Opening Statement

Interviewer:
Goedemorgen en welkom bij mijn interview. Als aller eerst wil ik u bedanken dat u bereid bent deel te nemen aan dit interview. Mijn naam is Imane Akhyar en ik ben masterstudent Information Studies aan de Universiteit van Amsterdam. Dit interview maakt deel uit van mijn scriptieonderzoek, dat ik uitvoer bij Kouters van der Meer, over hoe kunstmatige intelligentie effectief kan worden geïntegreerd in het cybersecurity-risicomanagement binnen financiële instellingen. Het interview zal ongeveer 60 minuten duren en wordt opgenomen voor onderzoeksdoeleinden. Uw antwoorden worden volledig geanonimiseerd en vertrouwelijk behandeld. U kunt op elk moment een vraag overslaan of het interview beëindigen. Heeft u nog vragen voordat we beginnen?

Respondent:
Nee, geen vragen op dit moment.

Sectie 1: Achtergrond van de geïnterviewde

Interviewer:

Q1.1: Nou eerst introductievraag, kunt u kort even iets over uzelf vertellen en jouw rol binnen de organisatie waar je werkt?

Respondent:
Ja, dat is goed. [Naam], ik werk bij [Naam bedrijf], waar jij je scriptie ook schrijft. Natuurlijk een bureau in governance, risk en compliance, voornamelijk binnen de financiële sector, maar ook daarbuiten. Al werk ik voornamelijk binnen de financiële sector, nog specifieker voornamelijk bij pensioenfondsen, maar ook andere klanten. We zijn daar gefocust op voornamelijk het IT stuk, maar bij bepaalde klanten ook breder, dus enterprise risk management. Ik heb zelf aan de UvA gestudeerd, dezelfde opleiding als jij, Information Systems als master. Daarna ben ik nu bijna twee jaar geleden fulltime aan de slag gegaan bij [Naam Bedrijf] en ja, een grote verscheidenheid aan opdrachten gehad. Dus van in de richting van beheerswerk en risicoanalyses tot DORA-implementatie: hoe moet dat in beleid terugkomen, hoe moet dat in maatregelen terugkomen? Redelijk breed. En de laatste, wat zal het zijn, de laatste paar maanden, misschien vier, vijf maanden, ben ik ook druk bezig geweest met AI: de kansen en bedreigingen binnen ons bedrijf, en ook een stukje van wat we daar bij klanten voor kunnen doen

Interviewer:
Q1.2: Oké, top. Dus je had al vermeld dat je ongeveer twee jaar daar werkt. **Is het ook zoveel jaar ervaring dat je hebt met cybersecurity, risicomanagement of AI? Of heb je bijvoorbeeld nog langer ervaring met die domeinen?**

Respondent:
Nou ja, goed, dat gaat allemaal een beetje terug naar de studie, hè. Ik heb dus de master Information Systems gedaan en daarvoor Informatiekunde, daar komen die onderwerpen ook wel naar boven. Maar qua werkervaring is het echt de twee jaar bij [Naam Bedrijf]. Iets

specifieker nog heb ik ook de CISA-opleiding gedaan, de Certified Information Systems Auditor opleiding. Daarvan heb ik het examen ook afgerond, wat nog wel relevante kennis geeft over in ieder geval het audit-stuk (de relevantie waar AI ook een plek in gaat vinden). Maar qua werkervaring: ja, bijna twee jaar.

Interviewer:
Q1.3: Oké, top. **En dan had je eigenlijk ook al genoemd de DORA en de AI Act, dus daar ben je dan eigenlijk al best wel bekend mee, de DORA en AI Act?**

Respondent:
Ja, de DORA ken ik praktisch uit mijn hoofd helaas, en de AI Act is wat nieuwer en wat vager. Maar daar zijn we nu ook gewoon druk mee aan de slag, dus daar heb ik op zijn minst een goed beeld van welke aspecten daarin terugkomen en wat de focuspunten moeten zijn. En naast de AI Act heb je voor pensioenfondsen specifiek ook de Gedragslijn AI en Ethiek voor de pensioensector, die al probeert iets meer invulling te geven aan de AI Act. Wat daar wel interessant aan is, is dat de principes die daarin genoemd worden wat mij betreft breder inzetbaar zijn dan alleen voor pensioenen.

Sectie 2: Thematische verdieping

Interviewer:
Q2.1: Dat was het dan voor de introductie. Dan gaan we nu naar de kernvragen van het framework. Het is opgesplitst in bepaalde componenten; eerst gaat het voornamelijk over de elementen zelf en de tweede over bijvoorbeeld ethiek en governance, maar dat zien we zo meteen wel. De eerste vraag is eigenlijk best wel straight-to-the-point, gaat gelijk helemaal over het framework: **op welke punten binnen het cybersecurity-risicomanagement of risicomanagement in het algemeen zie je de meeste potentie voor LLMs om toegevoegde waarde te bieden?**

Respondent:
Ja, het is vooral een heel open vraag: dus op het punt cybersecurity en IT-risicomanagement: waar liggen de kansen voor AI? Oef. Nou ja, goed. Er zijn een hoop kansen, maar dat is een beetje het probleem: er zijn een hoop kansen. Dus ik zit nu even te kijken: wat zijn de focuspunten? Kijk, wat je natuurlijk sowieso kan doen is IT risicomanagement begint eigenlijk vanuit de eigen strategie, hè. Dus wat wil je als bedrijf bereiken? En AI kan op zichzelf al helpen bij hoe je AI wilt inzetten, zeg maar. Het kan al een beeld geven van wat de best practices in de markt zijn qua technologie gebruik. Daarna zou je je eigen strategiedocument hoe dat ook terugkomt in je organisatie, weer in kunnen laden en vragen van: joh, wat mis ik misschien nog? En daarbij de soort tips krijgen voor: hoe kan je dit integreren in je strategie? Risicomanagement heeft zoveel delen. Je kan op basis van je beleidsstukken en een beschrijving van de context van je organisatie ook vragen om inspiratie: welke risico's zouden wij misschien hebben? En dan ook weer: hoe zouden we die misschien kunnen mitigeren? Dus er zijn een hoop kansen. Ik denk wel dat bij al die kansen heel belangrijk is dat je de vakkennis hebt om wat AI aandraagt fatsoenlijk te

beoordelen. Want het is er in ieder geval op dit moment nog niet zo dat de informatie altijd klopt. Sterker nog, er zijn nog heel veel hallucinaties.
Ja, ik vind dit een moeilijke vraag om te beantwoorden op de vraag “waar kan het helpen?”, want ik denk: bijna overal.

Interviewer:
Q2.1a: Oké ja, en dan als ik het over LLMs heb: **zijn er bepaalde soorten LLM die jij het meest geschikt vindt binnen je eigen organisatie?** Of waarvan je denkt van ‘oké, deze kunnen we sowieso gebruiken’. Of zijn er nog andere waarvan je denkt ‘ze zijn een twijfelgeval’?
Respondent:
En wat bedoel je met bepaalde soorten LLM, zeg maar de standaard taalmodel, of een reasoning model, of?

Interviewer:
Bijvoorbeeld GPT-4 en Claude, dat soort tools .

Respondent:
Oké. Nou, wij hebben net eigenlijk bepaald welke tools wij op korte termijn willen inzetten. Daarvoor hebben we de afweging gemaakt om ChatGPT en Claude als standaardprogramma’s te gebruiken die gewoon gebruikt mogen worden, met de context dat we nu nog geen betaalde versie beschikbaar stellen. Wat bijvoorbeeld wel weer een kans is van een Copilot, is dat wij de Microsoft-omgeving hebben, we hebben SharePoint, we hebben Teams en dat integreert super fijn met die omgeving. Dus ja, dat zou een kans zijn: dat je heel makkelijk, als je Copilot inzet, kan zeggen van ‘nou ja, al die data wordt ingeladen en het wordt super makkelijk voor collega’s om bepaalde vragen te stellen. Hebben we hier al iets voor? Kunnen we op basis van wat we hebben een template maken? Wat staat er in onze handboeken?’.
Tegelijkertijd brengt dat ook weer een risico met zich mee, namelijk dat dat toegang heeft tot alle data. En als ik het goed zeg, heeft Copilot in de basis toegang, tenzij je die toegang uitzet. Dus als je dat op een gegeven moment niet goed ingericht hebt en je hebt geheime documenten waar iedereen ineens toegang toe heeft via Copilot, dan heb je een groot probleem. En ja, dat zijn de soorten risico’s waar we dan naar kijken bij de afweging: wat zetten we in? Maar ja, op dit moment zijn wij dus geland op GPT-4, omdat dat op dit moment gewoon een heel geavanceerd model is. Maar ja, die rat-race is nog gaande, dus misschien winnen ze het niet. Claude gebruiken we voor het programmeren. En Apple Intelligence, gezien we Mac-producten gebruiken en het al geïntegreerd is, dat zijn ja, een deel daarvan kun je lokaal draaien en dat deel kan ook gebruikt worden. Dus op dit moment zijn de afwegingen daarvoor voornamelijk privacy concerns geweest: hoe maken we het zo moeilijk mogelijk om per ongeluk data erin te zetten die je er niet in zou willen zetten?

Interviewer:
FQ2.1a: En is er al zelf geëxperimenteerd met die drie die je net hebt opgenoemd , dus ChatGPT ,Claude en Apple Intelligence, of komt dat nog in de toekomst?

Respondent:

Geëxperimenteerd, ja zeker. Binnen [Naam bedrijf] wij hebben dus een team binnen de organisatie die nu al bezig is. Of nou ja, vooral bezig is met: hoe kunnen wij faciliteren dat collega's het goed kunnen gebruiken?
En nou ja, wij zijn nu al een tijdje actief aan de slag om het ook bij onze eigen werkzaamheden in te zetten en om ook wat use cases uit te proberen. Deels: wat kunnen we nu al doen? En deels ook richting de toekomst. Bijvoorbeeld: als je een risicoanalyse van een klant hebt, dat kan ik nu dus nog niet doen, want we gebruiken nu nog geen klantdata , maar als je die wél hebt, wat kun je daar allemaal mee doen? Hoe kun je dat verwerken? Hoe kun je je eigen leven makkelijker maken?

Interviewer:
Q8: Is er binnen jullie organisatie al over nagedacht om een eigen LLM te maken? Of is dat iets waarbij jullie denken 'oh, dat kunnen we misschien in de toekomst nog doen'?

Respondent:
Sowieso: om een LLM echt volledig of echt goed in te kunnen zetten, moet je klantdata ook kunnen gebruiken. Want de grootste use cases zitten wat mij betreft in het dataverwerking stuk. Of nou ja, naast de brainstormen en inspiratie opdoen, want dat kan ook gewoon zonder klantdata. AI is het daarbij ook fijn als je een specifieke situatie kan schetsen (dat kan nu ook nog niet). Maar het dataverwerking stuk helpt een hoop. Bijvoorbeeld: als je zegt "we willen verantwoordingsrapportages gaan bekijken", nou, we hebben specifieke punten waar we op letten. En daarvoor moeten we een heel document afzoeken. Als we kunnen zeggen van 'nou ja', AI doet die eerste stap, dus die punten waar we altijd op letten, daarvoor geeft hij aan: waar staat het, en wat staat er ongeveer, op een manier die controleerbaar is. Maar vooral ook: welke punten zie ik niet terugkomen?', want dan weet je dat dat je focuspunten zijn en dat je daar voornamelijk advies op kan gaan geven. Dat helpt gewoon ontzettend dat maakt het werk een stuk efficiënter. En dan kunnen we ons met onze experts meer op de inhoud bezighouden, in plaats van dat we operationeel vervelend werk doen, zeg maar.

Interviewer:
Q2.2: Oké. En als LLM-systemen worden toegepast , dus het kan door iedereen in de organisatie gebruikt worden, zijn er dan bepaalde, ja, procedures waarbij er toezicht wordt gehouden op hoe de AI-systemen (dus hoe de LLMs) worden gebruikt?
Nou ja, een deel kan je technisch inrichten, hè. Dus het is ook mogelijk om je bestanden bepaalde eigenschappen mee te geven dat je zegt: nou, dit kun je niet laden. Verder ja, het toezicht op het gebruik. Kijk, wat wij sowieso gaan doen (hoe we AI ook in gaan zetten) is regelmatig uitvragen bij onze collega's hoe het nu gebruikt wordt. En daar hebben wij het een beetje makkelijk in, want wij hebben een team van twintig man. Ja, we hebben gewoon hele korte lijntjes en we zien hoe mensen het gebruiken; bij een grote organisatie zou dat een stuk lastiger zijn. Dus ja, wij hebben feitelijk de luxe dat we al meer zicht hebben op hoe het gebruikt wordt. We hebben nog niet gekeken naar of we een betaalde versie gaan inzetten of we dan ook inzicht hebben in de prompts en in welke data er gebruikt wordt. Dat zou ik eigenlijk niet weten; op zich wel interessant. Maar ja, inzicht in de prompts zou ik persoonlijk alweer een beetje eng vinden. Want ja, ik hoef ook niet van mijn collega's te zien wat ze op hun werk computer op Google zoeken dat vind ik heel invasief. Ik denk niet dat je zó ver moet gaan.

Interviewer:

Q2.4: Je had net ook over privacy, dus dat is een van de concerns. Zijn er nog andere risico's die je ziet bij het inzetten van LLMs, bijvoorbeeld bias, discriminatie of foutieve classificatie, waar een organisatie sowieso tegenaan kan lopen?

Ja, 100%. Nu heeft de wereld natuurlijk. Ja, privacy is één, kwaliteit is een tweede. En als je kijkt naar bias, ja, elke LLM is getraind op bepaalde data, en ook niet getraind op andere data. In de informatiesector (zal ik het even noemen) is een probleem dat data op zichzelf ook al gekleurd is. Bepaalde personen met bepaalde eigenschappen zullen meer meegenomen worden in data. Je ziet dat ook in de zorg bijvoorbeeld: dat bijna alles in het verleden op mannen is getest en heel weinig op vrouwen, waardoor we gewoon een stuk minder weten over hoe vrouwen behandeld moeten worden. Ja, dat is met alle data zo. We hebben geen gegeneraliseerde datasets, dus er zijn ook geen LLMs die getraind zijn op volledig gegeneraliseerde datasets. Dus bias is er. Nou, dat is überhaupt altijd inherent aan AI maar zeker met de data die beschikbaar is in de wereld. Dat is er gewoon, en dat is iets wat je super goed moet begrijpen wanneer je AI inzet. Wat ook wel interessant is: de AI Act geeft nu al aan dat, wanneer je AI inzet binnen je organisatie, je ervoor moet zorgen dat de mensen die het gebruiken voldoende AI-geletterd zijn.

Nou, dan is de vraag: wat is "AI-geletterd"? Daar is één definitie voor, die is nog een beetje breed. Maar het geeft wel aan dat je de systemen veilig kan gebruiken, weet hoe het werkt, en op basis waarvan jouw output tot stand komt. Daar komt het eigenlijk op neer. En ja, ik vind dat een deel daarvan ook is dat je dus begrijpt, nou ja, die bias zit erin, en die controle moet daar dus ook op blijven. Het blijft belangrijk. Ik denk dat het heel moeilijk gaat worden, zeker met die LLMs pakken feitelijk gewoon alle data waar ze hun handen op kunnen leggen, en de meeste data is gekleurd. Dus die bias zal gewoon blijven, en dat gaat heel lang duren om dat terug te dringen. Dus voor nu is het belangrijkste dat je je daarvan bewust bent en ook actief gaat kijken of je daar rekening mee moet houden in de output die je krijgt en wat je ermee doet.

Interviewer:

Q2.4a: Ja, ik had ook nog een vraag over de menselijke controle. Er zijn natuurlijk bepaalde beslissingen die een AI kan nemen, en de één zegt van "oké, dat kan volledig geautomatiseerd worden" en de ander niet. **Vind jij dat er dan bij elke output nog steeds menselijke controle nodig is, of dat bepaalde beslissingen volledig geautomatiseerd kunnen worden, dus dat het dan eigenlijk niet meer nodig is dat nog iemand (gewoon een human executive) het even checkt? Dus als je een LLM gebruikt?**

Respondent:

Nou, het verschilt per situatie. Kijk, in de basis vind ik: ons vakgebied is een vakgebied van expertise. Wij adviseren klanten over hoe je dingen het beste aan kan pakken, en alles vakinhoudelijke moet wat mij betreft gewoon nog steeds door mensen gecontroleerd worden, ook met het vier-ogen-principe. Zo doen we dat nu ook. Als ik een eindproduct oplevert aan een klant (stel, ik doe een opzet voor een beleid), dan doe ik dat niet in m'n eentje; dan kijkt er iemand mee. Als AI daarbij helpt, dan is het allereerst belangrijk dat ik ernaar kijk of ik het eens ben met wat de AI zegt. En daarna kijkt alsnog iemand mee, dus dat verandert niet. Kijk, als je het hebt over dingen als chatbots, ja, inherent zit daar geen controle meer op, want dat is gewoon AI die direct met een eindgebruiker praat. Dus op zich valt dat te automatiseren. Zelfs dan denk ik dat je een uitwijkmogelijkheid moet hebben, zodat er nog wel mensen aan te pas kunnen komen. En ja, er zitten ook weer bepaalde

risico's aan. Je ziet bijvoorbeeld dat heel veel chatbots die nu al worden ingezet gewoon nog niet zo goed zijn, terwijl het wél zou kunnen als je ze bepaalde bronnen meegeeft en je laat een GPT met de klant praten. Dan zou dat al best een eind komen. Maar dat zou ook de deur weer openzetten dat zo'n GPT iets zegt wat helemaal niet klopt, uit naam van het bedrijf. Ja, of dat mensen gaan proberen om die GPT iets raars te laten zeggen en dat 'ie ook echt gevaarlijke dingen gaat zeggen en dat willen bedrijven niet. Dus wordt het heel erg beperkt. Het is te automatiseren, maar daar komt weer een bepaald risico bij kijken. En dat risico moet je afwegen en kijken of je het kunt accepteren. Anders moet er nog iets tussenkomen.

Interviewer:
Q2.5: Ik vroeg me af: hoe gaan jullie eigenlijk om met de data die je zelf invoert in AI-tools, zoals LLMs? **Wordt er gekeken of die data aan bepaalde voorwaarden moet voldoen voordat je 'm gebruikt, bijvoorbeeld om bias te beperken? Of zijn daar nog geen echt duidelijke regels voor binnen jullie organisatie?**

Respondent:
Ja, vooralsnog niet. Ik vind het wel een interessante vraag. Kijk, in principe is de manier waarop we er nu naar kijken ook een beetje meer van: uiteindelijk wil je data beschikbaar gaan stellen. Er zit een deel in "wat mag je niet gaan gebruiken" en een deel "wat mag je wél gaan gebruiken". En het punt "wat mag je wél gaan gebruiken" ja, op termijn zal dat waarschijnlijk meer worden. Waarschijnlijk dat er gewoon in de algemene voorwaarden (wanneer we de opdracht aangaan met de klant) staat dat wij bepaalde classificaties aan data mogen gebruiken. Ik denk dat het lastig gaat worden om te zeggen dat je eigenlijk eerst een checklist langs moet voordat je een document in AI stopt, want het moet wel laagdrempelig genoeg blijven dat het de efficiëntie bevordert. Als je voor elk document dat je erin wilt zetten een checklist af moet gaan nou, dat maakt het een stuk lastiger. We werken met mega-veel bestanden die we continu weer van klanten krijgen. Dus ook als je van elk bestand dat binnenkomt gaat zeggen "Nou, we gaan het van tevoren bekijken of het voldoet" dat is lastig. Zeker met iets als bias; dat is eigenlijk niet te automatiseren, dat zou je handmatig langs moeten gaan.
Dus ik ben bang dat het voor ons onrealistisch is om te zeggen "het moet aan bepaalde bias-voorwaarden voldoen". Maar ja, wat ik ook zeg: ik denk dat je die bias altijd houdt, en dat is niet per se AI-specifiek trouwens. Dat is nu ook al zo in elke organisatie, die bias zit er op een bepaalde manier in. Dat is over het algemeen niet bewust. Het beste wat je kan doen, is je er wél bewust van zijn en ook af en toe bij jezelf de vraag stellen van "hé, wat is de bias waar we nu mee werken en moeten we daar niet wat mee?". Ja, voor AI specifiek volgt het een beetje de organisatie zelf, denk ik. En om echt een checklist langs te gaan, lijkt me moeilijk.

Interviewer:
Q2.6: En als het gaat om het gebruik van LLMs: zijn er bij jullie ook al duidelijke afspraken of richtlijnen over hoe je ermee mag werken? Bijvoorbeeld over dingen zoals prompt filtering of modeltraining, weten collega's wat wel of niet kan, of is dat nu nog een beetje grijs gebied binnen de organisatie?

Respondent:
Ja, het staat voor ons nog een beetje ver weg, denk ik. We zijn nog in de verkennende fase, waarbij stap één eigenlijk is om überhaupt collega's aan te moedigen om AI te gebruiken. En wij hebben daar dus wel een training in gedaan en dat blijven we ook doen met "hoe kun je dat het beste doen?". We hebben net de eerste training gehad en over een maand gaan we weer een meer praktische training doen, waarbij we ook gebruik-cases en meer voorbeelden gaan geven van "kijk, zo kan je het ook aanpakken". We hebben nu geen plannen om te beperken hoe er geprompt mag worden, behalve dat we onderling wel hebben afgesproken dat prompts niet herleidbaar mogen zijn naar klantsituaties of specifieke klanten.

Interviewer:
Q2.3: Ik had nog een vraag over regelgeving en governance. Regels zoals de AI Act, GDPR en DORA veranderen natuurlijk ook in de loop van de tijd. Hoe gaan jullie daarmee om als organisatie, zeker als je kijkt naar de inzet van LLMs in de toekomst?

Respondent:
Bij de meeste organisaties, zeker in de financiële sector, is er een compliance officer die verantwoordelijk is voor het bijhouden en toepassen van wet- en regelgeving. Dat is bij ons ook zo. Als er iets verandert in regelgeving, zoals met DORA of nu met de AI Act, dan pakt die persoon dat op. Er komt naar mijn verwachting geen apart team voor AI-compliance; het wordt gewoon opgenomen in de bestaande compliance-structuur.

Wat er dan gebeurt, is eigenlijk vrij standaard: er wordt gestart met een gap-analyse. Dus: wat zegt de nieuwe regelgeving precies, in hoeverre voldoen we daar al aan, en wat moet er nog worden aangepast in beleid of processen? Als dat is gedaan, wordt via interne audits gecontroleerd of alles ook echt wordt nageleefd. Die structuur ligt er al, die hoeft niet opnieuw te worden uitgevonden voor AI. Je hebt feitelijk de 'Run' en de 'Change'. Run is wat je standaard doet in de organisatie: daar start het proces bij Risk Identification & Assessment, want dat staat jaarlijks ingepland.

Kijk je vanuit Change, dan is er een trigger, bijvoorbeeld een wetswijziging, waardoor we een project moeten starten om onze werkwijze aan te passen. Je wacht dan niet op de reguliere risicoanalyse; je vraagt meteen: wat moeten we nu doen om aan de nieuwe eisen te voldoen?

Interviewer:
Q2.7 en Q2.8: Tot slot nog een vraag over het framework zelf: wat zou jij nodig hebben om echt vertrouwen te hebben in een AI-framework voor cybersecurity-risicomanagement? Denk je dat de elementen die er nu in staan voldoende zijn, of mis je nog onderdelen? En hoe zou zo'n framework volgens jou idealiter getoetst of in de praktijk verbeterd moeten worden?

Respondent:
Wat ik nodig zou hebben om echt vertrouwen te hebben in het framework, is dat het de volledige keten van risico-identificatie tot risicobehandeling duidelijk en logisch in kaart brengt. In het onderdeel Risk Identification & Assessment geef je nu al een paar heel

specifieke voorbeelden van hoe AI wordt ingezet, maar dat is volgens mij maar een klein stukje van het verhaal. Ik mis nog een stap terug: welke eigenschappen van AI vragen extra aandacht bij de risico-identificatie? Vanuit die analyse bepaal je vervolgens welke risico's voor jouw organisatie relevant zijn en welke maatregelen je moet nemen om die te mitigeren.
Die maatregelen geven dan weer invulling aan de wet- en regelgeving die juist is opgesteld om grotere, meer algemene risico's te beperken.
Met andere woorden: tussen je risico-identificatie en je wettelijke verplichtingen zit nog een laag waarin je de vertaalslag maakt naar organisatie-specifieke controls.
Natuurlijk geven wetten als de AI Act of DORA richting, maar uiteindelijk is het je eigen risicoprofiel dat bepaalt wat je nodig hebt. Dat onderscheid zou wat mij betreft duidelijker zichtbaar mogen zijn in het framework.

Daarnaast zou ik ook aanraden om iets op te nemen over het type LLMs dat je waar inzet. Niet per se een lijstje van specifieke tools, die veranderen toch continu, maar meer op hoog niveau. Bijvoorbeeld: waar gebruik je een general-purpose model, waar juist een reasoning model, en in welke context is een retrieval-based model geschikt? Dat soort richting helpt om het framework concreter en toekomstbestendiger te maken.

Als laatste zou ik het stukje educatie toevoegen. Als het framework die volledige samenhang tussen risicoanalyse, mitigatie, governance en inzet van de juiste modeltypes duidelijk maakt, dan zou dat voor mij echt het vertrouwen vergroten.

Afsluiting:
Dat brengt ons bij het einde van het interview. Nogmaals hartelijk dank voor uw tijd en het delen van uw inzichten, dit is enorm waardevol voor mijn onderzoek. Zoals eerder aangegeven wordt alles volledig geanonimiseerd en vertrouwelijk behandeld. In de tweede week van juni ontvangt u nog een korte Google Survey, waarin ik het definitieve AI-framework presenteer en enkele aanvullende validatie vragen stel. Op die manier kunt u aangeven of het framework overeenkomt met uw praktijkervaring en of er nog punten ontbreken.

Mocht u daarnaast graag een samenvatting van de bevindingen willen ontvangen zodra de scriptie is afgerond, laat het me vooral weten, dan stuur ik die graag toe!