

Bijlage B Business requirements (Concept Programma van Eisen en Wensen)

Business requirements

Wij zijn op zoek naar een standaardoplossing die met alleen configuratie (dus zonder of met minimale maatwerkontwikkeling) in ons systeemlandschap kan worden opgenomen.

Dit document bevat de business requirements die aan de Toetsmodule worden gesteld.

Functioneel

1. Gebruik van toetsen door systeem RADAR

- 1.1. De Toetsmodule heeft een 'service' om alle toetsen met een niet-ontwikkel status te selecteren.
 - Toelichting: In RADAR wordt vastgelegd op welke wijze een signaal van de KvK moet worden uitgevoerd. Een onderdeel hiervan is het koppelen van de toets waarmee de beoordeling moet plaats vinden. Hiervoor is het nodig om in RADAR de toets uit een lijst te selecteren.
- 1.2. De Toetsmodule heeft een 'service' die door systeem RADAR kan worden aangeroepen voor het uitvoeren van de toets. De vraag bevat de unieke identificatie van de toets en de unieke identificatie van de analyse. Het antwoord bevat het toetsresultaat en alle aanvullende gegevens.

2. Structuur van een toets

- 2.1. De toets in de Toetsmodule moet eenvoudig en flexibel instelbaar zijn afhankelijk van maatschappelijke behoefte en ontwikkelingen.
 - Toelichting: Dit betekent dat het niet nodig is om systeemontwikkeling in te schakelen bij het in productie brengen van een nieuwe toets. Alle taken moeten gedaan kunnen worden door de profielontwikkelaar en functioneel beheerders.
- 2.2. Een toets bevat één of meer profielen. Op ieder profiel wordt een score bepaald op basis van de samenstellende indicatoren.
- 2.3. Een profiel is samengesteld uit één of meer indicatoren, waarbij iedere indicator een eigen (relatief) gewicht in het profiel heeft. Het gewicht heeft een waarde van 0 of hoger.
- 2.4. Op ieder profiel kan een drempelwaarde worden ingesteld. Bij overschrijding van de drempelwaarde wordt er op het profiel gescoord.
 - Toelichting: Als er op een profiel wordt gescoord, dan is dat voor RADAR aanleiding om een TRM te maken.
- 2.5. Een indicator wordt toegepast op één of meer subjecten bij de analyse, waarbij de categorieën subjecten instelbaar zijn. Het subject met de hoogste indicatorscore bepaalt de score op de indicator voor de analyse.
 - Toelichting: categorie van subjecten is bijvoorbeeld 'alle natuurlijke personen in het functionarisnetwerk'.
- 2.6. Een indicator die wordt uitgevoerd voor een specifiek subject in de analyse is een waarde die bepaald wordt op basis van een selectie van gegevens van het subject of gegevens gerelateerd aan het subject. De waarde van de score is een getal van 0 of hoger.
 - Toelichting: Bij deze selectie kan bijvoorbeeld gebruik worden gemaakt van criminele antecedenten of financiële antecedenten, of het JDS-antwoord voor die persoon.
 - Toelichting: I.h.a. bestaat een indicator uit een lijst met businessregels, waaraan een scorewaarde wordt toegekend. De businessregel met de hoogste score die voldoet, is bepalend voor de indicatorscore.

- 2.7. Op iedere indicator kan een drempelwaarde worden ingesteld. Als een subject een indicatorscore boven de drempelwaarde heeft, dan is dat subject relevant voor die indicator.
- 2.8. Als op een profiel wordt gescoord, dan kan voor alle subjecten die relevant zijn voor de indicatoren in dat profiel, een selectie worden gedaan van aanvullende gegevens, dat wordt gevoegd bij het toetsresultaat.
- Toelichting: Bijvoorbeeld een profiel die indicatoren heeft voor de branche (SBI-code) van de 'primaire rechtspersoon' en de wetsartikelcodes van de 'natuurlijk persoon functionarissen'.
Als de indicatoren scoren op SBI-code en wetsartikelcode, en er is ook een score op het profiel, dan moet in de aanvullende gegevens o.a. zichtbaar zijn:
 - Alle relevante SBI-codes van de primaire rechtspersoon.
 - Het subject (NP functionaris), de wetsartikelcode en de zaak op het strafblad.Deze gegevens zijn nodig om de handmatige beoordeling van de TRM efficiënt uit te kunnen voeren.

3. Gebruik van brongegevens t.b.v. de toets

- 3.1. De Toetsmodule kan meerdere SQL-databases gebruiken voor selectie van de gegevens t.b.v. het uitvoeren van de toets.
- Toelichting: De Toetsmodule moet gebruik kunnen maken van de gestructureerde gegevens in de database van systeem RADAR en de lokale kopie van het Handelsregister.
- 3.2. Op basis van een unieke identificatie van een analyse in RADAR kunnen alle relevante gegevens t.b.v. de toets worden geselecteerd.
- Toelichting: In RADAR heeft iedere analyse een unieke technische identificatie. Alle gegevens zijn direct of indirect aan deze unieke identificatie gerelateerd.
- 3.3. De gegevens t.b.v. een toets kunnen ook in de vorm van een xml-bericht in een database veld zijn geplaatst. Hierbij moet in principe ieder veld in het xml-bericht kunnen worden gebruikt bij het bepalen van de waarde van de indicator.
- Toelichting: Dit is o.a. het geval voor de gegevens van een strafblad, waarbij het JDS-antwoord in de vorm van een xml-bericht (met een bekende structuur) staat in een databaseveld.

4. Gebruik van referentietabellen t.b.v. de toets

- 4.1. Bij de bepalen van de score van een indicator kan gebruik worden gemaakt van referentietabellen in de Toetsmodule.
- 4.2. Bij de bepalen van de score van een indicator kan gebruik worden gemaakt van referentietabellen in de database van systeem RADAR.
- 4.3. In de Toetsmodule zijn de referentietabellen voor ontwikkel- en testfase gescheiden van productie.
- Toelichting: De werking van een toets is afhankelijk van de vulling van de referentietabellen. Het beheer daarvan moet in de productieomgeving daarom vallen onder Functioneel Beheer. Tijdens de ontwikkeling van de toetsen vallen de referentietabellen onder de verantwoordelijkheid van de profielontwikkelaar. Bij het opleveren van een nieuwe toets naar productie hoort dan ook het opleveren van de nieuwe of gewijzigde referentietabellen.
 - Toelichting: Met Alert! wordt dit gedaan door de ontwikkeling te doen in de 'Alert! simulatieomgeving', die volledig gescheiden is van de 'Alert! productieomgeving'. Bij de inproductie van een toets wordt een export uit de simulatieomgeving geïmporteerd in de productieomgeving.

5. Overige aanvullende gegevens

- 5.1. Alle gegevens die behoren tot de specifieke analyse in RADAR die wordt getoetst, kunnen worden gebruikt voor de selectie van aanvullende gegevens, en worden gevoegd bij het toetsresultaat.

Toelichting: De aanvullende gegevens geven de medewerkers inzicht in bijvoorbeeld de wetsartikelen en straffen die voorkomen op de strafbladen van natuurlijke personen.

5.2. Van een specifieke analyse in RADAR die wordt getoetst, is het mogelijk om de dossiers te bepalen die hieraan gerelateerd zijn.

- Toelichting: De relatie tussen de analyses in RADAR wordt gelegd op basis van de natuurlijke personen die aanwezig zijn in de te toetsen analyse en reeds aanwezige dossiers in systeem RADAR. Dit geeft de medewerker inzicht in gerelateerde dossiers en risicomeldingen.

6. Ontwikkeling van toetsen

6.1. De toetsmodule biedt de functionaliteit om toetsen te ontwikkelen, te testen, te accepteren en in productie te nemen. De toetsmodule moet deze fasering in de ontwikkeling van toetsen ondersteunen.

6.2. Een toets met een test-, acceptatie- of productiestatus kan niet worden gewijzigd. Alleen toetsen met een ontwikkelstatus kunnen worden gewijzigd.

6.3. Een nieuwe toets kan vanaf het begin af aan worden opgebouwd, maar ook kan een bestaande toets als startpunt dienen voor de ontwikkeling van een nieuwe toets.

- Toelichting: De ontwikkeling van toetsen is in het algemeen een iteratief proces, met telkens kleine aanvullingen en verbeteringen. Het is dan noodzakelijk om een eerdere toets als startpunt te kunnen nemen.

6.4. De Toetsmodule bevat een verzameling toetsen, die elk onafhankelijk van elkaar zijn.

- Toelichting: De werking van de ene toets staat volledig los van de werking van een andere toets die aanwezig is in dezelfde omgeving. Er kan wel gebruik worden gemaakt van dezelfde referentietabellen.

Niet-functioneel

7. Performance

7.1. Het beoogd volume aan risicobeoordelingen bedraagt maximaal 5000 per uur.

7.2. De risicobeoordeling module is horizontaal schaalbaar. De webservice is bij voorkeur multi-threaded opgezet en het maximum aantal threads is bij voorkeur instelbaar (middels een threadpool).

7.3. Performance criteria:

- De maximale responsetijd van de service bedraagt 3 seconde.
- Minimaal 95% van de aanroepen dient binnen 1.5 seconde afgehandeld te worden.
- De responsetijden betreffen de verwerkingstijden binnen de servicelaag en niet de aanroep vanuit het integratieproces.
- Deze responsetijden dienen ook behaald te worden in situaties waarin de CPU-belasting van de betreffende servers tot 80% is opgelopen (en deze CPU-belasting veroorzaakt wordt door dezelfde service, niet door achtergrondprocessen).
- Bij voorkeur worden service-aanroepen onderbroken als de verwerking een drempelwaarde van een doorlooptijd overschrijdt en worden de betreffende resources vrijgegeven en de problemen gelogd.
- Het geheugengebruik van de servicecomponent is stabiel.

7.4. Uitgangspunten voor de performance criteria:

- De maximale omvang van een input bericht bedraagt 5 Mb.
- De variantie van de omvang van berichten is relatief klein.
- De hoeveelheid aanroepen per tijdseenheid kan enigszins worden gedoseerd.
- Voor het testen van de performance wordt gebruik gemaakt van gegevens die de werkelijkheid (productiegegevens) adequaat nabootsen.

8. Capaciteit

8.1. Op dit moment worden de toetsen, getriggerd door relevante gebeurtenissen, gemiddeld ongeveer 1500 keer per dag uitgevoerd. De Toetsmodule moet per dag minimaal 5x dit aantal aan kunnen.

- 8.2. De input van een toets betreft een netwerk van 1-6000 personen (met een gemiddelde van 100 personen, waarvan er gemiddeld 10 een natuurlijke persoon zijn).
- 8.3. De hoeveelheid data die in xml-format aan de toetsmodule wordt aangeboden is maximaal 5 Mb groot.

Architectureel

Risicobeoordelingsmodule

9. Afbakening

- 9.1. Met de risicobeoordeling module wordt de functionele component bedoeld die geautomatiseerd, zonder tussenkomst van gebruikers, profielen toepast op aangeleverde gestructureerde risico dossiers. Centraal daarin staat het profiel dat toegepast wordt om de risico's af te leiden. De module produceert een hit-/no hit indicator en geeft de onderbouwing voor de afleiding daarvan mee in het antwoord.

10. Vormgeving

- 10.1. De risicobeoordelingsmodule dient als webservice geïmplementeerd te zijn en bij voorkeur gehost te worden binnen Microsoft Internet Information Services om compliant te zijn met het applicatielandschap.
- 10.2. De aanroepen van de webservice zijn stateless.

11. Transparantie

- 11.1. De risicobeoordelingsmodule implementeert logging-functionaliteit en ondersteunt de toepassing van loglevels.
- 11.2. De webservice produceert gestandaardiseerde foutafhandelingsberichten in het geval van technische problemen. Deze berichten worden gelogd of zijn herleidbaar.
- 11.3. De risicobeoordelingsmodule biedt functionaliteit voor het detecteren van onregelmatigheden, zowel in de productie omgeving als in de ontwikkel-, test- en acceptatie-omgeving. Deze auditinformatie is beschikbaar via een grafische user interface.
- 11.4. Indien de afhandeling van de service niet gerapporteerd kan worden (bijvoorbeeld doordat een daartoe benodigde database transactie faalt), dan wordt er een foutbericht retour gezonden, ook indien de afleiding gelukt is. Een niet navolgbare toets heeft geen inhoudelijke betekenis.

12. Servicedefinitie

- 12.1. De oplossing genereert automatisch WSDL-bestanden die gebruikt kunnen worden om de service aan te roepen.
- 12.2. Het streven is om in de servicedefinitie, tegen de gewoonte in, geen restricties of controles op te leggen aan de meegezonden inhoudelijke criteria. Een wijziging in de beoordelingscriteria vereist daarmee geen wijziging van de aanroepende integratieprocedures.
- 12.3. De gevraagde functionaliteit wordt daarmee altijd aangeroepen via één specifieke functie waarbij de profielinformatie wordt meegezonden in het request bericht.
- 12.4. Wijzigingen in de afleidingen leiden bij voorkeur niet tot wijzigingen in de service definities.

13. Gebruik

- 13.1. Alle relevante inputgegevens worden opgenomen in het request bericht. Daarmee hoeft binnen de service geen aanvullende informatie verzameld te worden. Er is geen mogelijkheid tot een dialoog: er kan aan de aanroepende software geen aanvulling van gegevens verzocht worden.
- 13.2. Er is slechts één aanroep (request) en één antwoord (response) vereist om de volledige risicobeoordeling uit te voeren, ook als intern de resultaten in meerdere stappen verkregen worden.
- 13.3. De onderbouwing van de risicobeoordeling is direct en integraal afleidbaar uit het responsebericht van de service.

- 13.4. Het is bij voorkeur mogelijk om meerdere versies van een risicobeoordelingsmodel naast elkaar te hosten in één omgeving en los van elkaar aan te roepen (via verschillende URL's).
- 13.5. Het systeem garandeert dat voor de periode dat de service aanroepbaar is, alle instanties welke op alle betrokken servers geïnstalleerd zijn, identiek geconfigureerd zijn en aanroepen met gelijke gegevens ook tot identieke resultaten leiden, onafhankelijk van de specifieke instantie van de service waardoor ze afgehandeld zijn.

14. Herbruikbaarheid

- 14.1. Indien Justis op een later moment deze service wenst toe te passen binnen andere producten of procedures, dan:
- Kunnen de verschillende toepassingen binnen één omgeving onafhankelijk van elkaar gehost worden.
 - Hebben de verschillende toepassingen eigen lifecycles.
 - Delen de verschillende toepassingen alle aanpalende functionaliteit als logging en monitoring.
 - Kan de omgeving (capaciteit) daartoe eenvoudig, bij voorkeur zonder onderbreking van de dienstverlening, uitgebreid worden.

Profielstudio

15. Afbakening

- 15.1. Met de profielstudio wordt een (web)applicatie bedoeld waarmee profielen geconfigureerd en getest kunnen worden. Wanneer de profielen goed bevonden zijn, worden zij gepubliceerd naar de risicobeoordeling module (webservice).
- 15.2. De profielstudio kan mogelijk bestaan uit meerdere, losse modules waarmee de functionaliteit opgesplitst wordt (bijvoorbeeld in ontwikkeling, beheer en test).

16. Platform

- 16.1. De profielstudio is bij voorkeur geïmplementeerd als webapplicatie óf als MS Windows-applicatie. De onderliggende configuratie gegevens worden centraal opgeslagen en kunnen door meerdere gebruikers tegelijkertijd aangepast worden. Daarbij voorziet het systeem in versiebeheer.
- 16.2. De profielstudio wordt lokaal (on premise), dus niet in de cloud, gehost.

17. Koppelingen

- 17.1. De profielstudio is in staat te koppelen naar zowel databases als webservices voor het inlezen / ophalen van testgegevens. Voor deze koppelingen wordt gebruik gemaakt van standaard technologieën.

18. Ontwikkeling

- 18.1. De ontwikkeling en aanpassing van toetsmechanismen / profielen vergt geen software ontwikkeling, scripting, of anderszins diepe technische kennis.
- 18.2. Medewerkers die profielen ontwikkelen hoeven zich niet te bekommeren over de performance-eigenschappen die voortvloeien uit de betreffende configuratie van de profielen.
- 18.3. De profielstudio is bij voorkeur in staat om geautomatiseerd rapportages over de configuratie te genereren welke als documentatie beheerd kunnen worden.
- 18.4. De ontwikkelde modellen / profielen dienen dusdanig helder te zijn dat personen die niet ingewijd zijn in de software, ze eenduidig kunnen begrijpen in verband met mogelijk audits op de inhoud van de profielen.

19. Test en acceptatie

- 19.1. Het systeem voorziet in functionaliteit voor het uitvoeren van testen in de test- en acceptatiefase. Daarbij moeten individuele testgevallen uit bronnen geselecteerd (en aangepast) kunnen worden of handmatig samengesteld kunnen worden.

- 19.2. Bovendien moeten bulktesten op geselecteerde bronbestanden uitgevoerd en gevalideerd kunnen worden. De resultaten van deze testen dienen vanuit meerdere perspectieven onderzocht te kunnen worden, waarbij de onderbouwingen voor de uitkomsten onderzocht moeten kunnen worden.
- 19.3. Bulktesten kunnen als background processen opgestart worden, zodat ze het interactief gebruik van de profielstudio niet blokkeren. De voortgang ervan kan vanuit de profiel studio gemonitord worden.
- 19.4. Problemen die in productie ontstaan, kunnen eenvoudig binnen de testomgeving onderzocht worden aan de hand van bijbehorende request- en response berichten.
- 19.5. De inhoudelijke afhandeling van testgevallen in de test- en acceptatie-omgeving is gegarandeerd 100% identiek aan die in de productie-omgeving.

20. Herbruikbaarheid

- 20.1. Om te borgen dat de profielstudio ook voor andere producten / processen binnen Justis ingezet kan worden, voorziet de profielstudio in een projectstructuur die het mogelijk maakt om die toepassingen binnen de applicatie te scheiden.

21. Toekomstige ontwikkelingen

- 21.1. De profielstudio biedt naast de gevraagde toets mechanismen ook alternatieve algoritmes waarmee in de toekomst de toetsing verrijkt kan worden. Graag aangeven welke mechanismen dit betreft en tot welke verbetering dit kan leiden.

Beheersmatig

22. Gebruikersautorisatie

- 22.1. Alleen geautoriseerde personen hebben toegang tot de Toetsmodule voor het ontwikkelen van toetsen. De Toetsmodule maakt voor de autorisatie gebruik van de 'AD' bij Justis.

23. Beveiligde inlogprocedures

- 23.1. Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
- 23.2. Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.
- 23.3. Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.

24. Systeem voor wachtwoordbeheer

- 24.1. Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
- 24.2. Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.
- 24.3. In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1).
- 24.4. De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.
- 24.5. Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.
- 24.6. Wachtwoorden die voldoen aan het wachtwoordbeleid, hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van zes maanden.

25. Usability

- 25.1. Er zijn gebruikers- en beheerhandleidingen beschikbaar.

26. Security

- 26.1. Het is mogelijk om door Beheer of de leverancier de rechten en rollen af te schermen voor onbevoegden.
- 26.2. Er is vanuit de applicatie een overzicht beschikbaar met alle actieve gebruikers, met de toegekende rollen en rechten.
- 26.3. De applicatie is voorzien van een audit trail t.b.v. audit controles.
- 26.4. De applicatie voldoet aan het wachtwoordbeleid.

27. Maintainability

- 27.1. Er is een duidelijke beleid omtrent ALM en de releasekalender. Functioneel beheer kan middels een RFC/user story wijzigingen aanvragen op de applicatie.

28. Portability

- 28.1. De applicatie ondersteunt de gewenste internetbrowser (Edge) en/of is te benaderen via het startmenu.