



Kwaliteitsaanpak ICTU Software Realisatie

ISR maatregelen

versie 1.0.2

Producten

Maatregel 1: Op te leveren producten (M01)

ISR

ISR hanteert de volgende documenten, templates en documentstandaarden:

- 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 ISR 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 ISR hanteert.

Het genoemde onderzoek voert ISR 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 ISR en de verwachte samenwerking.

Maatregel 2: Continu voldoen aan kwaliteitsnormen (M02)

ISR

Bij ISR wordt tijdens de voorfase het voldoen aan de kwaliteitsnormen met behulp van reviews gecontroleerd. Tijdens de realisatiefase van projecten wordt het voldoen aan de kwaliteitsnormen diverse malen per uur gemeten door het 'Kwaliteitssysteem'. 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)

ISR

Functionele eisen in de vorm van user stories zijn gekoppeld aan logische testgevallen. Ontwerpdokumentatie in de vorm van use cases is gekoppeld aan logische testgevallen. ISR 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)

ISR

ISR hanteert een norm voor de dekking van regressietests.

Processen

Maatregel 5: Iteratief en incrementeel ontwikkelproces (M05)

ISR

ISR gebruikt hiervoor Scrum, een raamwerk voor productontwikkeling. ISR 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.

Maatregel 6: Frequentie meting (M06)

Maatregel 7: Continuous delivery pipeline (M07)

ISR

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

Maatregel 8: Technische schuld (M08)

ISR

ISR gebruikt het ISR-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 het kwaliteitssysteem kan meten.

Maatregel 9: Implementatie kwaliteitsaanpak (M09)

ISR

Bij ISR 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)

ISR

Bij periodiek projectoverleg zijn de software delivery manager, een vertegenwoordiger uit het kernteam en de scrum master vereist.

Project Organisatie

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

ISR

Iedereen die werkzaam is bij de afdeling kan een wijzigingsvoorstel indienen bij het hoofd van de afdeling. Het ISR-kernteam 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)

ISR

De kwaliteitsaanpak is te vinden op de afdelingsbrede wiki. Publicatie van een nieuwe versie wordt aangekondigd via een afdelingsbrede e-mail en, indien relevant, 'de zeepkist'.

Bij ISR zijn de kwaliteitsnormen (op dit moment) te vinden in elke kwaliteitsrapportage, in het 'helpmenu'.

Maatregel 13: Dekking ISO-25010 (M013)

ISR

De kwaliteitsnormen van ISR betreffen de productkwaliteitskenmerken:

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

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

ISR

Bij ISR heet de voorbereidingsfase de 'voorfase'.

Maatregel 15: Open source tools (M015)

ISR

Tools die ISR ontwikkelt, worden bij voorkeur als open source beschikbaar gesteld.

Maatregel 16: Verplichte tools (M016)

ISR

ISR gebruikt hiervoor de volgende tools:

- a) Jira – De 'eisen' worden, conform Scrumterminologie, geregistreerd als epics en/of user stories, de werkvoorraad als backlog, de iteraties als sprints.
- b) Jenkins voor Javaprojecten en Team Foundation Server (TFS) voor DotNet-projecten.
- c) SonarQube, inclusief ICTU-specifieke kwaliteitsprofielen die aansluiten bij de ICTU-kwaliteitsnormen.
- d) Releasemanager.
- e) Reporting (Birt).
- f) Kwaliteitsrapportage (HQ).

Maatregel 17: Snel beschikbare tools (M017)

ISR

ISR gebruikt hiervoor de volgende tools:

- a) Docker dashboard
- b) MediaWiki
- c) 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)

ISR

ISR 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)

ISR

Bij het inzetten van medewerkers zijn Ã©Ã©n of meer leden van het ISR-kernteam betrokken.

Maatregel 23: Warme kennisoverdracht (M023)