

Continuïteit in de risicoanalyse

Hoe beoordeel je de levensvatbaarheid van jouw klant

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Systems Engineering Management Plan
Continuïteitsapp

Oktober 2026

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Nederland rekent op zijn accountants.

De leden van de Koninklijke NBA vormen een brede, pluriforme beroepsgroep van ruim 22.000 professionals werkzaam in de brede accountantspraktijk, bij de overheid, als intern accountant en in het management van organisaties. Integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, vertrouwelijkheid en professionaliteit zijn essentiële beginselen voor iedere accountant. De Koninklijke NBA helpt accountants hun cruciale rol in de maatschappij te vervullen, nu en in de toekomst.

© 2026 Koninklijke NBA
Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij door middel van druk, fotokopieën, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van de NBA.

Colofon

De Taskforce Continuïteit van NBA Accounttech heeft het thema Continuïteit in de risicoanalyse, hoe beoordeel je de levensvatbaarheid van jouw klant uitgewerkt. De uitwerking leverde drie handleidingen op: de Handleiding Continuïteitsapp voor de Cliënt van de Accountant, de Handleiding Continuïteitsapp voor de Accountant en de Handleiding Systems Engineering Management Plan Continuïteitsapp.

Kerngroep NBA Accounttech: Prof. dr. Joost van Buuren RA (voorzitter), Age Lammers (programmamanager NBA Accounttech), Drs. Marcel Bongers RE RA CIA CISA CFE CBM, Dr. Eric Mantelaers RA AA CFE CISA C|CISO, Drs. Vincent Wanders RA.

NBA Accounttech richt zich op het bevorderen van innovatie en digitalisering binnen alle werkvelden van accountants. Accounttech biedt de beroepsgroep oplossingen die de kwaliteit van het werk verbeteren, het beroep aantrekkelijker maken en de efficiëntie verhogen.

Deze publicatie is een samenwerking tussen diverse professionals:

NBA Accounttech Taskforce Continuïteit: Prof. dr. Joost van Buuren RA (voorzitter), Drs. Arjaan van den Berg, Mr. drs. Paul van Dam RV, Drs. Han Dieperink, MMAV Melissa Klaver-Drost RA, Dr. Robert Los, Drs. Vincent Wanders RA, Jan Wietsma AA en Age Lammers (programmamanager NBA Accounttech).

Disclaimer:

De continuïteitsapp is uitsluitend bedoeld als voorbeeld van ondersteunend hulpmiddel en vervangt niet de professionele oordeelsvorming, eigen verantwoordelijkheid of toepasselijke werkzaamheden van de gebruiker. De Nederlandse Beroepsorganisatie van Accountants (NBA) en Nyenrode Business Universiteit geven geen garantie over de juistheid, volledigheid, geschiktheid of uitkomsten van de app en zijn, voor zover wettelijk toegestaan, niet aansprakelijk voor enige directe of indirecte schade die ontstaat door of verband houdt met het gebruik van de continuïteitsapp of het vertrouwen op de uitkomsten daarvan. De gebruiker blijft zelf verantwoordelijk voor de toepassing, interpretatie, verificatie en vastlegging van de resultaten.

Inhoud

Colofon 3
1. Inleiding en doel 5
2. Projectgegevens en uitgangspunten 5
2.1 Basis Projectgegevens 5
2.2 Uitgangspunten 5
3. Inventarisatie vereisten belanghebbenden 6
3.1 Vaststelling behoeften van belanghebbenden 6
3.2 Vereisten Externe Gebruikers (Assurance-gebruikers) 8
3.3 Vereisten Interne Gebruikers (Accountantskantoren) 8
3.4 Vereisten Bedrijfsvoering 9
3.5 Vereisten voor regelgeving en maatschappij 9
4. Technische vereisten definitie 10
4.1 Functionele vereisten 10
4.2 Niet-functionele vereisten 10
5. Ontwerpoplossing 11
5.1 Overwogen Alternatieven 11
5.2 Theoretische werking voorkeursoplossing 11
6. Architectuur 13
6.1 Functionele Architectuur 13
6.2 Work Breakdown Structure 13
7. Implementatiestrategie 14
7.1 Implementatiestrategie per Fase 14
8. Verificatie en validatie 14
9. Operationsplan en risicomanagement 15
9.1 Identificatie en beoordeling kritieke risico's voor voortgang project 15
9.2 Risicoanalyse beheer van app 16
9.3 Communicatiestrategie 20
9.4 Benodigde documentatie 20
10. Configuratie- & versiebeheer 20
10.1 Configuratiemanagementstrategie 20
10.2 Change Control (opzet) 21
10.3 Versiebeheer 21
10.4 Bewerkers- en overige overeenkomsten 21
10.5 Openstaande punten 21
11. Bijlagen 21
12. Referenties 21
Bijlage afkortingen 23

1. Inleiding en doel

Dit Systems Engineering Management Plan (SEMP) beschrijft hoe de Taskforce Continuïteit van Accounttech het innovatieproject voor een open-source continuïteitsbeoordeling-applicatie zal aansturen volgens de principes van systems engineering, zoals toegepast volgens het raamwerk van Van Buuren en Wijma (2022).

2. Projectgegevens en uitgangspunten

2.1 Basis Projectgegevens

Tabel 1
Projectgegevens

Kenmerk	Omschrijving
Projectnaam	Taskforce Continuïteit - Applicatie voor Continuïteitsbeoordeling
Opdrachtgever	MT NBA (via Age Lammers, NBA)
Projectleider	Joost van Buuren (Nyenrode) en Arjaan van de Berg (product owner)
Startdatum	November 2025
Einddatum Fase 1	30 oktober 2026
Doelgroep primair	Reguliere vergunninghouders en mkb-accountantskantoren
Projecttype	Proof-of-Concept / MVP-ontwikkeling

2.2 Uitgangspunten

Volgens Van Buuren en Wijma (2022) zijn schaalbaarheidskeuzes kritisch voor effectieve innovatiegovernance. Voor deze Taskforce gelden de volgende criteria:

- Organisatorische schaal: Klein, interdisciplinair team (NBA, universitaire omgeving met externe programmeur)
- Complexiteit: Middel (integratie van rode vlaggen NBA in applicatie-logica; datamodel, hosting, validatie)
- Risico-profiel: Laag tot middel (open-source COTS-benadering, beperkte Minimal Viable Product (MVP)-scope, Nederlandse hosting/AVG-compliantie kritisch) – disclaimer NBA en Nyenrode aanvaarden geen aansprakelijkheid voor functioneren: het is een een MVP.
- Maturity-doelstelling: MVP met validatie en reproduceerbare methode

Consequenties voor SEMP:

- Vereenvoudigde documentatie (beperkt tot kritische onderdelen per Van Buuren en Wijma-model)
- Integratie van vier vereisten-kwadrant-groepen (externe gebruikers, interne gebruikers, bedrijfsvoering, regelgeving)
- Focus op iteratieve validatie eerder dan formele milestone-gates
- Participatief ontwerp met stakeholders (NBA Werkgroep Continuïteit, pilotdeelnemers).

3. Inventarisatie vereisten belanghebbenden

3.1 Vaststelling behoeften van belanghebbenden

De Taskforce heeft de volgende primaire belanghebbenden geïdentificeerd:

Tabel 2
Belanghebbenden, behoeften en rollen

Belanghebbende	Type	Behoefte	Rol in project
MT NBA/kerngroep Accounttech (Interne gebruiker)	Opdrachtgever	Verbetering controlekwaliteit continuïteitsbeoordelingen	Strategische goedkeuring, budgetbesluit
Accountants (vergunninghouders) (Interne gebruiker)	Primaire gebruikers	Ondersteuning bij oplossen van door AFM (2025, p. 5) geconstateerde tekortkomingen bij de beoordeling van continuïteit: • Ondersteuning bij identificatie van rode vlaggen en documentatie. Signalen van continuïteitsproblemen worden nu niet altijd tijdig, volledig en samenhangend herkend of vastgelegd, mede door gebrek aan holistisch cliëntinzicht en focus op afvinkwerk. • Verbreding van tijdshorizon tot 2–3 jaar. Beoordelingen zijn vaak te sterk gericht op de korte termijn, terwijl risico's voor continuïteit juist ontstaan door toekomstige ontwikkelingen, scenario's en externe schokken. • Versterking PKI. Accountants kunnen te dicht op de cliënt zitten of managementaannames te weinig kritisch toetsen, waardoor confirmation bias kan ontstaan en tegenbewijs onvoldoende gewicht krijgt. • Accountant als strategisch gesprekspartner. Het gesprek over continuïteit is te weinig geïntegreerd, vooruitkijkend en multidisciplinair, terwijl juist tijdige duiding, escalatie en consultatie cruciaal zijn.	Functionele vereisten definiëren
Nyenrode Universiteit	Wetenschappelijke partner	Methodische betrouwbaarheid, validatie-legitimiteit	Theoretisering en Validatieonderzoek uitvoeren
NBA Taskforce Continuïteit	Methodologische partner	Afstemming rode vlaggen-handreiking, kennisbasis	Inhoudelijke governance
Robert Los (implementatiepartner)	Technische uitvoerder	Heldere specificaties, werkbare omgeving, ondersteunde architectuur	Technische realisatie

Belanghebbende	Type	Behoefte	Rol in project
Pilotdeelnemers	Testgebruikers	Praktische bruikbaarheid, feedback-mogelijkheden	Validatiedata
Accounttech community	Ecosysteem-partner	Open-source beschikbaarheid, onderhoudbaarheid	Adoptie en verspreiding
Bestuurders/CFO's ondernemingen (externe belanghebbende)	Secundaire gebruikers	Inzage continuïteitsrisico's, transparantie	Informatie-ontvangers
Banken/financiële instellingen (externe belanghebbende)	Secundaire gebruikers	Vroegsignalering van niet naleven-convenanten	Cliënt motiveren contact op te nemen met bank
Belastingdienst (externe belanghebbende)	Secundaire gebruikers	Signalering problemen levensvatbaarheidstoets	Cliënt motiveren contact op te nemen met Belastingdienst

3.2 Vereisten Externe Gebruikers (Assurance-gebruikers)

Definitie controlekwaliteit (Van Buuren en Wijma, 2022, p. 21):
"De kwaliteit van een assurance-opdracht is de mate waarin voldoende en geschikte assurance-informatie is verkregen om een conclusie tot uitdrukking te brengen om de mate van vertrouwen van beoogde gebruikers (niet zijnde de verantwoordelijke partij) in de uitkomst van de meting of evaluatie van het onderzoeksobject ten opzichte van criteria zo veel mogelijk te versterken."

Specifieke vereisten:

1. Toegevoegde waarde
    - Verkleining verwachtingskloof (accountant-bedrijf-stakeholders)
    - Vroege risicodetectie (horizon twee tot drie jaar)
    - Versterking poortwachtersfunctie
    - Versterking strategisch gesprekspartnerschap accountants met bedrijf

3.3 Vereisten Interne Gebruikers (Accountantskantoren)

1. Functioneel
    - Systematische effectieve en efficiënte identificatie van de rode vlaggen (NBA, 2023):
        - nauwkeurige identificatie van risico's (acceptabel aantal type I-fouten)
        - volledige identificatie van relevante risico's (acceptabel risico op type 2 fout)
        - tijdigheid van identificatie rode vlaggen, dus vlaggen geven aanleiding vroegtijdig het goede gesprek te voeren met het management van de controlecliënt
        - werking en gebruik van de methode is te verantwoorden door accountants en uitlegbaar naar interne en externe toezichthouders
    - Scenarioanalyses voor levensvatbaarheid (twee tot drie jaar horizon)
    - Structurering van rode vlaggen als symptomen van onderliggende oorzaken (NV COS 315)
    - Vragenlijst ca. 100 vragen met intuïtieve navigatie
    - Ondersteuning van NV COS 315, NV COS 570 en NV COS 4410
    - Integratie/aansluiting met NBA AuditWorkBook (NBA, 2024)
    - Exportmogelijkheden naar veelgebruikte audittools
    - Gebruiksvriendelijke werkwijze
    - Input vanuit gesprekken kunnen gebruiken, bijvoorbeeld bedrijfsverkenning.
    - Relevante, bondige en betrouwbare output
2. Gebruikerservaring
    - Webinterface (responsive design)
    - Nederlandse taal
    - Time-to-complete: realistische duur voor mkb-praktijk
    - Output: downloadbare antwoorden van vragenlijst en indicatoren
3. Technisch
    - Adequate toegangsbeveiliging/cybersecurity-proof
    - Prestatie: responstijd <3 seconden per vraag
    - Beschikbaarheid: 99% uptime (productie-eis post-MVP)
    - Datakwaliteit: validatie van volledigheid, juistheid en consistentie van vragenlijstgegevens
    - Offline-mogelijkheid
4. Organisatorisch
    - Eenvoudige training en onboarding
    - Ondersteuning medewerkersvaardigheden (SFIA 9 framework)
    - Compatibiliteit met kantoor-bedrijfsvoering en legacy-systemen

[voor accountantsorganisaties kunnen interne functionele, performance en technische vereisten van toepassing zijn.]

3.4 Vereisten Bedrijfsvoering

1. Compliance en kwaliteitsborging
    - Versterking PKI accountants
    - AVG-conformiteit (encrypted lokale dataopslag, privacy-by-design)
    - Beveiligde Nederlandse hosting
    - Open-source licentie (reproduceerbare governance; Copyleft (GPLv3 / AGPLv3)
    - NIS2
    - Afstemming NBA-kwaliteitsborgingsraamwerk innovatie
2. Lifecycle-beheer
    - Configuration Management
    - Versiebeheer open-source codebase
    - Versiebeheer vragenlijst
    - Escalatie-procedures voor issues/beveiligingsproblemen
    - Termijn bewaren data in app beperkt tot maximaal een maand; de data en analyse moet worden vastgelegd in het controledossier.
    - Doel waarvoor de data gebruikt mag worden: identificatie van rode vlaggen
    - Plan afstoting van data met vernietiging van datasets.
3. Onderhoud en Kostenbeheersing
    - Beroepsgedragen technische en inhoudelijke ontwikkeling van app
    - Resource beschikbaarheid voor softwareontwikkeling
    - Datacentrum/hosting-infrastructuur

[voor accountantsorganisaties kunnen interne kwaliteitshandboeken, aansluiting op bestaande softwaresystemen, etc., ook van toepassing zijn.]

3.5 Vereisten voor regelgeving en maatschappij

1. Wet- en regelgeving
    - NV COS 315, NV COS 570, NV COS 4410 en NV KM
    - NBA-Handreiking 1151 Rapporteren over de controleaanpak continuïteit in de controleverklaring
    - NBA rode vlaggen tool (nba.nl)
    - BW2 titel 9, artikel 384 lid 3, 393 lid 3 en 5
    - NBA-kwaliteitsborgingsraamwerk innovatie controlemethodologie
    - GDPR/AVG
    - Kaders voor continuïteit en levensvatbaarheid: DSCR- en kredietratings van banken en kredietbeoordelaars, Basel IV en de Wet homologatie onderhands akkoord (WHOA). Aanvullende beoordelingsmethoden en modellen: Delphi-methode en OURA-rating.
    - AFM rapport (oktober 2025) “Verkenning naar de aanpak van (dis)continuïteit in wettelijke controles”
    - AFM-rapport (december 2025) “Voor beheerst gebruik van audit-tooling: 12 bouwstenen”
    - IFIAR (november 2023) “Use of technology in audits – observations, risks and further evolution”
2. Maatschappelijke relevantie
    - Bijdrage aan vertrouwen jaarrekening
    - Ondersteuning verantwoorde innovatie in accountantsvak
    - Bewijs dat kleinere kantoren door samenwerking kunnen innoveren

4. Technische vereisten definitie

4.1 Functionele vereisten

Tabel 3
Functionele vereisten

#	Functionele Eis	Specificatie	Relatie Stakeholder	Realisatie
F1	Vragenlijst administreren	vragen over rode vlaggen en financiële ratioanalyse, Nederlandse taal, webinterface	Accountants (gebruikers)	Kan in de app, maar ook via Excel-import
F2	Antwoorddata verwerken	Datamodel opbouw (scenario twee tot drie jaar levensvatbaarheid)	Applicatie-backend	
F3	Risicoanalyse genereren	Output: rode vlaggen per categorie, scenarioscore	Accountants (output)	
F4	Rapportage exporteren	PDF/Excel-download, NBA AuditWorkBook-aansluiting	Accountants (distributie)	Export naar PDF en OpenOffice Calc
F5	Dataveiligheid waarborgen	Encrypted storage NL-hosted, AVG-compliant logging	NBA (governance)	Database niet benaderbaar van buiten de hostinginstantie op demoserver.
F6	Validatieonderzoek ondersteunen	Pilotdata-verzameling (50-75 accountants × 2-3 klanten = 140-150 cases)	Nyenrode (validatie)	Evaluatie uitgevoerd door studenten.

4.2 Niet-functionele vereisten

Tabel 4
Niet-functionele vereisten

#	Vereiste	Specificatie	MOP/TPM
NF1	Performance	Response-time <3 sec per vraag; laadtijd <5 sec	Latency-meting
NF2	Betrouwbaarheid	MVP: uitvoeringssucces ≥99% (kritieke paden)	Incident-logging
NF3	Usability	SUS-score ≥70 (System Usability Scale) pilottest	gebruikersvragenlijst
NF4	Veiligheid	AVG-conformiteit, encrypted storage, access-control	Compliance-audit, pen-test (OWASP pentest suite in opbouw), security by design
NF5	Beschikbaarheid	MVP: 95% uptime (productie: 99%)	Uptime-monitoring. Glitchtip geïnstalleerd. Matomo beschikbaar.
NF6	Schaal	MVP: 100-150 pilotdeelnemers; toekomst: schaalbaar naar 1000+	Concurrency-testing. Nginx als loadbalancer ingezet.
NF7	AVG-compliance	100%	Voor go-live

5. Ontwerpoplossing

5.1 Overwogen Alternatieven

De Taskforce heeft expliciet de volgende alternatieven overwogen en verworpen:
Tabel 5
Beoordeling van alternatieven

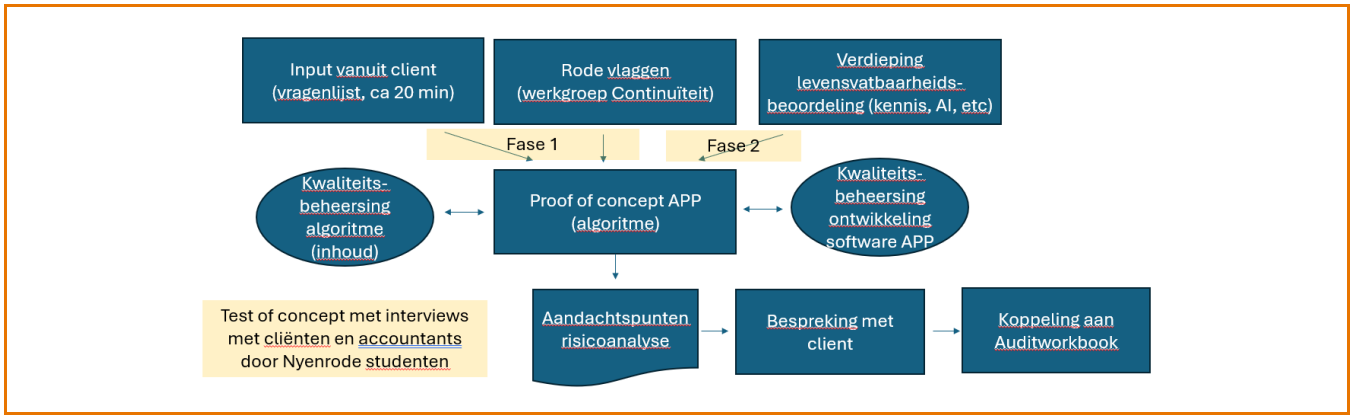
Alternatief	Evaluatie	Reden afwijzing
Uitsluitend handreikingen + training	Bewezen beperkte effectiviteit	Accountants worstelen dagelijks met complexiteit; niet voldoende
Closed-source commercial software	Hoge kosten, afhankelijkheid, geen innovatie-bewijs	Te belastend voor kleine kantoren; mist open kennisdeling
Direct AI/data-integraties	Interessant toekomstperspectief	Te complex voor een eerste fase; verder onderzoek nodig

Gekozen voorkeuroplossing: Open-source MVP met wetenschappelijke validatie
Rationale:

- Laagdrempelig te gebruiken en verder te ontwikkelen door mkb-kantoren
- Transparantie en reproduceerbare methodologie
- Aansluiting NBA-kwaliteitsborgingsraamwerk van innovaties en Nederlandse standaarden (met name NV COS 315, NV COS 570 en NV COS 4410)
- Bewijs dat kleinere kantoren door samenwerking kunnen innoveren
- Basis voor verdere uitbreiding (Fase 2+)

5.2 Theoretische werking voorkeursoplossing

Figuur 1
Opzet van de continuïteitsapp



Dit SEMP ziet op fase 1 met een MVP van de app. Fase 2 kan in een later moment worden toegevoegd.
De volgende tabel geeft de fase 1 met onderdelen en kwaliteitsborging weer.

Tabel 6
Onderdelen en kwaliteitsborging van fase 1

Onderdelen	Input	Output
Input vanuit cliënt	• Vragenlijst gebruikt in MKB levensvatbaarheid. à validatie met onderzoek universiteit Leiden en Nyenrode met bespreking van risicogebieden met deelnemers • Opstellen van verbeterde en/of sectorspecifieke vragenlijsten door NBA-commissie of taskforce (vervolgstap)	Risicogebieden met mogelijke continuïteitsproblemen
Rode vlaggen	• Lijst is gebaseerd op de rode vlaggenlijst van werkgroep Continuïteit van de NBA • Aanvullingen in praktijk en sectorspecifiek door NBA-commissie of taskforce (vervolgstap)	• Periodiek bijgewerkte geaccepteerde lijst met rode vlaggen; mogelijk specifiek gemaakt naar omvang en branche.
App/ algoritme	• Mapping van vragenlijst cliënt en rode vlaggen door experts levensvatbaarheid • bijgewerkt door NBA-commissie of taskforce (vervolgstap)	• Geïdentificeerde lijst met rode vlaggen
Aandachtsgebieden risicoanalyse	• Geïdentificeerde lijst met rode vlaggen • Initiële resultaten uit onderzoek	• Validatie van relevantie van rode vlaggen en analyse false positives/negatives op basis van interviews met beroepsbeoefenaren en informatie uit controledossiers • Input voor verbetering vragenlijsten/rode vlaggen/mapping
Bespreking met de cliënt	• Input van use-cases en kantoren	• Input voor verbetering vragenlijsten/rode vlaggen/mapping

In de opzet van de app is een feedbackloop voorzien die door een NBA-commissie of taskforce kan worden verwerkt in de onderdelen van de app.

6. Architectuur

6.1 Functionele Architectuur

Vanuit de vereisten wordt de applicatie logisch ontleed in onderstaande niveaus:

Tabel 7
Logische architectuur van de continuïteitsapp

Continuïteitsapp - Logische Architectuur
User Interface (webportaal)
• **Vragenlijst-module (100 vragen)**
• **Input-validatie & UI-logica**
• **Rapportage-download (PDF/Excel)**
Applicatie-logica (dataverwerking)
• **Datamodel (roodvlag-categorisering)**
• **Scenarioanalyse-algoritme (twee tot drie jaar horizon)**
• **Risicoaggregatie & scoring**
• **Export-generators**
Data & Persistentie (Backend)
• **Vragenlijstconfiguratie (roodvlaggen-structuur)**
• **Gebruiker-sessies & antwoordopslag**
• **Rapportage-templates**
• **Audit-logging (AVG-compliant)**
Ondersteuning & Beheer
• **Hosting (Nyenrode-server NL)**
• **Backup & Disaster Recovery**
• **Monitoring & Alerting**

6.2 Work Breakdown Structure

De benodigde controlewerkzaamheden voor continuïteit zijn beschreven in standaard 315 (en 570) en NBA-tooling voor rode vlaggen. De werkzaamheden die de app ondersteunt betreffen die van de identificatie van de rode vlaggen en de koppeling daarvan aan inherente risicofactoren.

7. Implementatiestrategie

7.1 Implementatiestrategie per Fase

Fase 1: MVP Development & Validation (november 2025 – oktober 2026)

Milestone 1a: Datamodel-afronding (november 2025)
- Output: Definitief datamodel voor 100 rode vlaggen
- Eigenaar: Robert Los
- Deliverable: Datamodel-documentatie (ERD, SQL-schema, UML-model)

Milestone 1b: Applicatie-prototype (december 2025 – januari 2026)
- Output: Werkende applicatie met webinterface, beveiligde opslag
- Eigenaar: Robert Los
- Deliverable: Werkende applicatie vanaf een testserver

Milestone 1c: Pilottest en validatie (december 2025 – september 2026)
- Output: Resultaten van 50-75 accountants met 140-150 ondernemingen
- Eigenaar: Nyenrode (Robin Litjens, Joost van Buuren) + 50+ studenten
- Deliverable: Validatiedata, eerste bevindingen

Milestone 1d: Afronding en publicatie van het MVP (oktober 2026)
- Output: Definitieve applicatie + validatierapport
- Eigenaar: Taskforce (gezamenlijk)
- Deliverable: Werkende applicatie, SEMP en initiële validatie

Fase 2: Uitbreiding en operationalisering (na oktober 2026)
- Scope nog niet uitgewerkt; afhankelijk van Fase 1-evaluatie
- Mogelijke richtingen: AI-integratie, data-connectoren, schaaluitbreiding
- Planning: T.b.d. na MT NBA-besluitvorming

8. Verificatie en validatie

Zie bijlage 1.

9. Operationsplan en risicomanagement

9.1 Identificatie en beoordeling kritieke risico's voor voortgang project

Tabel 8
Kritieke projectrisico's en beheersmaatregelen

#	Risicogebied	Potentieel Gevolg	Waar-schijn lijkheid	Impact	Mitigatie	Risico-eigenaar
R1	Beschikbaarheid ontwikkelaars	Projectvertraging	LAAG→ MIDDEL	KRITIEK	Backup-programmeur; voldoende spec's/docs vóór start	Taskforce
R2	AVG-conformiteit hosting	Wettelijk risico/reputatierisic o	MIDDEL	KRITIEK	Compliance vaststelling; externe auditor	Taskforce
R3	Pilotdeelnemers-werving (100+ ondernemingen)	Onvoldoende validatiedata	MIDDEL	HOOG	Vroege werving via Nyenrode kanalen	Nyenrode
R4	Scope-creep (extra vereisten tijdens dev)	Deadline-risico	HOOG	LAAG	Strikte change-control; MoSCoW-prioritering (Must/Should/Could/Won't haves)	Taskforce
R5	Methodologische afstemming beroepsreglementering	Applicatie niet acceptabel	MIDDEL	HOOG	Regelmatige afstemming programma-manager met Werkgroep Continuïteit; design-reviews	Taskforce
R6	Onjuist gebruik van app	Onjuiste controle conclusies	MIDDEL	HOOG	Trainingen, documentatie, review en evaluatie	Implementatiet eam (valt buiten bestek taskforce)

9.2 Risicoanalyse beheer van app

Accountantsorganisaties zijn op grond van SKM 1, paragraaf 32f, verplicht de betrouwbaarheid en veiligheid van IT-systemen te borgen. In de gevallen waarin de app wordt geïntegreerd met bestaande systemen, zullen diverse risico's ondervangen zijn. De onderstaande risico's betreffen veel voorkomende risico's; de lijst is niet limitatief en andere risico's kunnen van toepassing zijn.

Tabel 9
Risicoanalyse voor beheer van de continuïteitsapp

Risico	Omschrijving	Maatregel / verificatie in SEMP
1. Identiteit en toegang		
Omschrijving continuïteitsapp: Het klant- en gebruikersbeheer is ingericht vanuit het uitgangspunt dat klanten zichzelf bij de applicatie kunnen aanmelden of door een accountant kunnen worden geregistreerd. Beheerders kunnen accountants registreren en groeperen per accountantskantoor. Zodra een klant aan een accountant is gekoppeld, hebben andere accountants geen toegang tot de klantgegevens, ook niet via URL-manipulatie. Deze beveiliging kan nog verder worden aangescherpt. Er is niet gekozen voor volledige multitenancy, omdat dit het proces voor het vinden en koppelen van klanten onnodig zou bemoeilijken en bovendien buiten de scope van het MVP lag. Accountantskantoren kunnen wel een eigen installatie gebruiken. Met een Docker Compose-script kan de applicatie op een eigen server worden geïmplementeerd. Hiervoor kan toegang worden verleend tot de Docker-images die voor de applicatie zijn ontwikkeld. Het huidige gebruikersbeheer is gebaseerd op de standaardfunctionaliteit van Django, aangevuld met het Allauth-pakket. Deze inrichting biedt een goede basis voor een toekomstige migratie naar een professionelere Keycloak-omgeving. Via federatieve koppelingen kunnen dan verschillende organisaties aansluiten en kan eventueel gedelegeerd accountbeheer worden ingericht. Ook een koppeling met bijvoorbeeld DigiD behoort dan tot de mogelijkheden. Een dergelijke uitbreiding vormt echter een zelfstandig vervolgproject.		
Gebroken toegangscontrole en tenant-isolatie	Gebruiker ziet dossiers van een ander kantoor of een andere klant; omvat ook autorisatiefouten in API's op object- en functieniveau (BOLA/BFLA).	Autorisatiemodel en tenant-scheiding als ontwerpeis vastleggen; verificatie via geautomatiseerde autorisatietests en periodieke pentests.
Zwak identiteits- en toegangsbeheer (IAM) en authenticatie	Te ruime rechten, ontbrekende MFA, slecht beheerde credentials en niet-menselijke identiteiten (service-accounts, API-sleutels).	Verplichte (phishingbestendige) MFA, least privilege, periodieke herbeoordeling van rechten, centraal secretsbeheer; verificatie via access reviews en audits.
2. Cloudinfrastructuur en beheer		
Omschrijving continuïteitsapp: De applicatie draait momenteel in een Docker Compose-omgeving op een virtuele machine binnen een professioneel beheerde rootserver. De gelaagde architectuur biedt aanvullende beveiliging: wanneer de Django-applicatie wordt gecompromitteerd, ontstaat niet automatisch toegang tot de database of andere onderdelen van de server, zoals de certificaatopslag en de reverse proxy. De rootserver en virtuele machines worden met scripts ingericht en beheerd via QEMU/libvirt. Momenteel wordt onderzocht of Terraform en Ansible kunnen worden ingezet om deze inrichting verder te automatiseren en te standaardiseren.		

Risico	Omschrijving	Maatregel / verificatie in SEMP
Voor iedere build wordt een afzonderlijke container-image gegenereerd. Deze images worden opgeslagen in daarvoor bestemde repositories, zowel in de cloud als lokaal in een Nexus-repository bij de ontwikkelaar. Hierdoor kan vanuit compliance- en auditperspectief worden vastgesteld welke softwareversie op welk moment in productie is geweest. De applicatielogging wordt naar de standaarduitvoer geschreven, zodat de logs met de Docker Compose-tooling kunnen worden geraadpleegd en geaudit. In een latere fase kan de logging worden gekoppeld aan bijvoorbeeld Grafana of een Elastic Stack-omgeving; deze koppeling is momenteel nog niet gerealiseerd. Wel is GlitchTip, vergelijkbaar met Sentry, gekoppeld om foutregistratie en technisch beheer te ondersteunen. Van de database worden back-ups gemaakt, zodat herstel na bijvoorbeeld een ransomware-aanval mogelijk is.		
Misconfiguratie en gebrekkig wijzigingsbeheer	Onjuiste instellingen zoals open opslag, uitgeschakelde logging, onveilige back-ups en te ruime rechten. OWASP A02	Infrastructure-as-code, vastgestelde configuratiebaselines, geautomatiseerde configuratiecontrole, formeel change management; verificatie via configuratiescans.
Kwetsbaarheden en trage patching	Bekende kwetsbaarheden worden snel uitgebuit; voorbeeld is het binnendringen bij het Openbaar Ministerie via een kwetsbaarheid in Citrix Netscaler (European Union Agency for Cybersecurity [ENISA], 2025; Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV], 2025a).	Kwetsbaarheidsscans, patch-SLA's naar ernst, externe pentest per grote release; verificatie via patchrapportages.
Ransomware en verlies van beschikbaarheid/ integriteit	Versleuteling of vernietiging van data en back-ups; ransomware vormt de kern van de inbraakactiviteit in de EU. Raakt ook de wettelijke bewaarplicht van gegevens (ENISA, 2025).	Onveranderbare/offline back-ups, periodieke hersteltests, vastgelegde RTO/RPO-eisen, netwerksegmentatie; verificatie via hersteloefeningen.
3. Applicatie en ontwikkeling		
<u>Omschrijving continuïteitsapp:</u> De standaardfunctionaliteit van Django is uitgebreid met Django Axes om herhaalde en onbeperkte inlogpogingen tegen te gaan. Op de rootserver is daarnaast Fail2ban geconfigureerd. Er wordt een afzonderlijke virtuele machine ingericht voor het uitvoeren van beveiligingstests met Burp Suite en/of een OWASP-testsuite. Deze tests verschaffen inzicht in de technische beveiliging en mogelijke kwetsbaarheden van het systeem. Bij ingebruikname van een productieomgeving wordt sterk aanbevolen om tevens een onafhankelijke penetratietest uit te voeren.		
Onveilige interfaces en API's	Zwak beveiligde of publiek bereikbare koppelingen met banken, boekhoudpakketten en overheidssystemen.	API-inventaris, authenticatie en autorisatie per endpoint, rate limiting; verificatie via API-securitytests.
Cryptografische tekortkomingen	Onversleutelde of zwak versleutelde gegevens en gebrekkig sleutelbeheer, met risico op blootstelling van gevoelige gegevens. OWASP A04 (OWASP Foundation, 2025).	Versleuteling in transit en at rest, sleutelbeheer (bij voorkeur eigen sleutels/HSM), geen zelfgebouwde cryptografie; verificatie via configuratie- en codereview.

Risico	Omschrijving	Maatregel / verificatie in SEMP
Onveilig ontwerp en ontwikkeling	Injectie, ontwerpfouten, integriteitsfouten en onjuiste foutafhandeling ('fail open'). OWASP A05, A06, A08 en A10; CSA 'Insecure Software Development' (OWASP Foundation, 2025; Cloud Security Alliance, 2024).	Threat modeling per ontwerpfase, privacy by design (AVG art. 25), secure-codingstandaard (OWASP ASVS), code-review, SAST/DAST in de pipeline.
Compromittering van AI-functies (alleen indien de app AI gebruikt)	Manipulatie of misbruik van AI-modellen, data, agents, tools en pipelines. (Cloud Security Alliance, 2026).	Scheiding van klantdata, beperkte rechten voor AI-componenten, geen klantdata naar externe modellen zonder grondslag; verificatie via AI-specifieke tests.
4. Keten en leveranciers		
Kwetsbare software-toeleveringsketen	Gecompromitteerde bibliotheken, buildsystemen of distributie. OWASP A03: weinig voorkomend in de data, maar met de hoogste gemiddelde exploit- en impactscores (OWASP Foundation, 2025).	SBOM, dependency-scanning, ondertekende builds; verificatie via pipeline-controles. Samenwerking zoeken met een leverancier voor de hosting die ISO-27001 en NEN-7510 is gecertificeerd.
Onveilige derde partijen	Risico's via cloudprovider, sub-verwerkers en externe diensten. (Cloud Security Alliance, 2026; Landau, 2026).	Leveranciersbeoordeling, verwerkersovereenkomsten (AVG art. 28), beoordeling van assurance-rapporten; periodieke herbeoordeling.
Concentratierisico	Bij afhankelijkheid van een klein aantal aanbieders kan één incident veel afnemers tegelijk raken, zoals de CrowdStrike-storing van juli 2024 (Nationaal Cyber Security Centrum, 2024).	Exit- en continuïteitsstrategie, uitwijkscenario's; verificatie via continuïteitstests.
Geopolitieke afhankelijkheid en datalocatie	Veranderende geopolitieke verhoudingen kunnen bestaande digitale afhankelijkheden risicovol maken (NCTV, 2025a).	Bewuste keuze van cloudprovider en datalocatie, periodieke herbeoordeling van afhankelijkheden.
5. Mens en dreigingsactoren		
Phishing en accountovername	Gestolen inloggegevens van accountants of beheerders; de AP zag in 2025 een aanzienlijke stijging van datalekken door phishing (Autoriteit Persoonsgegevens, 2026; ENISA, 2025).	Phishingbestendige MFA, detectie van afwijkend inloggedrag, awareness voor gebruikers; verificatie via phishingsimulaties.

Risico	Omschrijving	Maatregel / verificatie in SEMP
AI-versterkte aanvallen	Aanvallers gebruiken AI voor snellere verkenning, kwetsbaarheidsontdekking en overtuigender phishing. (Cloud Security Alliance, 2026; Autoriteit Persoonsgegevens, 2026).	Kortere patchcycli, sterkere detectie, aanvullende controles op identiteit.
Onbedoelde openbaarmaking	Per ongeluk gedeelde of publiek gezette gegevens. (Cloud Security Alliance, 2024; Autoriteit Persoonsgegevens, 2026).	Dataclassificatie, DLP-controles, standaard privé-instellingen voor opslag en deellinks.
Accountants als aantrekkelijk doelwit	Toegang tot financiële gegevens van veel klanten tegelijk maakt de app een waardevol doelwit (eigen afleiding, geen bron).	Meewegen in dreigingsanalyse en risicoscoring.
6. Detectie en respons		
Onvoldoende logging en alerting	Incidenten worden niet of te laat ontdekt; geen bewijs van wie welk dossier inzag. Logging zonder alerting heeft weinig waarde. OWASP A09 (OWASP Foundation, 2025).	Centrale logging (SIEM), manipulatiebestendige audittrail van dossiertoegang, alerting op relevante gebeurtenissen.
Gebrekkige incidentrespons en meldplicht	Meldtermijnen worden niet gehaald: AVG-meldplicht binnen 72 uur en melding van significante incidenten onder de Cyberbeveiligingswet (Verordening (EU) 2016/679, 2016, art. 33).	Incidentresponsplan met rolverdeling, meldprocedures en periodieke oefeningen.
7. Governance en compliance		
Niet voldoen aan de AVG	Onvoldoende passende technische en organisatorische maatregelen, geen DPIA, geen privacy by design (Verordening (EU) 2016/679, 2016, art. 25, 32 en 35).	DPIA uitvoeren, privacy-eisen opnemen in de requirementsbaseline en traceerbaar verifiëren.
Onduidelijke positie onder de Cyberbeveiligingswet	De Cbw geldt sinds 15 augustus 2026; of een SaaS-dienst als cloudcomputingdienst kwalificeert vraagt een zorgvuldige analyse. Klanten die er wel onder vallen kunnen ketenverplichtingen opleggen (NCTV, 2025b).	Juridische toets op toepasselijkheid; voorbereiden op leveranciersvragen van klanten.
Ontbrekende security-governance	Geen eigenaarschap van risico's en geen traceerbaarheid van beveiligingseisen. (Landau, 2026).	ISMS (ISO/IEC 27001, aangevuld met 27017/27018), risico-eigenaren benoemen, traceerbaarheid van security-eisen in het SEMP.

9.3 Communicatiestrategie

Tabel 10
Communicatiestrategie

Bericht	Ontvanger	Frequentie	Format
Voortgangsrapport	MT NBA, Age Lammers	Maandelijks	E-mail en onepager
Technische status	Projectteam	Tweewekelijks	Teamoverleg
Milestone-updates	Stakeholders	Per milestone	presentatie Acc.tech community
Validatieresultaten	NBA, Accounttech	Per pilotfase	Interimrapport
Eerste bevindingen	Alle stakeholders	Oktober 2026	SEMP + presentatie eerste bevindingen
Periodieke update	Alle stakeholders	Halfjaarlijks en bij een nieuwe release	Bij Accounttech-bijeenkomsten

9.4 Benodigde documentatie

Uit te produceren documenten:

1. Technische documentatie
    - Datamodel-specificatie (ERD)
    - API-documentatie (backend)
    - Deployment-handleiding (hosting)
    - Datasecurity
2. Gebruikersdocumentatie
    - Quickstart guide
    - FAQ-document
    - Trainingmateriaal
3. Projectdocumentatie
    - Dit SEMP
    - Rapport met theoretisering van app
    - Onderzoeksrapport met verificatie en validatierapport van app
    - Design Review Records
4. Opensourcegovernance
    - README.md (project-intro)
    - CONTRIBUTING.md (bijdrage-richtlijnen)
    - LICENSE (bijv. Apache 2.0)
    - CHANGELOG.md (versiebeheer)

10. Configuratie- & versiebeheer

10.1 Configuratiemanagementstrategie

Baselines:

1. Requirement Baseline (februari 2026)
    - Verzamelde functionele/niet-functionele vereisten
    - Akkoord alle stakeholders
    - Onderdeel system design review
2. Design Baseline (januari 2026)
    - Datamodel, architectuur
    - Interface-specificaties
    - implementatieplan

3. Product Baseline (15 mei – oktober 2026)
    - Werkende applicatie
    - Validatierapport
    - Documentatie & code

10.2 Change Control (opzet)

- Minor changes (bug-fixes, documentatie-updates): goedkeuring door de projectleider
- Major changes (scope-aanpassingen, wijzigingen in vereisten): Stakeholder-akkoord + Projectleider
- Configuration Item (CI): Applicatie-codebase, datamodel, documentatie
- Version Control: Git (open-source repository)

10.3 Versiebeheer

Tabel 11
Versiebeheer

Versie	Datum	Auteur	Status	Opmerkingen
1.0	26 oktober 2026	Joost van Buuren/Arjaan van den Berg	Fase 1 bijna afgerond	Presentatie Accounttech

10.4 Bewerkers- en overige overeenkomsten

Deze moeten nog worden uitgewerkt.

10.5 Openstaande punten

- Beperkt aantal dossiers betreffen lopende dossiers tijdens het onderzoek (30%); mogelijke bias vanwege defensieve houding accountants (zie bijlage 1,
- Verificatie van continuïteitsapp nog definitief maken (zie bijlage 1 par 6.2).
- Opensourcestandaard nog definitief maken
- Onderhoud technisch en inhoudelijk nog afspraken over maken
- Update van de vragenlijsten

11. Bijlagen

1. Theoretisering en validering van de continuïteitsapp
2. Methodeverificatie checklist
3. Interviewprotocollen
4. SEMP bijlage 4 Rode Vlaggen en Continuiteit A Vlaggen v1.2
4. SEMP bijlage 4 Rode Vlaggen en Continuiteit B Mapping v1.2

12. Referenties

1. Van Buuren, J. (2022). Vooronderzoek naar de opzet van een Raamwerk voor Kwaliteitsbeheersing van Innovatie van Controlemethodologie. Nyenrode Business Universiteit. nba.nl
2. Van Buuren, J. (2023). Vooronderzoek naar theoretisering en validering van Controlemethodologie. Nyenrode Business Universiteit. nba.nl
3. Van Buuren, J. (2024). Gebruik AuditWorkBook. Handleiding en use-case onderzoek over toepassing van auditworkbook. Nyenrode Business Universiteit. nba.nl

4. Van Buuren, J. & Wijma, W. (2022). Over kwaliteitsborging van datagedreven controlemethodologie. Maandblad Voor Accountancy En Bedrijfseconomie, 96(1/2), 15–25. https://doi.org/10.5117/mab.96.785564.
5. Projectdocumenten Accounttech Taskforce
    - 20251017-Project-Programmavoorstel-AccTech-TF-cont.docx
    - 20251017-projectvoorstel.docx
    - 20251105-Continuiteit-opzet-opdrachtformulering.docx
6. NBA-normen (HRA):
    - NV COS 4410 (Samenstellingsopdrachten)
    - NBA (2023). Interactieve wegwijzer bij de risicoanalyse : Rode vlaggen bij het tijdig en adequaat signaleren van continuïteitsvraagstukken. Werkgroep Continuïteit. Geraadpleegd op 20 oktober 2026, van nba.nl (link).linklink
7. Compliance-kaders
    - GDPR / AVG
8. AFM. (2025a). Voor beheerst gebruik van audit-tooling: 12 bouwstenen. AFM.nl
9. AFM. (2025b). Verkenning naar de aanpak van (dis)continuïteit in wettelijke controles. AFM.nl
10. IFIAR. (2023). Use of technology in audits. Observations, risks and further evolution. IFIAR.org
11. IT- en cyberrisicomanagement
    - Autoriteit Persoonsgegevens. (2026). Report data breaches 2025. https://www.autoriteitpersoonsgegevens.nl/en/documents/report-data-breaches-2025
    - Cloud Security Alliance. (2024). Top threats to cloud computing 2024. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024
    - Cloud Security Alliance. (2025). Top threats to cloud computing deep dive 2025. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025
    - Cloud Security Alliance. (2026). Top threats to cloud computing survey report 2026. https://cloudsecurityalliance.org/artifacts/top-threats-cloud-computing-2026
    - European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
    - Landau, H. (2026, 20 augustus). CSA Top Threats to Cloud Computing 2026: AI reshuffled what counts, and it landed on access. Act Security. https://act.security/resources/csa-top-threats-to-cloud-computing-2026-ai-reshuffled-what-counts-and-it-landed-on-access
    - Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025a). Cybersecuritybeeld Nederland 2025. https://www.nctv.nl/onderwerpen/c/cybersecuritybeeld-nederland
    - Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025b). Welke organisaties vallen onder de Cyberbeveiligingswet? https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet/welke-organisaties-vallen-onder-de-cyberbeveiligingswet
    - Nationaal Cyber Security Centrum. (2024). Cybersecuritybeeld Nederland. https://www.ncsc.nl/wat-doet-het-ncsc-voor-jou/cybersecuritybeeld-nederland
    - OWASP Foundation. (2025). OWASP Top 10:2025. https://owasp.org/Top10/2025/
    - Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). (2016). Publicatieblad van de Europese Unie, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Bijlage afkortingen

- SEMP: Systems Engineering Management Plan
- MVP: Minimum Viable Product
- NBA: Nederlandse Beroepsorganisatie van Accountants
- ISA: International Standards on Auditing
- AVG: Algemene Verordening Gegevensbescherming (GDPR)
- CI: Configuration Item
- UI/UX: User Interface / User Experience
- SUS: System Usability Scale
- RGS: Referentie GrootboekSchema

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Mercuriusplein 3
2132 HA Hoofddorp
Postbus 242
2130 AE Hoofddorp

T 088 4960 301
E nba@nba.nl
I www.nba.nl