# AI-gestuurde Risicodetectie & Mitigatie Referentiemodel voor GRC

**1. Inleiding**

In een tijd waarin cyber-, data- en AI-gerelateerde risico’s exponentieel toenemen en wetgeving continu evolueert, is er een groeiende behoefte aan oplossingen die niet alleen risico’s detecteren, maar ook de wetgevende implicaties hiervan helder maken. Ons concept richt zich op het ontwikkelen van een uniek referentiemodel dat uiteenlopende contextgegevens (zoals bedrijfscontext, business capabilities, jaarverslagen, klant- en leveranciersdata, auditrapporten, Gartner-docs en sector-specifieke informatie) koppelt aan een AI-gestuurde risicoanalyse. Het model genereert een gedetailleerd risicoprofiel én biedt concrete mitigatievoorstellen door te linken naar intermediaire standaarden of clauses die meerdere risico’s en wettelijke verplichtingen kunnen afdichten. Deze aanbevelingen worden in begrijpelijke taal uitgelegd en aangepast aan de specifieke context van de organisatie.

Dit document beschrijft onze unieke waardepropositie, de verschillende scenario’s om dit product op de markt te zetten, de bijbehorende trade-offs en een voorstel voor een gefaseerde opstartplanning.

**2. Probleemstelling en Marktbehoefte**

**Uitdagingen in de markt:**

* **Complexe regelgeving en risico’s:** Organisaties moeten voldoen aan steeds strenger wordende wet- en regelgeving op het gebied van cyber, data en AI.
* **Gebrek aan geïntegreerde oplossingen:** Veel GRC-oplossingen richten zich enkel op het blootleggen van risico’s. Er is echter behoefte aan een oplossing die ook de wetgevende implicaties verduidelijkt en concrete mitigatievoorstellen doet.
* **Data-integratie:** Er is een behoefte aan een oplossing die uiteenlopende bronnen en contextinformatie integreert, zodat risico’s nauwkeurig in kaart worden gebracht en passende maatregelen kunnen worden voorgesteld.

**Onze oplossing:**

Een AI-gestuurd referentiemodel dat diverse data-input (bedrijfscontext, business capabilities, jaarverslagen, klanten-, leveranciers- en auditsgegevens, branche-inzichten) analyseert met behulp van Large Language Models (LLM’s) en decision matrices. Dit resulteert in:

* **Een gedetailleerd risicoprofiel,**
* **Duidelijke uitleg van de bijbehorende wetgevende implicaties,** en
* **Concrete mitigatievoorstellen** die koppelen naar intermediaire standaarden of specifieke clauses die meerdere risico’s en wettelijke verplichtingen adresseren.

Deze aanbevelingen worden in ‘mensentaal’ uitgelegd en vertaald naar de unieke context van de organisatie, waardoor zowel kmo’s als corporate organisaties direct inzicht en toepasbare acties krijgen.

**3. Waardepropositie**

* **Uniek Referentiemodel met Wetgevende Focus:**  
  Naast het blootleggen van risico’s, verduidelijkt ons model de wetgevende implicaties die aan deze risico’s ten grondslag liggen. Dit biedt organisaties direct inzicht in welke wettelijke verplichtingen zij mogelijk niet naleven.
* **Concrete Mitigatievoorstellen:**  
  De voorgestelde maatregelen zijn gekoppeld aan intermediaire standaarden of specifieke clauses, zodat meerdere risico’s en verplichtingen met één aanbeveling kunnen worden afgedekt. Deze aanbevelingen worden verder uitgelegd in begrijpelijke taal en vertaald naar de context van de organisatie, zodat de impact en implementatie duidelijk worden.
* **Automatisering en Integratie:**  
  Mogelijkheid tot automatisering via API-extensies voor zowel input (bijv. SIEM of asset management systemen) als output (integratie in GRC-platformen).
* **Brede Doelgroep:**  
  De oplossing is niet langer beperkt tot kmo’s; ook corporate organisaties hebben baat bij een geïntegreerd overzicht van risico’s, wetgevende implicaties en de bijbehorende mitigatievoorstellen.
* **Optioneel - Advies en Consultancy:**  
  Naast de technische oplossing bieden wij de mogelijkheid om als adviesbureau maatwerk te leveren. Hierdoor kunnen organisaties niet alleen hun risico’s in kaart brengen, maar krijgen zij ook advies over de implementatie van de meest effectieve maatregelen.

**4. Product & Implementatie Scenario’s**

**Scenario 1: MVP – Website met Output in PDF of CSV**

* **Beschrijving:** Een eenvoudige webinterface waarin gebruikers relevante data invoeren en als output een gedetailleerd risicoprofiel ontvangen, inclusief uitleg over de wetgevende implicaties en concrete mitigatievoorstellen (in PDF/CSV-formaat).
* **Doel:** Snel valideren van het concept en het verzamelen van feedback van vroege gebruikers.
* **Kostenniveau:** Laag; snelle implementatie en minimale investeringen in de eerste fase.

**Scenario 2: MVP met API-extensie -> deferred (kijk of klanten hier op termijn nood aan hebben)**

* **Beschrijving:** Uitbreiding van de MVP door het aanbieden van API’s voor integratie met inputbronnen (zoals SIEM of asset management systemen) en output richting GRC-platformen.
* **Doel:** Automatiseren van data-integratie en real-time risicodetectie in bestaande IT-ecosystemen.
* **Kostenniveau:** Medium tot hoog; vereist extra ontwikkelingsinspanningen en beveiligingsmaatregelen.

**Scenario 3: Consulting Model**

* **Beschrijving:** Positioneer onszelf als een adviesbureau dat het referentiemodel intern gebruikt voor het leveren van maatwerk risicoanalyses, waarbij zowel de risico’s als de wetgevende implicaties en mitigatievoorstellen op een begrijpelijke wijze worden vertaald.
* **Doel:** Diepgaande klantrelaties opbouwen en premium adviesdiensten leveren.
* **Kostenniveau:** Laag tot medium (software wordt intern ontwikkeld), maar minder schaalbaar.

**Scenario 4: Plug-in voor ERP/GRC-systemen (bijv. ODOO, Exact) -> deferred (kijk of klanten hier op termijn nood aan hebben)**

* **Beschrijving:** Lever het platform als een plug-in binnen bestaande ERP- of GRC-systemen, zodat gebruikers direct in hun vertrouwde omgeving toegang hebben tot het risicoprofiel en de bijbehorende aanbevelingen.
* **Doel:** Toegang krijgen tot een bestaande gebruikersbasis en de adoptie binnen MKB- en corporate-omgevingen vergemakkelijken.
* **Kostenniveau:** Medium; afhankelijk van de integratienoden met het hostende platform.

**Scenario 5: White Labeling --> geen piste, je maakt competitie slimmer dan nodig en rijker dan nodig**

* **Beschrijving:** Het referentiemodel beschikbaar maken als white-label oplossing voor derde partij consultingproviders (bijv. Spinae, Deloitte) die het onder hun eigen merk kunnen aanbieden.
* **Doel:** Snelle marktpenetratie via gevestigde merken, met lagere eigen marketing- en saleskosten.
* **Kostenniveau:** Medium; vereist strikte contracten en bescherming van intellectueel eigendom.

**Scenario 6: Volledig Geïntegreerd GRC Platform**

* **Beschrijving:** Ontwikkel een compleet geïntegreerd platform dat alle aspecten (risicodetectie, compliance monitoring, mitigatievoorstellen, etc.) in één oplossing bundelt.
* **Doel:** Een alles-in-één oplossing bieden voor organisaties die zowel kmo’s als grote corporate spelers bedienen, met een volledig overzicht van risico’s, wetgevende implicaties en praktische oplossingen.
* **Kostenniveau:** Hoog; lang ontwikkeltraject en uitgebreide operationele ondersteuning vereist.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenario | Voordelen | Nadelen / Uitdagingen | Complexiteit & Investering | Doelgroep & Markttoegang |
| MVP (Website) | Snelle validatie, Lage ontwikkelkosten, Inzicht in risico’s, wetgeving en mitigatie | Beperkte functionaliteit, Geen integratie met andere systemen | Laag | N/A – focus = leren of er interesse is en of concept haalbaar is |
| MVP met API-extensie | Automatisering, Integratie met SIEM/GRC, Real-time data-analyse | Hogere ontwikkelings- en onderhoudskosten, Complexe beveiligingsvereisten | Medium tot Hoog | Middelgrote tot grote bedrijven met geavanceerde IT-ecosystemen |
| Consulting Model | Hoge toegevoegde waarde, Sterke klantrelaties, Premium pricing | Minder schaalbaar, Afhankelijk van consultant expertise, Hogere servicekosten | Laag tot Medium | Organisaties met complexe risico-behoeften, zowel kmo’s als corporates |
| Plug-in (ODOO/Exact) | Toegang tot bestaande gebruikersbasis, Lagere adoptiedrempel | Afhankelijkheid van platform roadmaps, Beperkte maatwerkopties | Medium | MKB én corporate organisaties die reeds gebruikmaken van ERP/GRC-systemen |
| White Labeling | Snelle marktpenetratie via partners, Lagere eigen saleskosten | Minder controle over eindklanten, Risico op kennisverspreiding, Contractuele complexiteit | Medium | Consultancybureaus en adviserende partijen met een groot netwerk |
| Volledig Geïntegreerd GRC Platform | Compleet aanbod, Sterke marktpositionering, Volledige compliance | Hoogste investering, Langere time-to-market, Operationele complexiteit | Hoog | Grote ondernemingen die een alles-in-één oplossing zoeken |

**5. Opstartplanning en Next Steps - Suggestie**

**Fase 1: Conceptvalidatie & MVP-ontwikkeling (0-6 maanden)**

* **Doelen:**
  + Ontwikkelen van een basale webinterface (scenario 1) die een risicoprofiel genereert inclusief uitleg van wetgevende implicaties en mitigatievoorstellen in PDF/CSV.
  + Feedback verzamelen van vroege gebruikers en verfijnen van het referentiemodel.
* **Acties:**
  + Samenstellen van een kernteam (softwareontwikkelaars, data scientists, domeinexperts).
  + Inventariseren van benodigde datasets en ontwikkeling van de eerste versie van AI/LLM-modellen.
  + Implementeren van basis security- en datagovernance maatregelen.

**Fase 2: Integratie & Uitbreiding (6-12 maanden)**

* **Doelen:**
  + Uitbreiden van de MVP met API-extensies (scenario 2) voor geautomatiseerde input (bijv. SIEM/asset management) en output richting GRC-platformen.
  + Initiëren van pilots voor integratie in bestaande systemen via plug-ins (scenario 4).
* **Acties:**
  + Ontwikkeling van API’s en het opzetten van gedetailleerde documentatie.
  + Realiseren van pilotprojecten met partners en klanten binnen de doelmarkten.
  + Verfijnen van risicoprofielen, wetgevende analyses en mitigatievoorstellen op basis van live data.

**Fase 3: Marktuitbreiding & Partnerschappen (12-24 maanden)**

* **Doelen:**
  + Uitrollen van een consulting model (scenario 3) en/of white labeling (scenario 5) om via derde partijen sneller schaal te bereiken.
  + Evalueren van de behoefte en haalbaarheid voor een volledig geïntegreerd GRC-platform (scenario 6).
* **Acties:**
  + Opzetten van strategische samenwerkingsverbanden en afsluiten van licentie-/white label contracten.
  + Uitbreiden van marketing- en salesactiviteiten gericht op zowel kmo’s als corporate organisaties.
  + Continu investeren in R&D om de innovatiekracht en concurrentiepositie te waarborgen.

**Fase 4: Consolidatie & Groei (24+ maanden)**

* **Doelen:**
  + Opschalen van de oplossing naar een volledig geïntegreerd GRC-platform indien de markt dit vraagt.
  + Continueren van innovatie en het onderhouden van een sterke concurrentiepositie door regelmatige updates en uitgebreide data-integratie.
* **Acties:**
  + Uitbreiden van het team met gespecialiseerde sales, marketing en support professionals.
  + Versterken van data governance en compliance maatregelen.
  + Bouwen aan een ecosysteem van strategische partners en tevreden klanten.

**6. Conclusie**

Ons AI-gestuurde referentiemodel voor risicodetectie en mitigatie biedt een uniek concurrentievoordeel doordat het:

* Niet alleen risico’s blootlegt, maar tevens de bijbehorende wetgevende implicaties helder maakt,
* Concrete mitigatievoorstellen geeft door te koppelen naar intermediaire standaarden en clauses op de meest effectieve & efficiente wijze (één standaard of clause die verschillende risico’s afvangt)
* Deze aanbevelingen vertaalt naar begrijpelijke taal, afgestemd op de context van de organisatie.

Door een modulaire en gefaseerde aanpak te hanteren, kunnen we snel een MVP lanceren, de markt valideren en vervolgens strategisch uitbreiden via API-integraties, plug-ins, consulting of white labeling. Deze aanpak richt zich op zowel kmo’s als corporate organisaties, en biedt daarmee een schaalbare en commercieel succesvolle oplossing in een complexe en snel veranderende markt.