Kwaliteitsaanpak ICTU Software Realisatie

ISR maatregelen

Manifest

ICTU werkt aan een betere digitale overheid. Wij willen het niveau van software-ontwikkeling bij de Nederlandse overheid naar een hoger plan brengen.
In ons werk zijn we het volgende gaan waarderen:

- Het belang van de burger staat voorop.
- We delen wat we goed kunnen, en gebruiken wat anderen beter doen.
- Op zoek naar de juiste oplossing is het experiment soms de kortste weg.
- Wij geloven in agile werken bij de overheid.
- Wij geven inzicht in de kwaliteit van ons werk.

versie 1.1.20

Producten

Maatregel M25 : Randvoorwaardelijke producten (M25)

Maatregel 1: Op te leveren producten (M01)

ICTU

ICTU hanteert de volgende documenten, templates en documentstandaarden voor softwarerealisatieprojecten:

- De beschrijving van niet-functionele eisen is gebaseerd op ISO-25010, BIR en SSD, en bevat een prioritering van de niet-functionele eisen. De beschrijving van niet-functionele eisen is gebaseerd op het ICTU NFE-template. De beschrijving bevat in ieder geval eisen aan toegangsbeveiliging, aan beheerfuncties, aan logging en aan het gewenste gedrag van de software bij uitval van infrastructurele diensten zoals een log-server;

- De beschrijving van functionele eisen bestaat uit een geprioriteerde backlog met epics en/of user stories. De beschrijving bevat in ieder geval 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;

- De ontwerp- en architectuurdocumentatie bestaat uit een projectstartarchitectuur (PSA), een softwarearchitectuurdocument (SAD), een infrastructuurarchitectuur (IA), een globaal functioneel ontwerp (GFO) bijvoorbeeld in de vorm van use cases, en een prototype en/of interactieontwerp. De SAD, IA en GFO zijn gebaseerd op de ISR-templates. De

architectuurdocumenten moeten expliciet inzichtelijk maken hoe aan de niet-functionele eisen wordt voldaan door uit te werken welke (beveiligings)mechanieken gekozen zijn, bijvoorbeeld voor identificatie, authenticatie, autorisatie, versleuteling of logging;

- De testdocumentatie bestaat uit een master testplan, gemaakt op basis van een productrisicoanalyse (PRA). Beveiligingstesten zijn een integraal onderdeel van het mastertestplan en worden als zodanig afgestemd met de opdrachtgever;
- Het informatiebeveiligingsplan is gebaseerd op een dreigingen- en kwetsbaarhedenanalyse (TVA, threat and vulnerability assessment) en bevat een maatregelenselectie informatiebeveiliging. De TVA wordt tijdens de voorfase opgesteld op basis van de resultaten van de BIA, de eventuele PIA (zie maatregel M25 Randvoorwaardelijke producten) en inhoud van de ontwerp- en architectuurdocumentatie. Een TVA levert een deel van een traceerbare onderbouwing voor de te treffen beveiligingsmaatregelen.
- Het vrijgaveadvies bevat ten minste alle nog openstaande testbevindingen en geconstateerde beveiligingsbevindingen. Zie ook maatregel M26 Periodieke beoordeling informatiebeveiliging en M16 Verplichte tools. Indien er beveiligingsissues zijn, zijn deze voorzien van een beschreven voorziene impact.
- 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.

Zie Bijlage documenten voor maatregel M1 voor een uitgebreider overzicht van de documenten en documentstandaarden die ICTU hanteert voor softwarerealisatieprojecten.

Het genoemde onderzoek voert ICTU uit als onderdeel van een “due diligence”. Een due diligence wordt uitgevoerd in samenwerking met een potentiële opdrachtgever en biedt, naast het genoemde onderzoek, ook de opdrachtgever de kans zich een oordeel te vormen over de werkwijze van ICTU en de verwachte samenwerking.

Maatregel 2: Continu voldoen aan kwaliteitsnormen (M02)

ICTU

Bij ICTU wordt tijdens de voorfase van softwarerealisatieprojecten het voldoen aan de kwaliteitsnormen met behulp van reviews gecontroleerd. Tijdens de realisatiefase van softwarerealisatieprojecten wordt het voldoen aan de kwaliteitsnormen diverse malen per uur gemeten door het 'Kwaliteitssysteem' (HQ). Het project kijkt dagelijks of er afwijkingen van de normen zijn en onderneemt actie indien nodig. Ook de kwaliteitsmanager signaleert afwijkingen en meldt deze bij het project. De ICTU-specifieke invulling van de kwaliteitsnormen is te vinden in het helpmenu van de geautomatiseerde kwaliteitsrapportages van ICTU.

Maatregel 3: Traceerbaar voldoen aan eisen (M03)

ICTU

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.

Maatregel 4: Geautomatiseerde regressietests (M04)

ICTU

ICTU hanteert een norm voor de dekking van regressietests.

Maatregel 26 : Periodieke beoordeling informatiebeveiliging (M25)

ICTU

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

Indien door de opdrachtgever gewenst kunnen securitytesten door een onafhankelijke derde partij worden uitgevoerd in een daarvoor door de opdrachtgever beschikbaar gestelde omgeving. Dit kan zowel incidenteel als structureel worden ingericht. Afspraken hierover worden bij voorkeur al in de voorbereidingsfase gemaakt.

De beveiligingstesten vinden plaats in aanvulling op de door tools uitgevoerde continue beveiligingsanalyse van de gerealiseerde software, zie maatregel M16 Verplichte tools. Bevindingen uit zowel een beveiligingstest als de continue analyse worden in Jira als issue – gemarkeerd als beveiligingsbugreport – vastgelegd op de backlog van het project.

Processen

Maatregel 5: Iteratief en incrementeel ontwikkelproces (M05)

ICTU

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

- Scrum team bestaand uit product owner, ontwikkelteam en Scrum master,
- Proces: daily scrum, sprints, sprint planning, sprint review, sprint refinement,
- Definition of Done,
- Definition of Ready,
- Product backlog.

Vast onderdeel van de Definition of Done is dat producten actueel en onderling consistent zijn (M01 Op te leveren producten) en voldoen aan de door de projectenorganisatie vastgestelde kwaliteitsnormen (M02 Continu voldoen aan kwaliteitsnormen).

Maatregel 6: Frequente meting (M06)

ICTU

Bij een ICTU-softwareproject is het voldoen aan de normen onderdeel van de 'Definition of Done' en wordt het voldoen aan kwaliteitsnormen meermaals per uur gemeten. Projecten nemen de kwaliteitsrapportage door tijdens de stand-up en tijdens het wekelijks projectoverleg.

Maatregel 7: Continuous delivery pipeline (M07)

ICTU

ICTU gebruikt Jenkins of Team Foundation Server (TFS) als tool voor de implementatie van de continuous delivery pipeline. De ICTU release manager ondersteunt de laatste stap (oplevering van het totale product).

Maatregel 8: Technische schuld (M08)

ICTU

ICTU gebruikt HQ (een door ICTU ontwikkeld, open source, geautomatiseerd kwaliteitssysteem) 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 HQ kan meten.

Maatregel 9: Implementatie kwaliteitsaanpak (M09)

ICTU

Bij ICTU speelt de software delivery manager de rol van projectverantwoordelijke zoals in deze maatregel beschreven. De software delivery manager stemt periodiek de zelf-assessmentresultaten af met het afdelingshoofd ISR.

Maatregel 10: Periodiek projectoverleg (M010)

ICTU

Bij periodiek projectoverleg zijn de software delivery manager, de kwaliteitsmanager en de scrum master vereist.

Maatregel M27 - Projecten expliciet afsluiten (M27)

ICTU

De software delivery manager is verantwoordelijk voor het archiveren. De SDM geeft het projectteam opdracht de archivering voor te bereiden en geeft het technisch beheerteam de opdracht de archivering uit te voeren.

Project Organisatie

Maatregel 11: Beheer en onderhoud kwaliteitsaanpak en -normen (M011)

ICTU

Iedereen die betrokken is bij softwarerealisatieprojecten kan een wijzigingsvoorstel indienen bij het hoofd van de afdeling ICTU Software Realisatie (ISR). Het ISR-coordinatieteam behandelt de wijzigingsvoorstellen en faciliteert besluitvorming door het afdelingshoofd.

Maatregel 24: Implementatie van wijzigingen aan de kwaliteitsaanpak en -normen (M024)

Maatregel 12: Publicatie kwaliteitsaanpak en -normen (M012)

ICTU

De kwaliteitsaanpak is te vinden op de afdelingsbrede wiki. Publicatie van een nieuwe versie wordt aangekondigd via een e-mail naar belanghebbenden en, indien relevant, 'de ICTU Software Realisatie-zeepkist'.
Bij ICTU zijn de kwaliteitsnormen (op dit moment) te vinden in elke kwaliteitsrapportage, in het 'helpmenu'.

Maatregel 13: Dekking ISO-25010 (M013)

ICTU

De kwaliteitsnormen van ICTU voor softwareproducten betreffen de productkwaliteitskenmerken:

- prestatie-efficiëntie
- beveiligbaarheid
- onderhoudbaarheid
- functionele compleetheid (subkarakteristiek van functionele geschiktheid)

Maatregel 14: Projecten splitsen in een voorbereidingsfase en een realisatiefase (M014)

ICTU

Bij ICTU heet de voorbereidingsfase van softwarerealisatieprojecten de 'voorfase'. In de realisatiefase wordt het Scrumteam aangestuurd door een product owner van de opdrachtgever. Bij aanvang van de voorfase is deze beoogde product owner bekend en hij/zij werkt ook mee in de voorfase.

Maatregel 15: Open source tools (M015)

ICTU

Tools die ICTU ontwikkelt ter ondersteuning van softwarerealisatieprojecten, worden bij voorkeur als open source beschikbaar gesteld.

Maatregel 16: Verplichte tools (M016)

ICTU

ICTU gebruikt hiervoor de volgende tools:

1. Jira – De 'eisen' worden, conform Scrumterminologie, geregistreerd als epics en/of user stories, de werkvoorraad als backlog, de iteraties als sprints.

2. Jenkins voor Javaprojecten en Team Foundation Server (TFS) voor DotNet-projecten.
3. SonarQube, inclusief ICTU-specifieke kwaliteitsprofielen die aansluiten bij de ICTU-kwaliteitsnormen.
4. Releasemanager.
5. Reporting (Birt).
6. Kwaliteitsrapportage (HQ).
7. OpenVAS en OWASP ZAP.
8. OWASP Dependency Checker.
9. Checkmarx.

Maatregel 17: Snel beschikbare tools (M017)

ICTU

ICTU gebruikt hiervoor de volgende tools:

1. Docker dashboard
2. MediaWiki
3. Wekan

De tools zijn beschikbaar via een eigen cloud (vergelijkbaar met een 'app store'), binnen een werkdag na aanvraag.

Maatregel 18: Ondersteuning verplichte tools (M018)

Maatregel 19: Digitale werkomgeving (M019)

ICTU

ICTU ondersteunt dit met Docker en/of virtuele machines (VM) en een VLAN per project. Een nieuwe digitale werkomgeving is binnen een werkweek na aanvraag beschikbaar.

Maatregel 21: Kwaliteit van medewerkers (M021)

Maatregel 22: Betrokkenheid bij inzet (M022)

ICTU

Bij het inzetten van medewerkers zijn één of meer ICTU-medewerkers betrokken die ruime ervaring hebben met de ICTU-werkwijze en -kwaliteitsaanpak.

Maatregel 23: Warme kennisoverdracht (M023)