken de risico's in het wekelijkse projectoverleg

E Wijzigingsgeschiedenis

Versie 2.5.0, nog te releasen

Kwaliteitsaanpak

- HTML-versie van de Kwaliteitsaanpak toegevoegd als toegankelijk alternatief voor de PDF-versie.
- Op meerdere plekken in de Kwaliteitsaanpak de gebruikte rollen aangescherpt of verbeterd door bijvoorbeeld ICTU te vervangen door project, team door Scrumteam en projectleider door software delivery manager.
- Bij maatregel "Het project levert in elke fase vastgestelde producten en informatie op" (M01): software bill of materials toegevoegd als op te leveren informatie.
- Bij maatregel "Het project gebruikt tools voor vastgestelde taken" (M16): de lijst van verplichte tools en ondersteunde tools gelijk getrokken, de genoemde tools bijgewerkt en software bill of materials toegevoegd als taak.
- Bij maatregel "Het project voert periodiek een self-assessment uit ten aanzien van de Kwaliteitsaanpak" (M28): de rol van de kwaliteitsmanager bij het uitvoeren van de self-assessment toegevoegd.
- Nieuwe maatregel "ICTU organiseert periodiek een gezamenlijke self-assessment ten aanzien van de Kwaliteitsaanpak" (M33) toegevoegd.
- Nieuwe maatregel "Het project draagt software beheerst over" (M34) toegevoegd.
- De term 'standup' vervangen door de officiële term 'Daily Scrum'.
- Kruisverwijzingen tussen maatregelen verwijderd om de onderhoudbaarheid van de tekst te vergroten.

Template Niet-Functionele Eisen

- Axe-core bijgewerkt naar versie 4.6 in de tabel met de WCAG 2.1 succescriteria.

Versie 2.4.0, 12 januari 2022

Kwaliteitsaanpak

- De titel van maatregel "Het project levert in elke fase vastgestelde informatie over het product op" (M01) veranderd in "Het project levert in elke fase vastgestelde producten en informatie op" zodat de titel beter past bij de scope van de maatregel.
- Bij maatregel "Het project levert in elke fase vastgestelde producten en informatie op" (M01): de tabel uitgebreid met product backlog, en de lopende tekst aangevuld en aangepast opdat deze consistent is met de tabel.
- Bij maatregel "Het project zorgt dat het product continu aan de kwaliteitsnormen voldoet" (M02): "Ook zorgt het project dat de performance van de software regelmatig wordt getest." toegevoegd.

Template Kwaliteitsplan

- Bijlage met periodieke (kwaliteits)controles toegevoegd.
- Beschrijvingen van release notes en performancetest toegevoegd.

Template Niet-Functionele Eisen

- Axe-core bijgewerkt naar versie 4.3 in de tabel met de WCAG 2.1 succescriteria.

Template Plan van Aanpak Realisatiefase

- UX: aanpassing producten uit de voorfase; verantwoordelijkheden van rol UX-designer aangevuld.
- Toelichting op te maken afspraken voor: release notes, vrijgaveadvies, beveiligingstest, performancetest.
- In hoofdstuk Verwachte inzet ICTU een tabel toegevoegd met te verwachten kosten voor door ICTU te benutten diensten.

Template Plan van Aanpak Voorfase

- UX: te realiseren producten toegevoegd: interactie-ontwerp (UX), wireframe, mockup, prototype, animatie.

Template Generiek

- Definities toegevoegd: release notes en vrijgaveadvies.

Self-assessment checklist

- Invulinstructie uitgebreid.
- Duidelijk gemaakt dat als maatregelen submaatregelen hebben alleen de status van submaatregelen hoeft te worden ingevuld.

Inwerkplan Kwaliteitsmanager

- Inwerkplan voor de rol van kwaliteitsmanager toegevoegd.

Versie 2.3.0, 14 mei 2021

Kwaliteitsaanpak

- Verwijzingen naar BIRT en de Releasemanager verwijderd uit de maatregel "Het project gebruikt tools voor vastgestelde taken" (M16) omdat deze tools niet meer ondersteund worden.
- Manifest verwijderd omdat de inhoud grotendeels terugkomt op andere plekken in de Kwaliteitsaanpak.

Samenvatting Kwaliteitsaanpak

- Een samenvatting van de Kwaliteitsaanpak als los document toegevoegd.

Presentatie Kwaliteitsaanpak

- Een presentatie van de Kwaliteitsaanpak als los document toegevoegd.

Alle templates

- Lijst van reviewers toegevoegd aan colofon.
- Leeswijzer uitgebreid met een beschrijving van de (standaard) bijlagen van de templates.
- Hoofdstuk "Managementsamenvatting" toegevoegd.

Template Detailtestplan

- Verwijzingen naar BIRT en de Releasemanager verwijderd.

Template Globaal Functioneel Ontwerp

- Template aangepast naar het gebruik van use cases om de functionaliteit te beschrijven.
- Kaders die niet relevant waren voor een GFO verwijderd.

Template Niet-Functionele Eisen

- Tabel met de WCAG 2.1 succescriteria toegevoegd. Per succescriterium geeft de tabel aan of Axe-core, en zo ja met welke regels, het succescriterium geautomatiseerd kan controleren.

Template Kwaliteitsplan

- Het kwaliteitsplantemplate sprak van een verantwoordingsparagraaf in alle documenten, maar deze paragraaf zat niet in de andere templates. Deze verantwoordingsparagrafen waren bedoeld om de eisen traceerbaar te maken. Omdat niet alle projecten dit nodig hebben, en er andere manieren in gebruik zijn om eisen traceerbaar te maken (bijvoorbeeld een losse administratie in Confluence) is de tekst over verantwoordingsparagrafen vervangen door een optionele paragraaf over tracering van eisen die nader kan worden ingevuld.
- Uit de bijlage "Gebruik van Jira" is de paragraaf "Velden in Jira" verwijderd omdat deze out-of-date en incompleet was en bovendien niet ging over velden in Jira, maar over metrieken die met behulp van de informatie in Jira gemeten kunnen worden. In plaats van deze paragraaf verwijst het kwaliteitsplantemplate naar de lijst op GitHub van metrieken die Quality-time kan meten.
- Uit de bijlage "Gebruik van Jira" is het issue type "Sprint bug" verwijderd omdat bugs die tijdens sprints worden gevonden normaal gesproken niet worden vastgelegd in Jira.
- Uit de bijlage "Gebruik van Jira" is het issue type "Custom issue" verwijderd omdat custom issues optioneel zijn en in de praktijk te weinig worden toegepast om apart te beschrijven.
- Het hoofdstuk "Kwaliteitsmaatregelen projectafsluiting" bevatte een lijst van activiteiten voor de software delivery manager. Die activiteiten zijn verplaatst naar het template plan van aanpak realisatiefase. De kwaliteitsmaatregelen bij projectafsluiting zijn beperkt tot een controle door de kwaliteitsmanager van de uitvoering van die activiteiten.

Template Plan van Aanpak Voorfase

- Paragraaf over projectafsluiting toegevoegd.

Template Plan van Aanpak Realisatiefase

- Paragraaf over projectafsluiting en bijlage met activiteiten voor projectafsluiting toegevoegd.

Alle documenten

- Vervang 'privacy impact analyse' door 'privacy impact assessment' en 'business impact analyse' door 'business impact analysis' zodat beide termen consequent op dezelfde manier geschreven worden.

Versie 2.2.0, 27 januari 2021

Kwaliteitsaanpak

- Afdeling ICTU Software Realisatie vervangen door de afdelingen ICTU Software Diensten en/of ICTU Software Expertise.
- ICTU ondersteunt alleen nog Quality-time als kwaliteitssysteem; HQ verwijderd.
- Leeswijzer uitgebreid met uitleg over beschrijvend en voorschrijvend karakter van de Kwaliteitsaanpak.
- Nieuwe maatregel "Het project beschikt over vastgestelde informatie" (M31) toegevoegd die beschrijft welke informatie de opdrachtgever aan een project beschikbaar stelt.
- Bij maatregel "Het project levert in elke fase vastgestelde informatie over het product op" (M01) met een plaatje de relaties tussen de voorfase producten toegelicht.
- De maatregel "Het project is gesplitst in een voorfase en een realisatiefase" (M14) hernoemd naar "Het project bereidt samen met opdrachtgever en belanghebbenden de realisatie voor".
- De maatregel "ICTU geeft de voorkeur aan open source tools" (M15) is verwijderd. De inhoud van M15 is verplaatst naar "ICTU biedt ondersteuning voor verplicht gestelde tools" (M18). Reden is dat de voorkeur voor open source geen apart uitvoerbare maatregel is, maar deel uitmaakt van de ondersteuning van projecten met tools.
- Bij maatregel "Het project gebruikt tools voor vastgestelde taken" (M16) performancetesttools toegevoegd.
- Maatregel "ICTU zorgt dat een aantal vastgestelde tools snel beschikbaar is voor een project" (M17) verwijderd omdat projecten deze tools ofwel via de kantoorautomatisering van ICTU kunnen gebruiken of zelf kunnen draaien in de afgeschermde digitale omgeving zoals beschreven bij M19.
- Bij maatregel "Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen" (M26) beter toegelicht onder welke voorwaarden de beveiligingstesten alleen door de opdrachtgever kunnen worden uitgevoerd.
- Bijlage "Risico's van softwareontwikkeling" verwijderd vanwege de overlap met de bijlage "Relatie met NEN NPR 5326".

Template Projectvoorstel Voorfase

- Template veranderd in een template voor een plan van aanpak voor de voorfase. Gebruik voor projectvoorstellen het ICTU-brede template.

Template Projectvoorstel Realisatiefase

- Template veranderd in een template voor een plan van aanpak voor de realisatiefase. Gebruik voor projectvoorstellen het ICTU-brede template.

Template Kwaliteitsplan

- Toegevoegd bij projectafsluiting dat VPN-keys, LDAP-accounts, Jira-accounts en werkstations moeten worden opgeschoond.
- Bij projectafsluiting de verantwoordelijke rol aangepast naar software delivery manager, conform Maatregel 27 in de Kwaliteitsaanpak.
- Het hanteren van codeerstandaarden toegevoegd aan de kwaliteitsmaatregelen tijdens de realisatiefase.

Versie 2.1.0, 2 september 2020

Kwaliteitsaanpak

- M30 ontbrak in de bijlage met het overzicht van alle maatregelen.
- Link naar Kwaliteitsaanpak op ICTU-website toegevoegd.

Alle templates

- Rubriceringsmogelijkheid conform Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) toegevoegd.
- Rubriceringsniveau, rubriceringsduur en totaal aantal bladzijden conform VIRBI 2014, bijlage 1, eis 6J toegevoegd.
- Link naar Kwaliteitsaanpak op ICTU-website toegevoegd in de bijlage over de Kwaliteitsaanpak.

Template Projectvoorstel Realisatiefase

- Projectvoorstel Realisatiefase template toegevoegd dat als basis kan dienen voor een projectvoorstel voor het uitvoeren van een realisatiefase aansluitend aan een voorfase.

Generiek template

- Generiek template toegevoegd dat als basis kan dienen voor documenten waarvoor nog geen specifiek template is.

Template Kwaliteitsplan

- Paragrafen 1.2, 1.5 en 1.6 uitgebreid met standaard teksten.
- Stakeholder management vervangen door het bescheidener identificeren van belanghebbenden en belangen.

Template Niet-Functionele Eisen

- Link naar Nederlandse vertaling van WCAG 2.1 toegevoegd aan het NFE-template.

Versie 2.0.0, 29 april 2020

- Naam van de Kwaliteitsaanpak veranderd van "Kwaliteitsaanpak ICTU Software Realisatie" naar "ICTU Kwaliteitsaanpak Softwareontwikkeling". Waar relevant "softwarerealisatie" veranderd in "softwareontwikkeling".
- Maatregelen, waar mogelijk, compacter geformuleerd.
- Maatregelen herverdeeld over de drie maatregelhoofdstukken.
- De maatregel "Het project levert in elke fase vastgestelde informatie over het product op" (M01) beknopter geformuleerd en toelichting op documenten uitgebreid.
- Bij de maatregelen "Het project zorgt dat het product continue aan de kwaliteitsnormen voldoet" (M02), "Het project maakt technische schuld inzichtelijk en lost deze planmatig op" (M08) en "Het project gebruikt tools voor vastgestelde taken" (M16) naast HQ ook Quality-time vermeld.
- Bij de maatregel "Het project maakt technische schuld inzichtelijk en lost deze planmatig op" (M08) toegevoegd dat projecten regelmatig en voldoende tijd besteden aan het voorkomen en oplossen van technische schuld.
- Bij de maatregel "Het project gebruikt tools voor vastgestelde taken" (M16) versiebeheer toegevoegd, met als concrete tools GitLab en Azure DevOps.
- Explicieter aandacht besteed aan gebruikskwaliteit in de maatregelen "Het project levert in elke fase vastgestelde informatie over het product op" (M01) en "Het project zorgt dat het product continue aan de kwaliteitsnormen voldoet" (M02). ISO 9241-210 opgenomen als standaard die ICTU hanteert voor gebruikskwaliteit.
- De maatregel "Betrokkenheid bij inzet" (M22) verwijderd.
- De maatregel "Implementatie van wijzigingen aan de kwaliteitsaanpak en -normen" (M24) verwijderd.
- Nieuwe maatregel toegevoegd voor het starten van projecten: "ICTU zorgt dat een project verantwoord kan starten" (M29).
- Nieuwe maatregel toegevoegd voor risicomanagement: "Projecten identificeren, mitigeren en bewaken risico's" (M30).
- Termen aangepast: 'projectverantwoordelijke' is vervangen door 'projectleider', 'projectenorganisatie' en 'projectorganisatie' door 'ICTU' en 'realiserend team' door 'projectteam'.
- De beschrijving van de rollen van software delivery manager en kwaliteitsmanager aangescherpt.
- Waar relevant bij de rationale van maatregelen verwezen naar overeenkomende risicobeheersmaatregelen uit de NPR 5326.
- Referenties aan de Baseline Informatiebeveiliging Rijksdienst (BIR) omgezet naar de Baseline Informatiebeveiliging Overheid (BIO).
- Referenties aan tools geactualiseerd.
- Tekstuele en stilistische verbeteringen.
- Actielijst toegevoegd aan self-assessment spreadsheet.
- Generatie van documenttemplates is onderdeel van de Kwaliteitsaanpak.

Versie 1.3.1, 1 mei 2019

- M14: Maatregeltitel ingekort zodat paginanummers in de inhoudsopgave niet overlappen.

Versie 1.3, 5 april 2019

- Overbodig kopje in de wijzigingsgeschiedenis van de generieke versie verwijderd.
- Bijlage met afkortingen toegevoegd.
- M07: Toegankelijkheidstests toegevoegd.
- M10: Aanwezigen bij periodiek projectoverleg aangepast.
- M16: Een tool voor het testen van toegankelijkheid toegevoegd.
- M01: Wbni, EN 301 549 en WCAG 2.1 als bron voor niet-functionele eisen toegevoegd. Toegankelijkheidsverklaring als mogelijke deliverable genoemd.
- M05: Iteratief en incrementeel ontwikkelproces: Sprint retrospective en sprint backlog toegevoegd.
- M16: Axe toegevoegd.
- WCAG 2.1 toegevoegd aan bijlage C: Documenten voor M01.

Versie 1.2, 1 augustus 2018

- M01: Op te leveren producten: Niet alle producten hoeven door het project te worden gemaakt.
- M02: Continu voldoen aan kwaliteitsnormen: Zo snel mogelijk voldoen aan kwaliteitsnormen in plaats van altijd.
- M13: Gebruik van NEN-ISO/IEC 25010: Verduidelijkt dat het om het toepassen van NEN-ISO/IEC 25010 in projecten gaat en verplaatsen naar hoofdstuk Producten.
- M19: Afgeschermde digitale omgeving: De titel van de maatregel verduidelijkt naar "afgeschermde digitale omgeving".
- M25: De inhoud is verplaatst naar M01: Op te leveren producten, M25 zelf is vervallen.
- M28: Self-assessment: Maatregel met betrekking tot self-assessment toegevoegd.
- Tekstuele en stilistische verbeteringen.
- Manifest toegevoegd.
- ICTU-specifieke invulling van maatregelen aangepast aan nieuwe organisatiestructuur en rollen zoals die in 2018 gelden.
- In M16: Verplichte tools, de verwijzing naar ICTU-specifieke SonarQube kwaliteitsprofielen verwijderd omdat ICTU de standaard Sonar Way kwaliteitsprofielen gebruikt.

Versie 1.1, 7 november 2017

- BIR-maatregelen toegevoegd.

Versie 1.0.2, 9 mei 2017

- Eerste publicatie.