Interviewee 3
Ik ben Carl Cooper en ik werk bij de Kern IT processen. Dat is eigenlijk een soort beleidsclubje van ORGANISATIE C. Wij schrijven beleid voor IT beheersing en IT processen. Ik ben nu bijvoorbeeld bezig met de major internet management proces inrichting. Voor DORA, ik weet niet of je dat kent. DORA is een wetgeving die op ons afkomt, en daar hebben we van alles voor moeten doen. We hebben daar ook een soort tracker rol in, om dat te vertalen naar een praktische inrichting. Dus daar werk ik. Ik heb bedrijfseconomie gestudeerd, maar altijd al de trek naar IT gehad, dus toen ben ik gaan werken op de afdeling interne controle. Toen al heel snel de IT audit opleiding gaan doen, dus ik ben IT auditor, en ik sta in het register ook. En later ook een jaar of 6 a 7 interne IT auditing gedaan bij ORGANISATIE C. Dus ik werk al een tijdje bij ORGANISATIE C. Inmiddels al dik 15 jaar bij ORGANISATIE C, en sinds een jaar of 7 aan de IT kant, zo te zeggen. Dus dat is een beetje mijn achtergrond. Veel risk management, veel bezig geweest met implementatie, hoofd kwaliteitsmanagement geweest, veel bezig geweest met de inrichting van pipeline en advisering over hoe je dat beheerst kan doen. Dus dat een beetje.

Rico Schilder
Oké, top gaaf.
Ja, mijn onderzoek gaat dus over de implementatie van AI bij het opstellen van een controleraamwerk en vooral ook de implementatie van een controlewerk. Dus laat ik met de eerste vraag beginnen. Ben je een beetje bekend met AI?

Interviewee 3
Nou, in de zin van, ik gebruik het zelf heel graag, dus ChatGPT gebruik ik veel, Bing, en ook al een tijdje die, als presentaties maak, laat ik de afbeelding genereren. Dat vind ik leuk om te doen. Maar hoe het precies werkt op de achtergrond? Ik heb er wel eens presentaties over gehad met nodes en die hersen dingen. Ik weet niet eens meer hoe het heet. Dus ik heb enig idee hoe het werkt en ik ben er zeker in geïnteresseerd, maar ik ben niet technisch onderlegd. Dus ik zou het niet kunnen nabouwen ofzo.

Rico Schilder
Nou, het maken van zo'n controleraamwerk of het integreren daarvan. Dat is een proces dat uit een aantal stappen bestaat, een aantal activiteiten, en dan zal ik heel even een venstertje delen, want ik heb een aantal stappen geïdentificeerd in literatuur en dat zijn deze stappen: risico identificatie, de ernst beoordeling, de prioriteit beoordeling, dan een risicobeheersing of een respons opstellen, en dan uiteindelijk ook het rapporteren van al die stappen.

Interviewee 3
Ja.

Rico Schilder
Klopt het een beetje?

Interviewee 3
Ja, zeker als je naar theorie kijkt, wel. Alleen in de praktijk zie je dat er heel veel best practices op de markt zijn waar je, zeker voor IT, informatie uit kunt halen, zoals COBIT. Dat is voor mijn branche mijn belangrijkste bron geweest voor het maken van het risico framework, omdat we eigenlijk al over deze dingen hebben nagedacht voordat je daarmee

gaat starten. Dus COBIT, maar ook NIST en ISO zijn wel raamwerken die eigenlijk dit voorwerk al gedaan hebben. Dit ben ik misschien vergeten te noemen, maar in 2019/2020 hebben wij de het key control raamwerk van ORGANISATIE C opgezet en geïmplementeerd. En eigenlijk was het de belangrijkste bron voor mij COBIT en heel veel kennis vanuit het verleden wat je eigenlijk al weet. Bijvoorbeeld: back up. Je weet gewoon dat de maatregel 'back up' nodig is, en dan hoef jij geen risico identificatie voor te doen. Je kunt altijd wel die risico's er aan koppelen, want je weet gewoon dat als je niet bij kunt, dat je informatieverlies risico er is. Als je hem heel netjes zou willen doen, zou je hem deze stapjes moeten volgen, maar in de praktijk werkt dat net iets anders, want dan weet je gewoon dat bepaalde maatregelen er gewoon in moeten zitten en dan blijft er een restrisico over, zeker voor die prioriteitbeoordeling. Dus wat is nou echt belangrijk voor ORGANISATIE C? Wat is nou echt belangrijk voor nu? Dus daar zit dan vooral die afweging in. Welke doen we, welke controles nemen we wel op? Welke controles nemen we niet op? Die blijft wel denk ik. En die risicobeheersing en respons, dan maak je zoveel mogelijk gebruik van de bedachte raamwerk dingen die er al zijn, want je kunt het zelf opnieuw gaan uitvinden, maar er zijn wel veel knappe koppen daarover nagedacht en daar maak je dan gebruik van.

Rico Schilder
Oké, dus wordt eigenlijk voornamelijk in de praktijk gewoon gebruik gemaakt van al die bestaande raamwerken.

Interviewee 3
Ja en die moet je natuurlijk wel doorvertalen naar de praktijk en de werkelijkheid van je organisatie, hè? Dus de control objectives noemen we dat dan, de leerdoelstellingen die heb je dan. Alleen hoe doe je dat dan in de praktijk bij je organisatie? Met welke technologie doe je dat en hoe past die controle objective op die technologie? En dan ga je daar vervolgens fijnslijpen, dus je hebt de why, de what, en de how. De why en de what kun je wel uit het risico framework halen, maar dat how niet. Die moet je zelf bedenken en toepassen en dan moet je in gesprek gaan met engineers. "Dit is de bedoeling. Dit is het doel zo, dit willen we bereiken. Hoe zou je dat kunnen doen in de technologie?" Liefst zoveel mogelijk geautomatiseerd natuurlijk.

Rico Schilder
Ja oke top, dus in principe zullen sommige van deze stappen wat minder spelen als je hem gaat implementeren, je raamwerk?

Interviewee 3
Ja. Klopt.

Rico Schilder
Ja oke top. En welke onderdelen van het proces zijn dan eigenlijk het meest intensief? En dat kan zijn door tijd of moeite die erin gaat.

Interviewee 3
Ja, dus de opzet is vrij makkelijk. Dus wat ik net ook al een beetje zei. Het is veel hergebruik van bestaande dingen. Je hebt binnen een dag een lijstje met je blaadje controls, je controleraamwerk. Maar vervolgens de vertaling naar de praktijk. Dat is het lastigste. En afstemming met je stakeholders. Daar gaat gewoon de meeste tijd in zitten.

Rico Schilder
Omdat het heel erg contextgebonden is?

Interviewee 3
Ja, het is maatwerk. Je moet voor elke technologie, en we hebben nogal wat technologieën en applicaties, elke applicatie is weer anders en elk platform is weer anders en daar moet je mee omgaan en kijken hoe je daar invulling aan geeft. En ook al die platformen en applicaties, maar zeker platformen, zoals AWS en ServiceNow. Al dat soort platformen en hebben allemaal weer best practices, hoe die vertaling gemaakt zou kunnen worden. Die link zou AI wel kunnen leggen wellicht. Ja, daar gaat wel de meeste tijd in zitten en wij hebben ook nog heel veel zelfbouw. Ja, en daar moet je echt zelf de ontdekking gaan doen. Pipeline is natuurlijk ook echt wel een ding van de laatste jaren, maar waar veel meer aandacht aan moet worden gegeven. Dus het opbouwen van je pipeline. Ook daar zitten heel veel maatregelen in, dus dat beweegt ook continu. Die technologie beweegt snel en daarmee bewegen ook je beheersingsmaatregelen mee.

Rico Schilder
Ja, en hoe vaak zou je dan zeggen dat je beheersingsmaatregelen dan daarop moeten worden aangepast?

Interviewee 3
Ja, eigenlijk continu. Vorig jaar heb ik bijvoorbeeld voor de pipelines voor 3 technologieën de belangrijkste maatregelen in kaart gebracht en geïmplementeerd bij de teams, maar inmiddels is er alweer een nieuwe pipeline bij gekomen. En eigenlijk moet ik daar weer hetzelfde voor gaan doen, dus ja, daar zul je daar opnieuw naar moeten kijken.

Rico Schilder
En als delen van dit proces geautomatiseerd zouden moeten worden door AI of deels geautomatiseerd. Welke onderdelen zouden daar dan het best passen, denk je?

Interviewee 3
Wat ik een heel mooie opportunity vind, is wat ik al zei. Je hebt de opzet van maatregelen en beheersmaatregelen, heb je in principe in dat soort raamwerken zoals COBIT en ISO, die ook als best practice worden bestemd in de markt en de hele wereld ook in principe gebruik van maakt, dat het ook makkelijk is voor de communicatie, hè? Maar hoe je dan de link legt tussen platformen? Dat zou hartstikke mooi zijn, dus dat heb ik ook weleens gedaan met ChatGPT. Ik had een heel raamwerk opgezet, voor CSD maatregelen en ik was daar een half jaar mee bezig geweest en vervolgens vraag ik aan ChatGPT: “Geef mij eens de…” Dat was toen net in opkomst, dat net op de markt, dus ik probeerde wat en vervolgens krijg ik gewoon exact het lijstje waar ik een half jaar aan gewerkt heb. Ja, dus dat is hartstikke mooi en vervolgens stel ik nog de vraag: “Maar hoe zou ik dat dan in technologie? Welke standaarden horen daarbij, welke technologiën horen daarbij?” En dan gaf ik een lijstje met de technologie die we hadden en die zei: “Deze opzet kan je daarmee doen.” En dat zou nog een stapje dieper kunnen. Zover is ChatGPT nog niet, dat hij hele onderliggende standaarden van platformen precies kent, maar daar zou je wel, door het AI model te voeden met best practices, maar ook de standaarden vanuit de platformen, die link proberen te leggen. “Als je deze controlemaatregelen hebt op dit platform op die plek, dan is dit daarmee afgedekt." Dat zou enorme potentie hebben denk ik.

Rico Schilder
Ja, dat hij daarmee meteen je risico response berekent bedoel je?

Interviewee 3
Ja, misschien je respons berekent, maar de respons is wat mij betreft… Je hebt dat op verschillende niveaus. Dus zo'n risico response kan zijn: “Je moet een back-up maatregel treffen." Ja, maar hoe doe je dat dan en met welke tool? En als je dan de link legt met je rubriek, over ons platform voor voor back-ups, dan zou die daar kunnen doorhalen en dan kan je zeggen: “Maar in de rubriek moet je dit vinkje aanzetten en moet je dat zo configureren”, zodat je volledig voldoet aan die control objective. Dus dat eerste niveau, dat haalt AI nog wel op dit moment. Die kan gewoon prima zeggen: “Ja, je moet je verlies op data, maar dan moet je een backup maatregel treffen.” Dat dat snapt hij wel. Of als je op de cloud werkt, moet je dit en dit doen en dat is net wat anders. Maar hoe de configuratie vervolgens in elkaar zit, dat is waar wij continu tegenaan lopen als beleidspartij binnen ORGANISATIE C. Hoe maak je de vertaalslag van controls naar daadwerkelijke instructies in de tooling en in de werkelijkheid? Die is voor ons heel moeilijk te maken omdat wij geen techneuten zijn, maar wel verstand hebben van de control objectives, maar een AI zou wellicht wel die taal slag kunnen maken, omdat die alles kan leren van het platform door hem te trainen op het platform. Je kunt ze alles leren van die control objectives en die kan wellicht wel makkelijk die link leggen tussen de werkelijkheid en de best practices.

Rico Schilder
Ja oké. Exact. En zitten er ook onderdelen in in het proces waarvan je zegt, nou, dit zou absoluut niet geautomatiseerd kunnen worden met behulp van AI?

Interviewee 3
Ja, de dingen waar je zelf bouwt, dan moet je op een of andere manier die data uit je zelfbouw applicaties kunnen halen en kunnen voeden aan het trainingsmiddel. Ja, dat wordt wel heel lastig. Maar gestandaardiseerde platformen zoals ServiceNow of AWS, die kunnen dat wellicht ja. Dus dan kan je wellicht gewoon de instructies van AWS en instructies van van ServiceNow en al die andere platformen gewoon kunnen voeden en dan heb je voor 90 a 80%, en sowieso gaan we steeds meer over op die standaard platformen, heb je het te pakken en ik denk dat het wel heel lastig is voor een applicatie die helemaal zelf gebouwd is en waar je dus eigenlijk geen instructies voor hebt, al zou je die ook moeten hebben, maar die kan je niet zomaar voeden. Dan moet je dat zelf in de hand hebben, zeg maar. Die trainingsdata moet je dan zelf gaan voeden, dan zou het kunnen, daar moet je wel de know-how voor hebben natuurlijk.

Rico Schilder
Ja, dus dan zou je van dat proces of systeem hele specifieke documentatie moeten hebben, zeg maar?

Interviewee 3
Ja ja, exact en voor de gestandaardiseerde pap heb je dat gewoon. Daarvoor is die documentatie er, maar voor zelfbouw applicaties zou dat er minder zijn denk ik of niet zo uitgebreid als een gestandaardiseerd platform. Ja, hoe dan?

Rico Schilder
Oké. Ja. Dus je denkt niet dat AI het complete proces, al deze stappen, helemaal kan overnemen als ik het zo hoor?

Interviewee 3
Nou, dus wel de why en de what, dat kan AI prima doen, maar tot op dit niveau de how voor alle applicaties. Dat wordt lastig, denk ik. Maar goed, je kunt alles trainen natuurlijk. Als je de data hebt en daar ligt het probleem. De data is vaak niet kwalitatief op een goed niveau en dat is wel een randvoorwaarde om AI te kunnen trainen. Je moet goede data hebben. Dus alles kan, alleen je moet de data dan zo gaan maken dat het kan.

Rico Schilder
Juist oké, top. Nou, je noemde net al dat je zelf ook weleens experimenteert met AI. Maar wordt dat wel vaker gebruikt binnen jullie organisatie?

Interviewee 3
Nee, ja, we hebben een heel stom beleid binnen ORGANISATIE C. Ze zijn bang dat wij conclusies trekken uit verkeerde informatie, omdat je de bron niet kunt checken met AI, of niet bij alle platformen. Dus bij ons hebben ze alle AI, ChatGPT, hebben we allemaal dicht gezet. Toen in het begin nog niet. Dus ik kan het niet gebruiken, maar we zijn nu aan het onderzoeken op basis van interne datamodellen, AI kunnen gebruiken. Ik gebruik het privé nog steeds heel veel en heel stiekem gebruik ik het gewoon ook voor mijn werk, af en toe gewoon op mijn telefoon. Zeg maar, als ik even snel wat wil opzoeken. Maar ze zijn wel heel erg paniekerig over hoe de output van AI wordt geïnterpreteerd. En dan ja, dat vind ik heel jammer, want volgens mij mis je enorm veel kansen op dat vlak, zeker voor onze engineers, want die kunnen ook gewoon heel erg geholpen worden met schrijven van software op basis van AI. Maar ook voor ons als beleidsmakers helpt het enorm om heel kort en krachtig beleid in te zetten dat begrijpelijk is voor iedereen. En ja, dat is helaas niet mogelijk. Nog niet.

Rico Schilder
Ja, dus dat draait echt om de kwaliteit van de output vooral?

Interviewee 3
Ja ja, klopt. En waar onze security managers vooral bang voor zijn, is dat wij bepaalde, en dat is niet voor beleid, maar vooral voor medewerkers die met klanten in contact staan, is dat zij op basis van ChatGPT verkeerde conclusies trekken, en dat dat voor waarheid wordt aangenomen en daardoor een verkeerde beslissing nemen. Dat is de angst.

Rico Schilder
Ja. Oké. En daar kom ik straks ook nog weer even op terug. Maar eerst ja, een aantal vormen van AI die regelmatig worden gebruikt zijn bijvoorbeeld Natural language processing of Generative AI. Nou ja, ChatGPT is daar een bekende vorm van. Je bent bekend met allebei deze termen?

Interviewee 3
Ja. Ja.

Rico Schilder
Oke, top. En denkt u dat beide vormen van AI wel gebruikt kunnen worden in het proces van het maken van een controle raamwerk?

Interviewee 3
Ja, dat denk ik zeker ja.

Rico Schilder
Oke, top. Zijn er misschien nog meer vormen van AI die je ‘from the top of your head’ kan bedenken die je eventueel kunnen helpen hierin?

Interviewee 3
Nou ja, ik weet niet… Welke zei je net? Large language models en generative AI? Is dat niet hetzelfde?

Rico Schilder
Ik zei net Natural Language Processing, dus NLP, en Generative AI.

Interviewee 3
En de LLM, is dat generative AI?

Rico Schilder
Ja.

Interviewee 3
Ja ja precies.

Rico Schilder
Ja, generative AI, die gebruikt LLM’s om een output te genereren. Inderdaad, ja, dat klopt.

Interviewee 3
Ja precies. En, wat is die andere dan?

Rico Schilder
Natural Language Processing. Dus dat een vorm van AI die tekstuele input kan begrijpen, zeg maar.

Interviewee 3
Oh ja, precies. Nou, imaging zou ook heel erg… Zeker als je gaat kijken naar een implementatie, hè? Dus heb je imaging, maar ook text-to-speech en text-to-video. Die zouden heel erg kunnen helpen bij de implementatie van control frameworks. Daar had ik ook naar gevraagd laatst, bij onze AI club. “Kunnen jullie niet iets bieden van text-to-speech of text-to-video of een combinatie ervan, zodat wij, op basis van onze instructies of ons beleid, video's kunnen maken?” Dan kunnen we trainingsprogramma's maken die heel makkelijk te maken zijn met AI. Het gaat ons namelijk heel veel tijd schelen om dingen uit te leggen. Want nu zijn wij de mensen die het woord voeren en uitleggen aan de mensen wat ze moeten doen, en aan engineers wat ze moeten doen, en hoe ze dat moeten doen. En dan kan je 90% van de vragen al wegnemen, door trainingen of video’s aan te bieden, die ze

kunnen volgen. Dan hoef je alleen nog maar de uitzonderingen te beantwoorden. Dus in die zijn, het maken van het control framework, niet zo zeer, maar wel voor het uitdragen van het control framework kan je dat gebruiken. Dus text-to-speech, text-to-video.

Rico Schilder
Ja exact, dus dat is om ondersteuning om die controles ook echt na te leven?

Interviewee 3
Ja. Een stukje awareness creëren van die controls, en wellicht ook nog wel… Heel veel data van onze control frameworks toetsen wij. Dus we hebben allemaal control objectives, en daar zetten we toetsen bij uit, bij teams, om te checken of zij voldoen aan die controls. Je zou wellicht ook die data kunnen laten trainen door de AI. Dus dat is eigenlijk een soort monitoring tool AI, dat je kunt zeggen: “Oh, maar hier gaat een rood lampje branden op dit vlak bij dit team, want al een paar keer op rij gaan de toetsen niet goed”. Dus dat zou nog iets anders kunnen zijn, en dat zit meer in je risk management, ERM, die je daar op toepast. Volgens mij is ServiceNow nu ook bezig met een AI achtige oplossing. En die jou dan eigenlijk de goede weg op helpt. “Ik zie uit de resultaten van de monitoring dat hier niet goed op gescoord wordt. Dit zijn de te ondernemen acties die ik zou adviseren vanuit de AI”.

Rico Schilder
Dus dan combineer je dat eigenlijk een beetje met een soort interne audit?

Interviewee 3
Ja, eigenlijk een interne AI slimme auditor, die kijkt waar het allemaal mis gaat, en waar het goed gaat op basis daarvan een soort adviezen geeft. Dus bepaalde KPI’s hebben we nu ook. Bijvoorbeeld, een van de KPI’s is ‘changing causing incidents’. Dus we hebben heel veel changes die incidenten veroorzaken. Dat is niet goed, die KPI weten we ook, en kan je ook gewoon uit het ServiceNow platform halen, want elke change wordt gelogd. En elk incident wordt geregistreerd, en die moet je wel koppelen aan de change. Dat geeft al heel veel inzichten, maar het enige probleem is dat wij inzichten niet goed kunnen doorsnijden. Dus dan kun je hem niet teruggeven aan de doelgroepen. Dus daar kan AI bij helpen. En de actionability van een KPI, en daar bedoel ik mee: “Wat moet ik doen als mijn KPI op rood komt, of een dalende trend laat zien? Wat zijn de acties die ik dan moet nemen?” Een voorbeeld kan zijn, dat je beter je testen moet uitvoeren, of je moet meer geautomatiseerd testen toepassen, of je moet breder testen zodat je je incident gaat afnemen. En dat soort inzichten kan AI wellicht best bieden. Ik zit nu echt heel erg in de “wat zou kunnen?” he. Misschien is dat allemaal heel moeilijk.

Rico Schilder
Ja, maar dat maakt niet uit dat dat allemaal best wel interessant is natuurlijk en je kan er ook heel veel kanten mee op.

Interviewee 3
Waar we ook mee bezig zijn is, we hebben ook heel veel beleid binnen ORGANISATIE C en dat is allemaal een documentjes gestopt. Ja, er is niemand die dat leest. Dat is net zoals het wetboek, zeg maar. Iedereen weet dat er een wetboek is, maar niemand die het leest, want dat is gewoon niet door te komen, zeg maar. “Dus dit is de wet en daar staat dit en dit. Zorg ervoor dat je dat regelt.” En dat doen we nog wel. En mensen willen best wel voldoen aan de

wet, alleen ze weten niet hoe, of ze weten niet waarmee. Dus wat je aan die wet wilt vragen is, LLM, al je beleidsstukken… Dat hebben we ook al geprobeerd, en dat werkt ook best wel goed. Het laten voeden en laten trainen en daar dan vragen over stellen. “Wat moet ik doen? Aan welke eisen moet ik voldoen?” Als ik test, geeft hij gewoon een lijstje met eisen die hangen aan testen. En, die kan je dan teruggeven aan zo'n engineer en dan kan een engineer misschien nog eens doorvragen: “Maar ik zit op dit platform. Hoe werkt het daar dan?” En ook daar hangt en staat het weer bij de data. Je moet wel die data hebben om dat antwoord te kunnen geven, maar veel van die data hebben we, alleen die is niet vindbaar op dit moment. Dus het vindbaar maken van beleid zou daarbij kunnen helpen. Dus je control framework hoort daarbij, is ook een van je beleidsstukken.

Rico Schilder
Ja, en er zijn dus een aantal typen documenten of data die je nodig hebt als input daarvoor, voor een systeem dat AI gebruikt om een controleraamwerk op te stellen of om controls te formuleren. En je noemt nu beleid en ook data uit de processen. Zijn er nog meer dingen die je als input daarvoor nodig hebt?

Interviewee 3
Ja. Dus wat ik net al zei, dus je control framework, je beleid, maar ook je instructies, hè. Dus alle instructies, werk instructie niveau, die zou je daar allemaal in een groot trainingsmodel willen gooien. En eigenlijk een taxonomie heb je ook nodig om die relaties voor te leggen, want dat zie je nog weleens bij LLM’s. Dat relaties niet goed worden uitgelegd en dat je gekke antwoorden krijgt en door een taxonomie te hebben, dus dus eigenlijk zeg maar een kerstboom van: dit is het hoofdbeleid, daar hangen deze sub beleidsstukken onder, daar horen deze werkinstructies onder, kan hij die relaties wellicht beter leggen. Dus dus Ik denk dat je dat ook nodig hebt, maar dat ken ik AI niet goed genoeg voor. Maar het is alles, dus alle stukken heb je nodig, instructies, maar ook de relaties daartussen, dus die zijn belangrijk.

Rico Schilder
Ja, ja, exact. Dat is ook wel eigenlijk een soort technisch probleem. Want als je dus al die dingen als input gaat gebruiken, dan is dat wel een probleem dat zou kunnen voorkomen, als je dus niet die taxonomie goed in kaart hebt. Zie je ook nog meer technische problemen voor je op dat gebied?

Interviewee 3
Nou, we willen het niet in de cloud hebben, die data, want dat is ons eigen beleid, en heel veel van die data wordt ook nog in Amerika verwerkt. Dat willen we ook niet, want dat is Europese wetgeving. Dus je moet zelf iets gaan neerzetten. En als je zelf iets gaat neerzetten, dan zit je met schaalproblemen. Wij kunnen nooit op zo’n grote schaal die trainingsmodellen laten trainen, dus dat is echt heel technisch. Dus niet voldoende die NVIDIA H100 processoren neerzetten, om die data goed te trainen. Dus daar zie ik wel een technisch impediment, zeg maar. Dat je dat wel wilt, maar niet goed genoeg kunt, of niet genoeg rekenkracht daar tegenover zet om dat datamodel goed te laten werken. Misschien dat AWS en zo daar wel oplossingen voor gaan bieden. Maar volgens mij zijn ze niet zo ver nog op dat vlak.

Rico Schilder
Ja oké. En zijn er eventueel ook nog ethische problemen die je voorziet bij het verwerken van alle documenten die je net hebt genoemd als input?

Interviewee 3
Ja. Ik denk dat er weinig privacygevoelige informatie in ons beleidsstuk staat. Het is wel gevoelige informatie natuurlijk, want het is beleid dat je toepast, dus in die zin wil je de informatie bij je houden. Dat is ook de reden waarom dat bij ons dicht staat. En het gevaar is dat er een datalek kan ontstaan, omdat je zomaar per ongeluk klantdata in die ChatGPT machine gooit. Dus dat is wel een ethisch risico. Maar anders dan dat? Voor het control framework, ja denk ik dat het wel meevalt.

Rico Schilder
Oké en dus bij het genereren van bijvoorbeeld Controls. Zet daar dan ook nog een ethisch dilemma in?

Interviewee 3
Nee, het enige waar je voor moet oppassen is dat je volledig vertrouwt op het AI programma. Dat je het klakkeloos gaat overnemen. Dat is niet echt ethisch, maar dat is wel om… Je kunt niet zomaar je schoonmoeder sturen, en zeggen dat ze even een control framework moet maken, want die weet niet wat je verwacht. En ik zit in het vak en ik weet wat ik verwacht en ik kan het verifiëren. Dus het kan mij heel erg helpen om snel stappen te maken, en zo heb ik dat ook gebruikt bij mijn CSD kader. Maar af en toe stonden er ook gekke dingen in. Wat bedoelen ze daarmee? Soms is het niet helemaal juist geïnterpreteerd. Daar zit wel een risico in zeg maar. Dus dat is niet per se ethisch, maar wel een foutgevoeligheid. Je moet het kunnen verifiëren op een of andere manier.

Rico Schilder
Ja. En, wat kan er gebeuren als je te veel zou vertrouwen in die output?

Interviewee 3
Nou dat er aannames gedaan worden door de AI machine die niet juist zijn waardoor je dingen gaat implementeren die helemaal geen waarde toevoegen of die zelfs averechts werken. Dus dat het risico alleen maar groter wordt zelfs.

Rico Schilder
Ja dus wat daarvoor nodig is om dat probleem te verhelpen eigenlijk, is dat je wel genoeg ervaring moet hebben?

Interviewee 3
Ja, ervaring, bronvermelding zou helpen natuurlijk hè, dus dat je altijd de bron kunt naslaan. Waar kom ik vandaan en hoe hebben ze dat bedoeld? Maar misschien ook wel een stukje training van de gebruikers, hè, dus? Hoe moet je gebruiken waar? Wat kan je vertrouwen? Wat niet? Ja, er is gewoon ervaring en kennis nodig van het object waar je mee bezig bent.

Rico Schilder
Ja, en je noemde ook de traceerbaarheid van de bron. Maar dat is wel een lastigheid met AI toch?

Interviewee 3
Ja ja, klopt. Maar Bing doet het wel hè? Die doet wel verwijzingen. Ik weet niet of dat helemaal juist is dan die bronverwijzingen, maar het kan wel. Maar het zou wel helpen, als er iets is om te kunnen verifiëren of de informatie juist is of niet.

Rico Schilder
Ja exact en, dat is ook wel een cruciaal iets of?

Interviewee 3
Ja, denk ik wel. Als je mensen controls in je control framework laat bedenken, die er geen ervaring mee hebben en klakkeloos controls gaan invoeren, bedenken en implementeren. Dan ga je dingen doen die niet moeten denk ik. Dus is dat cruciaal? Het kost gewoon heel veel geld. Dan ben je heel veel resources kwijt, wat niet nodig is. Je moet ook goed die risico-inschatting doen. En dat is het lastige voor een AI-module. Die kan de risico's niet zo goed inschatten, zonder goede data. Voor ORGANISATIE C specifiek, voor mijn situatie. Wat zijn de risico's bij? Want elk bedrijf is anders. Elk bedrijf heeft een andere cultuur. Dat zijn allemaal 'soft-maatregelen' die ook bestaan en die heel erg cruciaal zijn voor het risiconiveau. En als je controls gewoon klakkeloos gaat implementeren, terwijl het voor een bepaalde control, of die specifieke situatie of context helemaal niet belangrijk is, dan sla je de plank mis denk ik. En andersom kan ook gelden dat een control minder belangrijk wordt geacht door het AI-model, maar misschien juist wel heel belangrijk is in de situatie van ORGANISATIE C. Dus dat zijn in ieder geval afwegingen die, in ieder geval nu nog, niet door een AI-model kunnen worden gemaakt. Misschien op termijn wel, als je kijkt naar risicomanagement met modules, dat je die meer laat trainen en ziet welke trends er zijn, en dat de AI dan ziet: "Maar deze kant kun je opgaan." Maar dat is volgens mij nog wel 10 jaar verder. Alhoewel, het gaat heel snel met AI, dus het kan ook zomaar 5 jaar zijn, maar dat weet ik niet.

Rico Schilder
Ja, het gaat wel snel inderdaad. En je noemde net ook heel even die 'soft-maatregelen', je bedrijfscultuur en zo. Maar dat is dus ook heel belangrijk om als input mee te geven.?

Interviewee 3
Ja, alleen die is natuurlijk heel, heel soft, heel lastig om hard te maken. Ja voorbeeld: bij ORGANISATIE C is er heel veel aandacht voor beschikbaarheid van onze applicaties en robuuste systemen, zeg maar. Het komt wel eens voor dat de systemen eruit liggen, maar we liggen er lang niet zo vaak uit als andere organisaties in hetzelfde domein, omdat in de cultuur is ingebakken dat dat het belangrijkste is wat er is. En daar bouwen we ook op. Zo bouwen we de spulletjes ook. Dat geeft een ander gewicht aan de control. En hoe maak je die hard? Dat is gewoon heel lastig.

Rico Schilder
Ja dus, dan zou je eigenlijk al moeten voortbouwen op een soort set normen en daarmee dan zeg maar je bedrijfscultuur moeten gaan beschouwen en gaan documenteren op een bepaalde manier.

Interviewee 3
Ja ja, precies ja.

Rico Schilder
Oke. En als dan een gebruiker zo'n systeem zou gebruiken, of AI zou gebruiken bij internal control. Wat zijn dan voor die gebruikers essentiële aspecten? Want je noemde het net al, die gebruiker moet veel ervaring hebben en misschien zelfs een training moet hebben in de omgang met AI. Zijn er nog meer dingen die erbij komen kijken?

Interviewee 3
Nou, prompten is natuurlijk wel een dingetje, hè? Dus hoe krijg je de juiste antwoorden? Dat is een heel vak apart. Dus je moet dan wel, en dat hoort misschien bij die training, maar als je gaat prompten, moet je dat wel onder de knie hebben voordat je daarmee aan de slag gaat. Want hoe stel je de juiste spraken? Hoe krijg je de beste informatie uit zo'n AI model? Ja, Dat is wel relevant natuurlijk.

Rico Schilder
Ja, dus ja, zou je eigenlijk ook wel inderdaad bij die training kunnen?

Interviewee 3
Dat is een van de aspecten van die training. Hoe haal je informatie eruit? Maar een ander aspect, is hoe je die informatie verifieert. Dus het zijn nu twee dingen die belangrijk zijn, denk ik. Het extraheren en het verifiëren van informatie.

Rico Schilder
Oké ja, top. Denk ik dat we de meeste van de vragen wel gedekt hebben die ik had staan. Had je vanuit je eigen werkervaring nog een inbreng op dit onderwerp?

Interviewee 3
Hoe bedoel je dat?

Rico Schilder
Het zou natuurlijk kunnen zijn dat ik bepaalde vragen gemist heb, dus dat je denkt: "Nou, dit schiet me nog te binnen over je over het onderwerp." Je moet het zo zien dat ik uiteindelijk in mijn scriptie probeer ik een soort high level design probeer te maken van hoe een systeem dus AI kan gebruiken voor internal control en het opstellen van controls. Dus ik zal op globaal niveau een soort schets proberen te maken van stappen die daarvoor nodig zijn. Welke vormen van AI de gebruikt kunnen worden, wat de consequenties daarvan zijn, eventuele risico's, maar ook de mogelijkheden. Dus ik vraag me af of je daar nog een extra kijk op hebt die misschien interessant is.

Interviewee 3
Ja, misschien de integratie, hè, dus hoe integreren we die informatie? Met mijn bestaande tools, dus hoe je daar nou? En ik heb laatst gevraagd naar AI tooling, die text-to-speech waar ik het net over had. En toen werd mij verteld dat ik zelf een AI-model moest bouwen. Dat werkt natuurlijk niet. Dus die AI moet wel toegankelijk zijn. Ik kan zelf geen AI-model bouwen. Dus hoe zou je dat integreren, en met welke tools? Doe je dat in een chatbot of in een webbrowser? Ja, dat lijkt me wel cruciaal voor de gebruikers. En hoe integreer je dat

dan weer met je control framework tool? Wij hebben ServiceNow ERM. En dat zouden we eigenlijk een op een willen. Dat je niet alles in een tekstbestandje krijgt en dat weer moet gaan overtypen in een ServiceNow tool. Het zou ideaal zijn als dat gewoon een op een is. “Dit zijn de controls. Hij maakt ze aan. Hij koppelt ze aan de systemen waar het voor geldt.” Dat zou wel de ideale wereld zijn.

Rico Schilder
Dus dat het gewoon echt een applicatie is als het ware, één systeem?

Interviewee 3
Ja ja.

Rico Schilder
En, dat is dan van input zoals je beleid, je data, je procesdata, dat soort dingen tot aan een…

Interviewee 3
Best practices.

Rico Schilder
Best practices ja, je normen kaders of je frameworks, je ISO en zo.

Interviewee 3
Ja. En dat die ook continu blijft lopen, dat je die continu laat leren en dat je aanpassingen krijgt op basis van veranderingen in de markt en omgeving. Dat is eigenlijk ook relevant natuurlijk dat je in je omgeving beweegt. Continu. Technologie beweegt continu. En je controle framework wil je eigenlijk… En nu doen we dat een keer in de paar jaar. Sowieso kijk je jaarlijks naar je control framework, maar eigenlijk gaan die veranderingen vaak sneller en loop je altijd achter de feiten aan. Dus wil je kort iteratief die aanpassingen doen en mee laten bewegen met de technologie je ook je control framework. Ja, en als je dat in een systeem doet. Ja, dan ben je spekkoper natuurlijk. Dan kunnen wij van 300 man, die met riskmanagement bezig zijn, naar 5 man die met risk management bezig zijn.

Rico Schilder
Die alleen maar de output een beetje hoeft te controleren?

Interviewee 3
Ja precies.

Rico Schilder
Ja exact ja, het zou inderdaad wel heel ideaal zijn als het gewoon in een soort ja GRC tool zit, waar je gewoon al die documenten in gooit en dat hij zegt: “Dit is je raamwerk. Succes”.

Interviewee 3
Ja, ja, en dat maar dat je het document er niet eens in hoeft te gooien, maar dat je ze connect met het internet. Dus je best practices, die veranderen ook continu dus dat je ze daarmee koppelt. Dat je met die wetgeving, daar hebben we ook tooling voor nu hè? Ruler noemen we dat. Dit haalt continu wetgeving van buiten naar binnen. Dat je die daarmee

voedt. Dat je hem voedt met technologie platformen, instructies en continu laat itereren op dagelijkse basis, dat je eigenlijk een knopje indrukt. “Ik heb een nieuwe control bedacht en gevonden, omdat er nieuwe technologie is of er gaan controles af." Vergeet dat ook niet hè, dat je controles moet opruimen, af en toe ook, want omdat er terminologie verandert, zijn bepaalde controles weer minder relevant geworden en het zit meer geborgd. En dat zie je met pipelines bijvoorbeeld vroeger heel erg. Toen waren we bezig met functiescheiding tussen ontwikkelaars en beheerders. Nu zitten alle ontwikkelaars en beheerders bij elkaar in het team, dus die moeten het allebei kunnen. Maar er zit weer een in de pipeline beheersmaatregelen ingebakken, in de techniek, die ervoor zorgt dat ze niet zelf iets introductie kunnen brengen als ze dat zelf hebben gebouwd. Dat soort veranderingen wil je eigenlijk continu in de gaten houden en nu doen we daar, ja wat ik zeg, met 300 man als het niet meer is, zijn we daar dagelijks mee bezig. Als je dat continu mee laat bewegen door een AI-model, ja dan kan je daar de factor 10 100 misschien wel minder mensen aan doen. En dat scheelt kosten voor de organisatie en dat kan je natuurlijk weer doorrekenen aan je klanten, dus kunnen die grote goedkopere producten afnemen. En zeker risk management is echt een hot topic op dit moment door alle wetgevingen, zoals DORA-wetgeving die aan zit te komen. Eigenlijk wil je gewoon DORA inlezen en dan zeggen: “Hey, er is een nieuwe wetgeving. En welke control moet ik bijvoegen? Welke controls moet ik aanpassen en dat die dat automatisch doet?” En dat je dan automatisch dagscripts uitzet naar teams die het uitvoeren. Dat zou de ideale wereld zijn.

Rico Schilder
Ja, als dat allemaal zo connected is, zeg maar, gewoon een stuk door verbonden is. Dat zou wel een soort Utopia zijn.

Interviewee 3
Ja precies, dat is de ideale wereld, maar dat hangt en staat bij data, en goede data. Daar zit vaak de crux en die is er niet altijd, vaak niet, laat ik het zo zeggen. Dan ga je interpretaties doen en dan heb je riskmanagers daarvoor nodig om die interpretaties te doen en risico's goed in te schatten. En bij AI is dat ook super van belang, want zonder goede data heb je geen AI, zeg maar.

Rico Schilder
Waarom is er niet altijd goede data?

Interviewee 3
Ja goeie vraag. In het verleden nooit goed over nagedacht. Oude data, dus soms heb je legacy, hè. Zit je met Legacy, dus bijvoorbeeld: dat nooit het belang geacht om goed, datum en even adres en van iedere medewerker of van iedere klant vast te leggen, omdat dat op dat moment niet relevant was, maar later bleek het wel relevant, omdat we voor privacy en voor poortwachterswet moeten we allerlei data checken of het inderdaad wel natuurlijke personen zijn of iets dergelijks. Ineens werd die data wel relevant, maar ja, ga maar dan eventjes alles als je dat ooit niet hebt vastgelegd en nu wel vast moeten leggen, allemaal weer eventjes aanvullen die data, dan moet je klantenlijst gaan vallen. Dan moet je eens formuliertjes laten invullen. Hebben ze allemaal geen zin in. Dus dat kost enorm veel tijd en geld. Ja, dus dat is ook in de loop van de jaren zo gegroeid natuurlijk en die data wordt steeds belangrijker. Maar dat was vroeger blijkbaar minder van belang.

Rico Schilder
Ja. Denk je dat het in de toekomst wel meegroeit, die datakwaliteit?

Interviewee 3
Ja, dat moet wel.

Rico Schilder
Dat als we bijvoorbeeld over 5 jaar met een soortgelijk probleem zitten, dat je dan zegt: “Nou ja, de data vanaf afgelopen 10 jaar is wel redelijk vergeleken met hoe het 5 jaar geleden was of 10 jaar geleden."

Interviewee 3
Ik denk dat dat wel moet. Ook voor wetgeving moet dat, dus daar zie je ook gewoon steeds meer wetgevingen opzetten, omdat je allerlei modellen hebt die op basis van die data berekeningen doen. Reserves voor de banken, reserves aanmaken, omdat je op basis van bepaalde data, omdat je groep van klanten uit een bepaalde regio hebt die een hoger risicoprofiel met zich mee hebben of een lager risicoprofiel, waardoor je allerlei aannames doet. Ja, dat dus, dat moet wel. Dat wordt steeds meer een ding die daar kwaliteit, dus ik denk dat het wel steeds beter wordt. Alleen connectability, zeg maar dus het integrale… Zeker voor de riskmanagement is dat gewoon nog heel slecht op het moment. Dus het is allemaal nog houtje touwtje, veel zit in Excel, veel zit in Word, alle beleidsstukken waar ik het over had is niet vindbaar, is verstopt, is niet goed, zijn geen goede relaties gelegd. Ja voordat je dat allemaal hebt. Ja, dan ben je heel wat verder en tot die tijd kan je ook niet goed die LLM’s daarop loslaten, denk ik.

Rico Schilder
Oké. Ja ja, interessant. Dankjewel. Ik denk dat we dan klaar zijn. Had je verder nog dingen toe te voegen?

Interviewee 3
Nee.

Rico Schilder
Nee. Oke nou top.
Ja heel erg bedankt dat je wil helpen bij mijn onderzoek. Nogmaals, ik waardeer het enorm dat je de tijd hebt genomen.