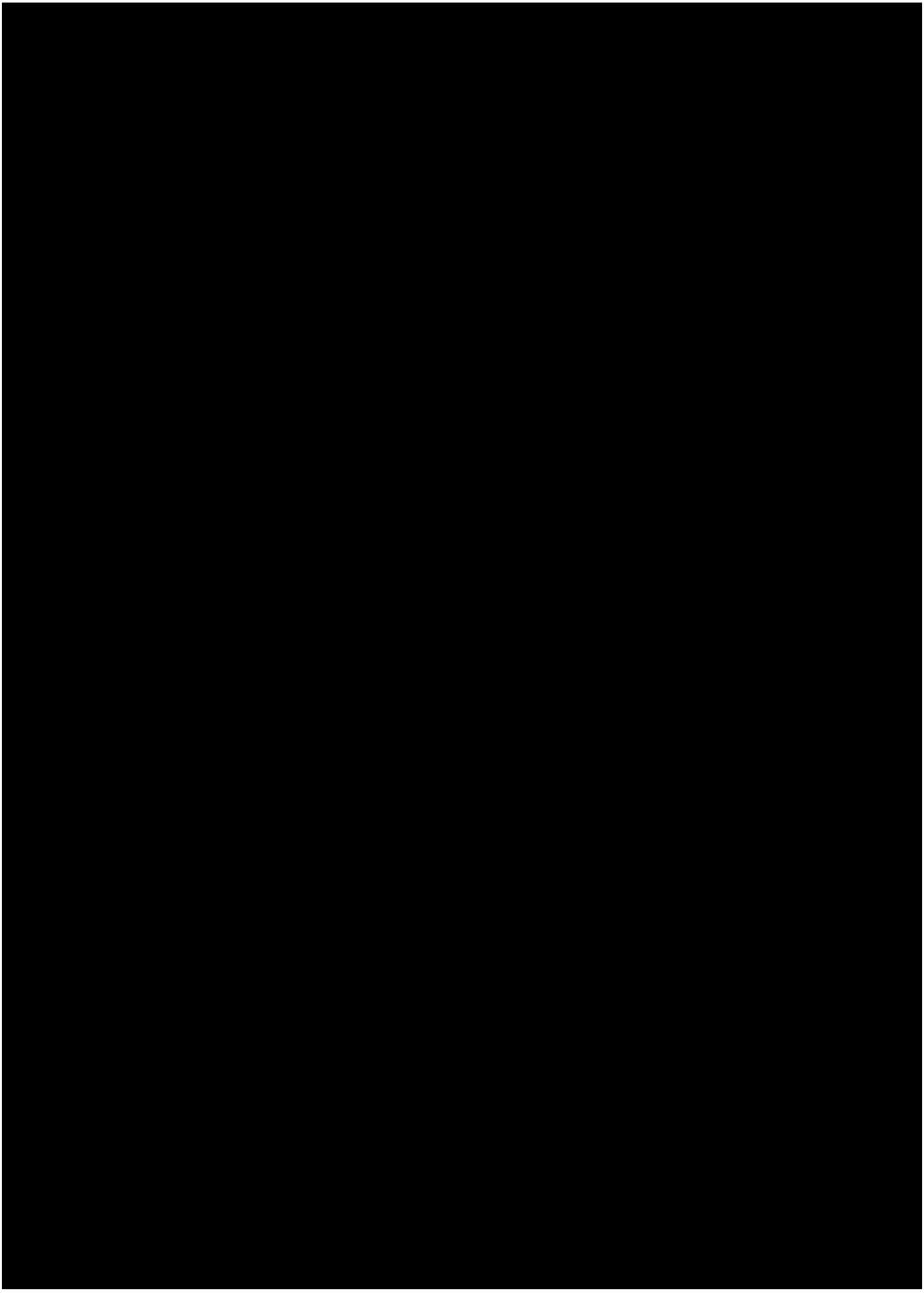


documentatieen architectuurstudie, crystalbox security audits (broncodescan) en penetratieaudits beoordelen deze experts of de software voldoet aan de projectspecifieke niet-functionele eisen die met betrekking tot beveiliging aan de software zijn gesteld, of bekende kwetsbaarheden (OWASP) vermeden zijn 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.

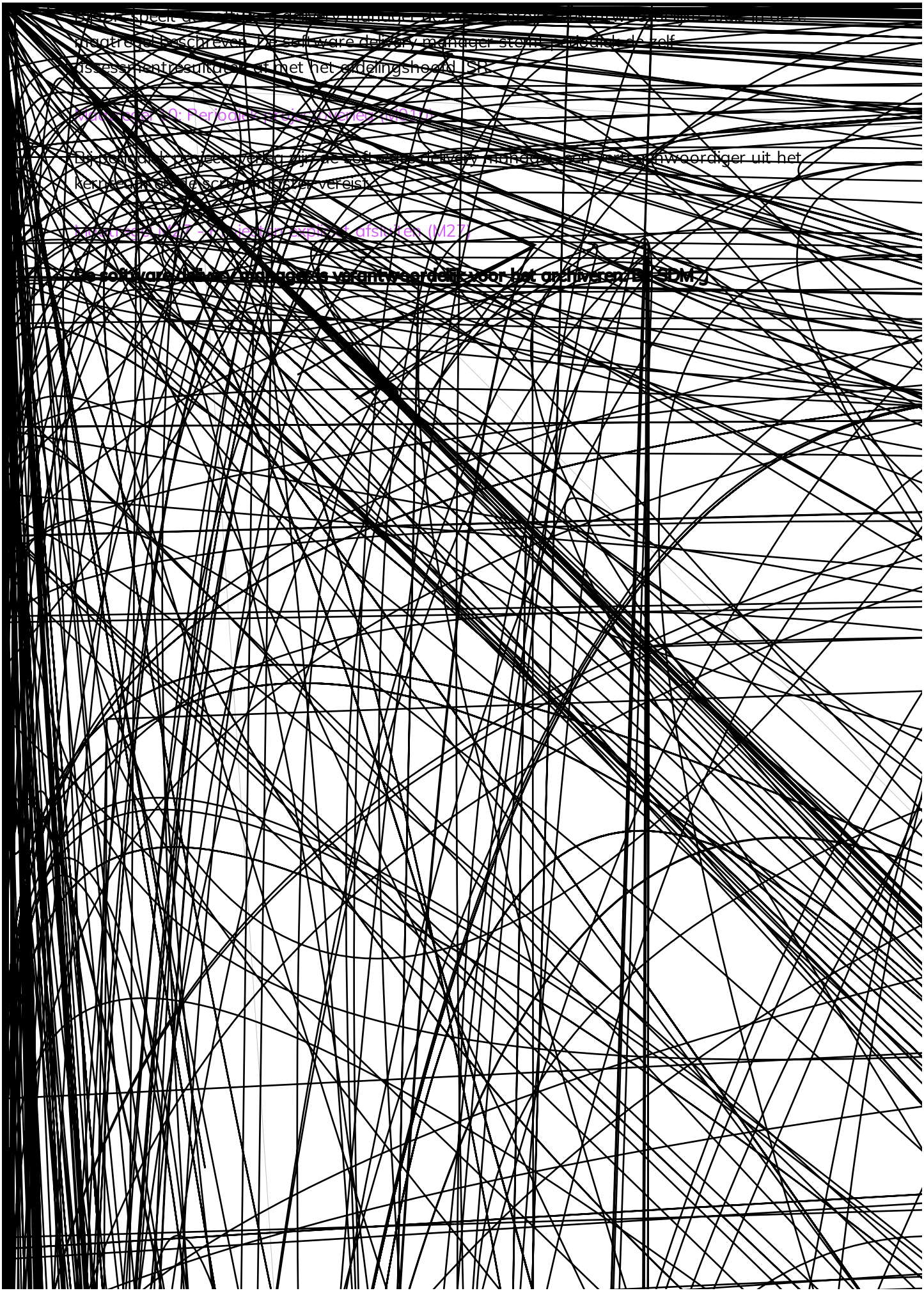
Processen

Maatregel 5: Iteratief en incrementeel ontwikkelproces (M05)

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.

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).



ISR 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)

ISR 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)

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)

Bij het inzetten van medewerkers zijn één of meer leden van het ISR-kernteam betrokken.

Maatregel 23: Warme kennisoverdracht (M023)