ICTU Kwaliteitsaanpak Softwareontwikkeling

Samenvatting

Versie 4.0.0-dev, 06-06-2023

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” [NEN 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 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, waarbij ruimte wordt geboden voor variatie of alternatieve invulling. Bijvoorbeeld stelt de Kwaliteitsaanpak: software wordt minimaal bij iedere grote release of tenminste twee keer per jaar onderworpen aan een beveiligingstest door beveiligingsexperts die ICTU daarvoor inhuurt (zie M26: Het project laat de beveiliging van het ontwikkelde product periodiek beoordelen). Een alternatief is dat de 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 voortkomen uit de bestaande werkwijzen van de projecten. Zoals blijkt uit de self-assessment die ICTU regelmatig uitvoert op de toepassing van de Kwaliteitsaanpak.

3 Maatregelen

Hieronder zijn alle maatregeldefinities uit de Kwaliteitsaanpak opgenomen. Zie de Kwaliteitsaanpak zelf voor een uitgebreidere beschrijving van de maatregelen, inclusief context en rationale.

3.1 Producten

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.

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.

M32: Het project onderzoekt de kwaliteit van over te nemen software
Als tijdens een project bestaande software dient te worden afgebouwd, onderhouden en/of herbouwd, vindt een onderzoek plaats naar de kwaliteit van deze software.

M02: Het project bewaakt continu dat het product aan de kwaliteitsnormen voldoet
Projecten bewaken zo snel mogelijk vanaf de start de door het project en ICTU vastgestelde kwaliteitsnormen en voldoen daar zo snel en goed mogelijk aan. 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.

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 en categorisering 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.

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.

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 de testomgevingen, test op functionele en niet-functionele eigenschappen en oplevert, al dan niet inclusief installatie in de productieomgeving.

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.

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.

3.2 Processen

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 beheerorganisatie 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.

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.

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 vertegenwoordigt voor de opdrachtgever. Behalve de software werkt het project ook iedere iteratie alle andere producten bij. Elke iteratie worden verwachtingen en werkelijke resultaten vergeleken en wordt de werkwijze aangescherpt op basis van inzichten en bevindingen.

M35: Het project hanteert een agile architectuuraanpak
Tijdens de voorfase verwerkt het project de door de opdrachtgever opgestelde projectstartarchitectuur (PSA) in een eerste versie van het softwarearchitectuurdocument (SAD). Tijdens de realisatiefase werkt het project het SAD bij op basis van nieuwe inzichten.

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.

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. controleren van container images op aanwezigheid van bekende kwetsbaarheden,
12. testen van performance en schaalbaarheid,
13. testen op toegankelijkheid van de applicatie,
14. produceren van een "software bill of materials" (SBoM) en
15. opslaan van artifacten.

M28: Het project voert periodiek een self-assessment uit tegen de actuele versie van de Kwaliteitsaanpak
De projectleider organiseert periodiek een self-assessment tegen de actuele versie van de Kwaliteitsaanpak en zet verbeteracties uit, waar nodig.

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", die al voorafgaand aan de start van het project wordt uitgevoerd, vormen het startpunt van deze risicolog. Risico's die tijdens de voorfase worden geïdentificeerd, bijvoorbeeld bij de productrisicoanalyse, worden toegevoegd aan de risicolog. Ook 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.

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.

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.

3.3 Organisatie

M29: ICTU organiseert voor aanvang van een project de interne dienstverlening
Voordat ICTU een softwareontwikkelproject start, dat gaat werken conform de Kwaliteitsaanpak, maakt de beoogde projectleider afspraken met de afdelingen ICTU Software Diensten (ISD) en ICTU Software Expertise (ISE) over de af te nemen dienstverlening.

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.

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

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.

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.