Rico Schilder
De eerste vraag is, is het correct? Of zie je fouten erin waarvan je denkt, nou dit, dit zou toch anders moeten?

Participant 1
Nou ja, toen ik het doorlas, hè? Ik had eventjes een paar dingen die ik wilde aanstippen, hè? Als je bij punt 1.2.2 over de ethical requirements. Daar spreek je op gegeven moment heel expliciet over IT risk management. Die kon ik even niet plaatsen ten opzichte van gewoon de interne console frameworks.

Rico Schilder
Ja IT risk, dat is het domein van mijn scriptie.

Participant 1
Maar die had ik even niet door, want dan zou je ook over, hè? Consequent over een IT control framework kunnen spreken in plaats van een internal control framework.

Rico Schilder
Dat is een goeie misschien.

Participant 1
Nou ja, voor de rest. Ik weet dat we het in ons vorige interview geraakt hebben, maar als je mij nu vraagt en ik kijk gewoon puur naar die Flow Charts hè, dan zie je in je noemde het net ook die verschillende AI types. Dan zie je eigenlijk dat er maar twee AI types worden gebruikt. En ik kan niet heel goed uitleggen wat dan echt het verschil is tussen NLP en Generative AI. En, volgens mij hebben we het ook gehad, en ik weet niet of je een bewuste keuze dan hebt gemaakt om het niet op te nemen, maar voor risk identification kan je inprikken op verschillende datastromen. En dan krijg je echt gewoon een beetje de klassieke AI. Hieronder, machine learning en et cetera van hoe hè en anomaly detection. De trend identificatie, patroon identificatie. Want als jij op een gegeven moment in je op bepaalde IT assets hè? Enorm veel incidenten ziet of opeens heel veel vulnerabilities ziet of opeens hè, in je security incidenten en je event monitoring tools zie je van buitenaf dat er bepaalde IT assets enorm worden aangevallen. Dan kan dat natuurlijk zijn, hè dat dat het risk exposure voor bepaalde IT assets opeens toeneemt. En dat kan toch een trigger zijn, hè? Om in ieder geval je risks en respons te herzien. Dat is anders dan vanuit je doelstellingen beredeneren hè? En dat kan natuurlijk heel goed met generative AI van ja, kijkend naar deze strategie, missie, visie, doelstellingen, hé, wat zouden dan mijn risico's kunnen zijn? Ik denk dat dat altijd van top down beredeneren en bottom up van wat zie ik nou echt in de praktijk gebeuren en dat dat uiteindelijk krachtig is om dat bij elkaar te brengen?

Rico Schilder
Oké. Top. Ik kan me ook wel herinneren dat we het daar de vorige keer inderdaad ook over hadden.

Participant 1
En even kijken verder had ik bij een punt 2.2.2 hè, dus dat is die requirements application. Ja, dit was wel een enorme opsomming waarvan ik dacht van, is dit niet handiger te? Ik lees

het door maar op een gegeven moment stop ik met lezen, want het gaat er bij mij niet in. Ik denk dat het toch handiger is om dit in een tabelstructuur te presenteren.

Rico Schilder
Ja, dat is wel een goeie.

Participant 1
Waarbij je kort even de requirements herhaald. En dan kan je het ook echt valideren. Klopt dit nou of niet meer? Op deze manier kan ik het echt niet valideren.

Rico Schilder
Ja ja, want de volgende vraag is inderdaad: is het high level design duidelijk?

Participant 1
Nou dat dus niet.

Rico Schilder
Ik denk dat ik dat ook wel ga doen inderdaad, want dat klinkt eigenlijk wel een stuk beter. Zijn er nog andere dingen die onduidelijk geformuleerd zijn?

Participant 1
Nou ja, voor de rest vond ik het juist wel een prima leesbaar stuk en ik vond vooral het plaatje dat spreekt goed en ik denk, hè, om het duidelijker te maken wel wat ik al aangeef hier en daar. En ik denk dat je vanuit de input van literatuur en je gesprekken een bepaald abstractieniveau erin hebt geprobeerd te zoeken, waardoor het misschien te abstract is geworden, waardoor je inderdaad met wat we net zeiden met een aantal voorbeelden het weer wat sprekender kan maken. Het is dus danig abstract geschreven dat het nog veel meer kan omvatten, dan denk ik dat dat een paar voorbeelden wel een elegante oplossing is.

Rico Schilder
Dan had ik nog de vraag, is het compleet?

Participant 1
Ja, je had volgens mij heel expliciet al opgemaakt of ergens vastgelegd dat objective setting dat je dat bewust niet had opgenomen in die flow hè, dus dat maar dan heb je in ieder geval uitgelegd. Ik moet zeggen dat ik wel heel even zat te kauwen op portfolio development.

Rico Schilder
Dat is een term die is overgenomen uit COSO 2017. Dat stond dan weer niet in het stuk wat ik je heb gestuurd inderdaad. Dat wordt in mijn literatuuronderzoek toegelicht.

Participant 1
Maar dan wordt het elders toegelicht, oké?

Rico Schilder
Maar misschien is het een goeie om dat nog even te verduidelijken in het figuur.

Participant 1
Ja, ik zat nog te denken, want tussen de input en output zit AI. En er zit tussendoor een soort high level prompt die je eventueel nog zou kunnen neerzetten. Bijvoorbeeld, bij de eerste stap “identify risks based on strategy and objectives”. En bij die tweede een andere prompt. Maar dan gaat het vooral voor de lezer even om die mee te nemen in de aanpak van aan de slag gaan. Want je input staat er, maar wat stop ik er nou nog meer in? Als ik een aantal documenten upload in ChatGPT, dan gebeurt er nog niks. Ergens moet ik het model iets meegeven, en dat staat wel in je requirements. Een gebruiker moet goed kunnen prompten, maar wat zou nou het start prompt kunnen zijn? Want uiteindelijk wil je het model voeden zodat hij de risk assessment ook gaat doen. Want je hebt het over assessment results, maar wat houdt dat in?

Rico Schilder
Nou dat ligt eraan. Dat kan in kwalitatieve vorm zijn of in kwantitatieve vorm. Het kan een stukje tekst zijn, maar ook een matrix met impact en kans. Maar een organisatie kan daar ook gewoon zeggen wat de eventuele gevolgen zijn als een bepaald risico voorkomt. Dus in die zin hangt dat heel erg af van hoe de organisatie dat wilt documenteren, en hoever je daarop ingaat.

Participant 1
Mag je naast de 10 pagina's nog een bijlage erbij doen met heel veel tekst?

Rico Schilder
Niet met heel veel tekst. Nee hoezo?

Participant 1
Nou, ik zou het wel gaaf vinden als je bijvoorbeeld de werking hiervan aantoont. Bijvoorbeeld een simpele powerpoint waarbij je laat zien wat er gebeurt als je een missie, visie, strategie en een aantal doelstellingen uploadt in ChatGPT en dan prompt. Identificeer de risico’s. En dan de output daarvan weer input en prompt naar de risico assessment. En ik denk dat je dan best wel goede resultaten krijgt waarmee je in de basis aan de slag mee kan. En dan kan je dat in de bijlagen zetten en ernaar verwijzen. En dan in het plaatje laat je zien wat je in de praktijk ook hebt gedaan. Ik heb als input deze documenten gedaan, en toen een high level prompt gegeven en het zo gedaan. En ik heb deze AI gebruikt en de output was dit en die heb ik vervolgens weer meegenomen naar de volgende stap.

Rico Schilder
Ja exact. Het zou wel interessant zijn om dat te kunnen toevoegen en uitproberen. Maar ik ben bang dat ik daar niet meer mee wegkom. Het zou niet passen in mijn scriptie. Maar het zou wel cool zijn en ook vooral een goede vervolgstap zijn.

Participant 1
Ik denk dat het dan vooral gaver zou worden om door te lezen. Daar gaat het vooral om.

Rico Schilder
Want het zou wel cool zijn inderdaad. Dan ik nog een paar vragen? Wat verwacht je exact per stap als output? Klopt dat een beetje wat hier zo staat? Of hoe zou ik dat voor me moeten zien?

Participant 1
Ja, op zich klopt dat.

Rico Schilder
Ik probeer voor mezelf een beetje een concreet beeld te krijgen van wat er per stap uiteindelijk nou uitkomt.

Participant 1
Ja, wat je zelf net al aangaf. Dat is afhankelijk van hoe je het als organisatie zelf wilt hebben. Daar worstelde ik ook al mee. Hoe wil je die assessment results hebben? Je kan het kwalitatief doen of kwantitatief. Het hangt ervan af wat je meegeeft. Bij ORGANISATIE A hebben we een risicomatrix van 5 bij 5. En dan hebben we handvatten meegegeven over hoe je die assen moet interpreteren. Want wat versta je onder hoge impact? Dat kan je financieel uitdrukken, of organisatie impact, media aandacht, klanttevredenheid, continuïteit. Dus we hebben daar een soort richtlijnen voor meegegeven. En die gaan over hoe je die assen moet interpreteren. Misschien kan je dat nog ergens benoemen als input voor de risk assessment. Maar misschien moet dat ook weer op een bepaald abstractieniveau.

Dan moet je dat ICF trouwens wel als input meegeven, want is dat niet, hè? Uiteindelijk wil je tot een ICF komen, toch? Want de laatste stap is je output, maar die ja, die pijl terug is weer je input, zeg maar dus.

Rico Schilder
Ja maar. Het moet zo kunnen zijn dat je wel kan itereren over het hele proces, zeg maar. Dus vandaar de pijl. Dan kan het ICF aan het begin als input worden meegegeven.

Participant 1
En er zit tussen de output en input nog een input van de gebruiker. Dus je hebt een requirement over de validatie van de gebruiker, maar die moet ook ergens terugkomen. Dus stel je voor dat je een lijst met 10 risico's hebt staan en een paar zijn niet relevant en een paar moeten aangepast worden, dan is dat ook input voor de volgende stap. Dus dat je dat expliciet ergens erin zet, misschien met een bolletje of een driehoekje waarbij je de results update.

Rico Schilder
Ja. Misschien even een poppetje of zo ertussen.

Participant 1
Hé, je user validation of results en dan eigenlijk is dat dan weer de input voor je volgende stap.

Rico Schilder
Juist. Ja, dat is een hele goeie inderdaad.

Participant 1
Want je hebt je assessment results in termen van kans en impact en risico en ik zie mezelf dan alweer schreeuwen tegen ChatGPT. Je hebt het risico te hoog ingeschat. Het moet lager. Dat is te laag ingeschat. Kan je beargumenteren waarom je dit risico als volgt hebt ingeschat? Dan ben je iteratief bezig met je risico assessment resultaten te krijgen zoals jij denkt dat ze goed zijn. En dan ga je naar de volgende stap.

Rico Schilder
Ja juist, want nu lijkt het inderdaad alsof je het gewoon accepteert en doorgaat naar de volgende stap, terwijl dat niet zo is inderdaad.

Participant 1
Nu kan je druk op de knop met deze input documenten en dan kan je tot de laatste stap doorgaan. Misschien komt er wel wat uit. Maar ergens denk ik dat er dan stappen niet goed gaan. En dat zou als vervolgstap helemaal interessant zijn. Dan kan je laten zien wat het verschil is tussen als je met user interference werkt en zonder user interference. En met user interference interacteer je dan een aantal keer met het model.

Rico Schilder
Ja. Nou, dat is heel goed voor vervolgonderzoek. Zou je eerder kiezen voor een open source model of een betaalde versie als je zou moeten integreren in zo'n systeem?

Participant 1
Ja, dat hangt ervan af wat de voorwaarden zijn. Als je van ChatGPT de open variant vergelijkt met de betaalde variant. De betaalde variant geeft je weer wat extra zekerheden dat je input data ook alleen voor jou is. En bij de open variant accepteer je eigenlijk dat het model verder wordt getraind op basis van jouw interacties en jouw input in het model. Maar, mits de voorwaarden goed zijn, is open source beter.

Rico Schilder
Ja. En dat is zodat het model verder kan trainen?

Participant 1
Ja. Daar gebruik je inderdaad de kracht van anderen. Het model is niet eenzijdig getraind, alleen maar op basis van hoe je eigen organisatie ermee omgaat. Maar dat weet ik verder niet zo goed.

Rico Schilder
We hadden het eerder al over hoe je prompt. En je zei dat je zelf vaak prompt door veel te vragen en dat ding te commanderen. Is dat de beste manier, of?

Participant 1
Nou ja, op die manier leer je. Dat is vaak je eerste interactie daarmee. En dat is ook hoe je een initieel prompt vormgeeft. Want als ik eerst aangeef dat hij de risico’s moet identificeren. En ik krijg de risico omschrijvingen te zien van een half A4'tje. Dan ga ik misschien wel zeggen dat het te kort en bont geformuleerd is. En daarna vind ik misschien de schrijfstijl te frivool en wil ik het zakelijk, kort en bondig hebben. En daarna wil ik de risico’s in oorzaak en gevolg hebben geformuleerd. Maar de volgende keer dat ik met risico identificatie aan de

slag ga weet ik direct wat ik kan zeggen bij die stap. Ik wil dat je de risico's kort en bondig in maximaal 3 regels zakelijk geformuleerd in termen van oorzaak en gevolg formuleert. En dan kan ik misschien die prompt wel opslaan voor de volgende keer. Deze organisatie wil altijd op deze manier zijn risico's geïdentificeerd hebben. Dus het is in eerste instantie een beetje uitvinden. Hoe formuleert het AI model wat je gekozen hebt van nature? En hoe moet ik vervolgens prompten op een manier dat het altijd in jouw gewenste stijl terugkomt?

Rico Schilder
Oké. Dus het is vooral zelf een beetje leren hoe je ermee om moet gaan? En hoe je dat het beste kan aanpakken? Dus door gewoon veel te prompten en te experimenteren.

Participant 1
Ja, maar dat is als je blanco begint. Als je uiteindelijk een ICF hebt met risico's en controls, dan kan je natuurlijk prima zeggen dat het model de risico's moet identificeren en moet formuleren in dezelfde stijl als de rest. Dus dat is als je in de volgende iteraties zit.

Rico Schilder
Wie exact zouden gebruikers zijn van het systeem dat omschreven is in het high level design? Dus wat voor een persoon is dat?

Participant 1
Wie is de gebruiker binnen de organisatie? Ik denk van nature dat dat de tweedelijns functies zijn. De risk- en compliance functies en de risk- en control functies. Maar ik zou het mooi vinden als het model breder beschikbaar is, waardoor het ook gewoon tussen de business en de eerste lijn zelf gebruikt gaat worden. Zodat zij ermee kunnen sparren. Zo iemand staat dan voor een vraagstuk voor een project en wilt eventjes nadenken over de risico's die er zijn. En die wil even actief het risicomanagement in en even met zo'n model aan de slag gaan. Maar dat conflicteert wel een beetje met je requirements natuurlijk. De gebruiker moet niet te veel gaan vertrouwen op de output. Het model is dan beschikbaar gesteld binnen de organisatie en die heeft gezegd dat dit de risico's zijn, maar die heeft me niet gewezen op andere risico's dus daar heb ik geen maatregelen op getroffen. En dan loopt het allemaal in de soep. En wie zijn schuld is dat dan? Dat ligt niet aan mij. Een van de developers kwam naar me toe en die vertelde dat ze zelf niks mogen installeren op hun laptops. Maar soms is dat nodig voor bugfixes, op bijvoorbeeld Firefox. Dus hij vroeg of ze Firefox mochten installeren, want dat hadden ze niet op de machine staan. Mag dat vanuit een risicomanagement perspectief? Ik zei dat hij eerst aan ChatGPT moest vragen wat de eventuele risico's ervan zijn, en daarna terug moest komen. Dan valideer ik het wel. Dus dat zou heel mooi zijn, als je dat model beschikbaar stelt aan de organisatie om zelf snel inzicht te krijgen. Dat ze zelf ook al mee kunnen nadenken, mits gevalideerd door mensen die er echt verstand van hebben. Dus het gebruik zou je juist veel breder willen hebben, denk ik, dan alleen de risk functies. Mits een goede governance in de juiste checks en balances binnen de organisatie aanwezig is.

Rico Schilder
Zijn er verschillen als die gebruiker intern of extern is?

Participant 1
Ja, intern extern. Ik denk dat het een interpretatie is van de vraag of je beschikking hebt over alle documentatie als je extern bent. Ik ben externe accountant of consultant, en ik kom bij een klant. Hoe moet ik die dan helpen, of moet ik die controleren? Hoe maak ik dan gebruik van het systeem? Dat is afhankelijk van de input documentatie die tot je beschikking is. Kan je aan je opdrachtgever aantonen dat je het goed doet en op een verantwoordelijke manier gebruikt? Ik denk dat dat het key verschil is.

Rico Schilder
Zou zo'n systeem als omschreven in het high level design goed genoeg zijn voor jou om te gebruiken?

Participant 1
Ja, deze vraag hangt heel erg samen met de dingen die we besproken hebben.

Rico Schilder
Ja juist. Nou, helemaal goed. Bedankt voor de validatie. Tot ziens!