Rico Schilder
Dan zal ik beginnen met wat weet je van AI?

Participant 1
Ja, ik vind dat ik er redelijk goed bekend mee ben. In de zin van dat ik op de universiteit hè, heb ik er nog een recent vak over gevolgd. Ik heb op data camp zelf diverse cursussen gevolgd, waarbij ik ook zelf in ieder geval data science machine learning achtige toepassingen heb geprogrammeerd. Ik heb diverse AI tools, we hebben onder de meest bekende natuurlijk ChatGPT, mee geëxperimenteerd. Kan ik de nitty gritty details vertellen van AI, dat niet. Ik denk dat ik best een eind kom, maar ik ben geen specialist, maar ik ben aardig bekend.

Rico Schilder
Bij het maken van zo'n intern controleraamwerk zitten een aantal elementen in dat proces, een aantal activiteiten, die uitgevoerd moeten worden. En activiteiten die ik uit de literatuur heb gehaald, begint bij risico identificatie, gevolgd door de beoordeling van de risico's, de ernst, de prioriteit van de risico's beoordelen dan een risicobeheersing of een response maken voor ook risico en dan uiteindelijk dat rapporteren van die voorafgaande stappen. Bent u het eens met deze? Ben je het eens met deze opdeling?

Participant 1
Die risico identificatie gaat nog een stap aan vooraf. En dat zijn natuurlijk je doelstellingen scherp hebben. Want afhankelijk van je doelstellingen. Hé, daar hangt je risico en daar hang je risico's mee samen en ook de wijze waarop, hè? Waarop je die assesst.

Rico Schilder
Ja, dus dat is eigenlijk een stap die je ook in dit rijtje wel echt thuishoort?

Participant 1
Ja, zou ik zeggen van wel.

Rico Schilder
Oké, oké top dan de volgende vraag: welke activiteiten in het proces zijn het meest intensief? (qua tijd of moeite)

Participant 1
Ja, ik denk dat de stap van een ernst beoordeling het meeste tijd kost. Dat komt omdat je daar vaak verschillende disciplines bij betrekt. Ja, dat doe je ook wel bij risico-identificatie, maar bij ernst beoordeling zit hem vaak dat vanuit de verschillende disciplines er anders tegen risico's wordt aangekeken. En hè om tot een consensus te komen dat er overleg voor nodig is. Je moet elkaar gaan begrijpen en je elkaar in elkaars standpunt gaan verplaatsen voordat je uiteindelijk tot een conclusie komt. En dat kost tijd.

Rico Schilder
Ja dus dus vooral die communicatie daartussen en verschillende visies op zo een risico. Oké en de andere onderdelen zijn die dan gelijk aan elkaar of zijn er ook nog verschillen tussen?

Participant 1
Als je het eens bent over de ernst. Dat volgt eigenlijk wel een beetje de prioriteitstelling uit en je gaat meer doen op je hogere risicogebieden dan op de gebieden waar je minder risico loopt. Ik denk dat daarna de wijze van response het meeste tijd kost.
En nu we het er dan over hebben, dan zou je eigenlijk hierin nog een stap verwachten.
En die zit denk ik tussen stap 3 en 4 tussen je ernst beoordeling en je prioriteitenbeoordeling is eigenlijk bepalen van welk risico ben je bereid te lopen? Want als je een hoog risico constateert, en je bent ook bereid een hoog risico te lopen, dan hoef je daar uiteindelijk weinig aan te doen. En risicobereidheid, dat is ook best wel een lastig onderwerp om het met elkaar over eens te worden. Dat is dat kost ook wel veel tijd. Maar als je uiteindelijk ziet van hé, ik loop een hoog risico en we zijn eigenlijk met elkaar bereid maar een laag risico te lopen. Ja, dan moet je daar wat aan gaan doen. En, dat is je risico response, hè? Of je gaat risicobeheersmaatregelen nemen. Je kan ook besluiten dingen niet meer te gaan doen, je kan verzekeren. Je kan proberen het risico op andere manieren te verkleinen en daar de balans in vinden. Ook dat kost natuurlijk tijd, maar ik denk dat op nummero een kwa meeste tijd is die ernst beoordeling, twee risicobereidheid bepalen en dan drie je het eens worden over de over de risico respons.

Rico Schilder
Ja, oke.

Participant 1
Hè? Want alle beheersmaatregelen uiteindelijk kosten geld en alles is een kosten-batenafweging. Nee, je kan iets helemaal dichttimmeren en je risico enorm beperken, maar uiteindelijk kost dat ook veel geld en laat je misschien ook wel kansen liggen.

Rico Schilder
Ja, terwijl als je risico gaat verkleinen of je accepteert om gewoon dan kan dat andere gevolgen hebben of uiteindelijk een ander netto risico opleveren?

Participant 1
Ja.

Rico Schilder
Welke activiteiten op welke van deze stappen zouden (deels) geautomatiseerd kunnen worden met behulp van AI?

Participant 1
Nou best wel veel stappen. Ik gebruik toch even gewoon het meest basis ChatGPT eventjes als voorbeeld en ik denk als je daar je daar doelstellingen in stopt, hè? Dat kan bijvoorbeeld zijn dat je daar gewoon een strategiedocument opstuurt. En waarin, in het geval van de ORGANISATIE A de missie, visie, en strategie van de ORGANISATIE A in benoemd worden en wat de belangrijkste doelstellingen voor de voor de komende 5 jaar, 3 jaar, komende jaar in staan vermeld en wanneer ChatGPT de opdracht geeft van: “hé identificeer de belangrijkste risico's op basis van dat dit document”, dat je een hele aardige set aan risico's voor de kiezen krijgt. Dus die risico identificatie is denk ik heel goed te doen met behulp van AI. Als je een normenkader erin gooit, een ISO normen kader, erin plakt en je zegt: ik wil dit transformeren tot een set, risico's en controls. Dan rolt daar ook echt een prima set uit

waarmee je kan gaan starten. Ik denk ook als je er een procesbeschrijving in stopt hè, waar we het net heel even in de introductie kort over hadden, net ten aanzien van de IT processen hoef je er niet eens een proces in te stoppen. Dan kan je gewoon tegen AI zeggen van: “pak eventjes het standaard incidentmanagementproces, en ik wil graag de risico's binnen het proces weten”. Nou dan komt er ook een goede set uit.
Wanneer het geen standaard proces is, maar je hebt wel goed het proces gedocumenteerd. Bijvoorbeeld bij ORGANISATIE A, het alarmcentrale proces, hè. Als wij dat gewoon goed gedocumenteerd hebben, dat in ChatGPT hangen, en vragen aan ChatGPT van: “identificeer de belangrijkste risico's”. Denk ik dat dat redelijk spot on is.

Rico Schilder
Ja dus het is vooral die risico identificatie en het formuleren van de controls. Dat zijn de voornaamste stappen?

Participant 1
Ja, en ik denk ook dat je met al die stappen AI met een antwoord komt. Maar dat gaat erover, hè? In welke mate heb je dan vertrouwen in dat antwoord? En dan denk ik niet, zeg maar dat de ernst beoordeling of de risicobeoordeling, dat hij zo goed is als dat we dat met verschillende stakeholders zouden kunnen doen. Ik denk dat je best wel met een aardige voorzet komt, maar dan moet je heel goed gaan prompten, of dat je moet gaan voeden met bijvoorbeeld: “Ik heb het alarmcentrale proces en ik wil nu dat je er met een security bril naar gaat kijken”. Dat zou een mooi experiment zijn trouwens. Ik heb dat nooit geprobeerd, maar dat je bijvoorbeeld daar informatiebeveiligingsbeleid en baselines en standaarden tegenaan gooit, en dan zegt: “Ik wil nu dat je de risico's beoordeelt vanuit security bril”. Vervolgens kan je dat natuurlijk ook doen door: “beste AI, je moet je nu even inleveren in een privacy professional. Je moet even de de geldende AVG, GDPR, en by the way ons eigen privacybeleid en kaders daarbij in ogenschouw nemen. En ik wil nu dat je vanuit dit perspectief een beoordeling doet en nu zit je in een operationeel perspectief”. Het moet ook allemaal werkbaar blijven, dit soort processen, het moet of vanuit een klantperspectief.
Ik denk dat je met een AI nog best wel vanuit verschillende gezichtsvelden een risicobeoordeling kan doen en dat je dan zegt: “summarise dit en kom dan met een eindconclusie en een prioriteitstelling”. Ik denk dat dat nog best wel aardige voorzetten kunnen zijn. Ik weet niet of ik zo ver zou gaan dat je daar helemaal op kan steunen, maar ik zou best wel eens in de praktijk de sessies met de mensen doen, maar daarbij misschien wel een toetsing kunnen doen die ik vanuit AI laat voeden. En dat ik dan bijvoorbeeld de AI output vergelijk met de risico assessment die we zelf hebben gedaan.
En dan AI laten helpen om bijvoorbeeld punten te benoemen waar we misschien zelf niet aan gedacht hebben. Of de wezenlijke verschillen nog eens eventjes tegen het licht te houden, van: “zelf vinden we het een hoog risico, maar de AI output is laag risico".
En dat we dan aan AI vragen van: “goh hè? Kan je dat ook nog eens een keer onderbouwen”? En dat nog eens een keer tegen onze eigen onderbouwing aan te leggen, om op die manier eigenlijk ons nog eens een keer extra te laten challengen.

Rico Schilder
Ja exact dus een beetje een soort extra test eigenlijk?

Participant 1
Ja.

Rico Schilder
Oké, dus eigenlijk in. In elk van deze stappen zou AI wel een functie kunnen bieden?

Participant 1
Ja absoluut en ook inderdaad vragen aan AI om beheersmaatregelen te definiëren die een risico afdekken. Zeker voor IT controls komt daar een goede set uit, over het algemeen.

Rico Schilder
Dus, dus dan zou je meer vertrouwen hebben in het opstellen van zo'n control, bijvoorbeeld dan zo een risicobeoordeling?

Participant 1
Ja.

Rico Schilder
Dat is een onderdeel wat wat meer gecontroleerd moet gebeuren, die risicobeoordeling?

Participant 1
Ja en het is ook welke AI tooling je gebruikt en hoeveel input geef je mee vanuit je eigen organisatie? Dus doe je het helemaal blanco? Dan zijn de resultaten natuurlijk anders, hè? Laat je AI puur op basis van de algemene kennis op het internet en die allemaal in dat taalmodel gestopt zijn met output komen of zeg je tegen je AI model: “Naast alles wat wat er de afgelopen jaren in dat model is gepropt vanuit internet, heb ik hier ook bij nog de organisatie specifieke documentatie, je hebt hier ook toegang tot het intranet, en by the way, ik ga jou heel gericht voeden met strategiedocumenten, jaarplannen, meerjarenplannen, budgetten, beleidsstukken, standaarden en ik wil dat je dat ook meeneemt in je risicobeoordeling". En er is ook de mate waarin je door je organisatie wordt toegestaan om dat te mogen doen. Ik denk dat dat heel erg de bruikbaarheid van AI, in het definiëren van je control framework, bepaalt.

Rico Schilder
Dus ook die AI ook echt trainen op je eigen historische data, zeg maar?

Participant 1
Ja en Ik weet niet eens of het trainen is, hè? Wij mogen binnen ORGANISATIE A nu de AI Bing gebruiken, wat is dat ook alweer? Ik gebruik zelf altijd ChatGPT, betaald. Ik gebruik het in mijn afstudeerscriptie trouwens ook voldoende. Dan stop ik gewoon literatuur in, dus dat is het model niet getraind op die literatuur, maar het model of ChatGPT leest wel de artikelen door die ik meegeef. Dus ik kan met ChatGPT prompten van: “Ik wil nu dat je deze 3 artikelen in ogenschouw neemt en wat zijn dan de belangrijkste punten die ik in mijn theoretisch kader moet meenemen?” Zo kan je dat natuurlijk ook zeggen van: “Ik stop deze ORGANISATIE A specifieke documenten, die attach ik, en ik vraag dan een risicoanalyse te doen, en daarin de content uit die beleidsstukken of die standaarden die organisatie documentatie daarin mee te wegen”. Dat geeft andere resultaten dan dat je gewoon blanco zegt: “Ik wil nu de risico's en de controls weten in een bepaald proces."

Rico Schilder
En denkt u dat uiteindelijk ook AI dat hele proces van het opstellen van zo'n controle raamwerk kan overnemen.

Participant 1
Ja. In grote mate wel. Ja, overnemen is een groot woord, hè, dus dat je zegt van: "nou, ik hoef geen controle framework meer op te stellen, dat doet AI wel voor mij en daar vertrouw ik op dat het helemaal goed zit". Met de nodige checks and balances denk ik aan de 80-20 regel, dat je 80% kan neerzetten.

Rico Schilder
Oké, maar wel nog onder controle van mensen?

Participant 1
Ja.

Rico Schilder
Gebruik je dan zelf ook AI bij binnen het bedrijf, binnen het risicomanagement?

Participant 1
Ja, dat is nog heel erg afhankelijk van de persoon, hè? Ik gebruik het volop. En ik gebruik het met name om te toetsen. Onze control framework is gebaseerd op procesdocumentatie, procesdocumentatie die door de organisatie zelf is opgesteld waarin alle processtappen zijn uitgewerkt, waarin de risico's zijn benoemd, waarin de controls zijn uitgeschreven, en vaak wordt aan mij gevraagd om dan te valideren. Is het ontwerp van dit proces goed?
Nou, de eerste check die ik doe is dat ik vraag aan AI om dat te checken.

Rico Schilder
Om een beetje een soort eerste stap op te zetten?

Participant 1
Ja hoor ja. En dan lees ik het zelf nog eens een keer door. Dan heb ik bepaalde twijfels en dan moet ik feedback geven. En dan zeg ik tegen het model van: "Nou weet je, ik twijfel over dit punt en hier zitten mijn twijfels. Kan je een advies formuleren om die twijfels weg te nemen?" Dan hoef ik tenminste zelf niet meer na te denken over hoe ik dat netjes formuleer en dan kan ik snel feedback geven en af en toe dan denk ik, voordat je dit mij aanlevert, waarom doe je dit zelf niet?

Rico Schilder
Dus wat ik wel merk is dat de manier waarop je dat prompt ook wel heel erg belangrijk is daarin. Moet wel goed weten, zeg maar hoe je dat moet vragen en hoe je een beetje moet poken om…

Participant 1
Ja, nou ja, dat denk ik wel dat je inderdaad enige ervaring moet opbouwen met dat soort modellen om te weten van: "Welke interactie moet ik hebben, hoe moet ik prompten?" En vaak is het ook gewoon een beetje vechten met het AI model voordat je het goede resultaat eruit krijgt. Ik weet niet hoe jij met je scriptie schrijven zit, maar hè, af en toe ben ik gewoon

dat ding aan het commanderen: “Ik wil het korter. Ik wil het korter, ik wil het zakelijker geformuleerd hebben en ik wil dat je deze artikelen betrekt en ik wil dat je geen eigen interpretaties daaraan geeft. Ja en dan komt hij weer iets en dan ben ik nog niet tevreden en dan gaan we net zo lang door totdat het totdat er output uitkomt waarvan ik het goed vind.

Rico Schilder
Ja oké. Nou ja, inderdaad veel vormen die gebruikt worden van AI zijn die je nu al ziet, bijvoorbeeld ChatGPT, dus dat generatieve AI, maar daarvoor komt natuurlijk ook NLP, natural language processing bij het verwerken van zo'n prompt en ook als je, zoals je zegt, bepaalde documenten als input levert erin. Ben je bekend met deze twee termen NLP en Gen AI?

Participant 1
Ja.

Rico Schilder
En deze types AI, die zouden dus wel gebruikt kunnen worden bij risicomanagement?

Participant 1
Ja, daar had ik het net de hele tijd over, generative AI. Het ligt in elkaars verlengde natuurlijk.

Rico Schilder
En je had het net al over het soort documenten dat als input gebruikt kunnen worden, dus dus wet en regelgeving, maar ook bedrijfsdoelstellingen. Dat soort dingen en misschien zelfs normenkaders. Maar wat voor type documenten zijn nou echt nodig en cruciaal bij het opstellen van zo'n controleraamwerk?

Participant 1
Hij ligt aan het doel van het control framework. Als iets compliance doelstelling heeft, dan moet je natuurlijk de wet en regelgeving of de normen kaders als input hebben.
Als het doel van control framework om aantoonbaar te maken dat je eigen interne beleid naleeft dan is je eigen beleid en de onderliggende basis en standaarden zijn de input, hè? Als het control framework er is om te zorgen dat ik mijn strategische of mijn tactische of mijn operationele doelstellingen haal, dan kom je meer op de inputdocumenten als je strategiedocumenten, je meerjarenplan, je jaarplannen, je kwartaaldoelstellingen. Het ligt eraan op welk niveau je natuurlijk je control framework wil gaan opbouwen. Vanuit security perspectief zat ik nog te denken dat je ook op externe bronnen wilt inprikken. Er zijn natuurlijk allerlei externe bronnen die informatie verschaffen over kwetsbaarheden in systemen, kwetsbaarheden die hackers gevonden hebben, achter deurtjes in Microsoft. Hé, daar kan je natuurlijk ook op inprikken waarbij je natuurlijk AI kan gebruiken om ook niet één keer je control framework op te bouwen, maar ook eigenlijk continu te checken of mijn control framework nog adequaat is, om te reageren op nieuwe externe omstandigheden.

Ik zat alweer echt een paar stappen verder te denken. Je kan natuurlijk een control framework heel erg opbouwen vanuit wet- en regelgeving of vanuit normenkaders en vanuit risico's, en dan allerlei theoretische controls bedenken. Maar je zou natuurlijk ook kunnen inprikken op processen, systemen, applicaties, en daar data uit kunnen halen en tegen AI

zeggen: “maak een control framework wat niet theoretische controles bedoeld, maar waarin je controles opneemt die ook daadwerkelijk zijn geïmplementeerd". Dit is even een paar stappen verder dan generative AI. Dus dat is denk ik AI die misschien nog niet bestaat, maar die je zou iets kunnen verzinnen van, je prikt met een bepaalde AI tooling in op standaard systemen SAP, Oracle, Microsoft, AWS, Azure, standaard systemen. Daarin hebben wij ook allerlei controls geïmplementeerd. En dat je dan zegt: "Vanuit die daadwerkelijke in de praktijk geïmplementeerde controls, zorg dat je daar een extractie van maakt en in je control framework neerzet."

Rico Schilder
Ja, dus dat je het eigenlijk een beetje aan het reverse-engineeren bent?

Participant 1
Ja, want nu heb je vaak dat vanuit de theorie nog vaak controls bedenken en dan die gaan implementeren. En dan moeten we aantonen dat we die controls effectief zijn. En dan blijkt er in de praktijk toch een mismatch te zijn tussen dat de control die in het framework staat en de controle die in de praktijk is geïmplementeerd, hè? Als je AI al gebruikt om de controles die je al daadwerkelijk in de praktijk hebt geïmplementeerd ten volste te benutten, en die controles alvast opnemen in je control framework dan heb je daar al winst te pakken, want dat zijn ook controls die je kan aantonen.

Rico Schilder
Dus als dat nog een keertje voorbij komt in een nieuwe normen set die je wilt adopteren, dat dat je dan ook kan zeggen: “ja, daar doe ik voldoend wel al aan”?

Participant 1
Ja nou die control, die heb je al.

Rico Schilder
Ja oké, Ik heb hem door. Interessant!

Participant 1
Dat doen we nog niet, hoor.

Rico Schilder
Nee, maar dat is goed. Dat is goed, want dat helpt ook voor future studies dit. Maar terugkomend op die verschillende input, types documenten, dat is wel echt context gebonden aan het soort risico's dat je wilt analyseren, zeg maar?

Participant 1
Nou ja, kijk, we hadden het net trouwens over die ernst beoordeling die we nog heel erg doen vanuit verschillende disciplines met mensen. We proberen dat ook steeds kwalitatiever te maken. Binnen het IT control framework kan je natuurlijk aan de ene kant bedenken van, we lopen het risico op phishing of lopen het risico op malware. En daar kan je allerlei controls voor bedenken. En, we kunnen daar zelf een risico-inschatting bij maken. “We vinden dit een heel hoog risico, want”. Maar je kan natuurlijk ook de data gebruiken uit je antimalware tooling hè? We hebben die tooling draaien en die tooling die houdt zoveel tegen en we hebben in totaal het afgelopen jaar met zoveel geïnfecteerde assets te maken gehad.

En daar zit een bepaalde trend in. Dat we zien het toenemen. Dat we vanuit AI een signaal krijgen van: “Dat risico wat jullie begin van het jaar als laag hebben ingeschat. Ja, let op, dat begint nu toch toe te nemen. Want je hebt steeds meer geïnfecteerde machines. Of dat risico is al aan het afnemen, want we zien gewoon steeds minder phishing mails binnenkomen. Die controls die jullie daarop hebben geïmplementeerd, jullie zouden kunnen overwegen de controls wat te gaan beperken.

Rico Schilder
Voordelig zijn om dat ook echt te combineren en te integreren met kwantitatieve data die je gewoon uit processen haalt?

Participant 1
Ja, en ik denk waarbij een control framework voorheen de afgelopen jaren dat een keer wordt neergezet en tuurlijk gaan we dat met een bepaalde frequentie beoordelen, actualiseren en ik denk dat je met AI een steeds dynamischer control framework gaat krijgen wat echt rekening houdt met het actuele risico beeld. Dat zou ik wel heel gaaf vinden, als we daar naartoe werken.

Rico Schilder
Ja, en zie je daar ook nog technische problemen voor wanneer je bepaalde soort documenten als input gaat gebruiken?

Participant 1
Het belangrijkste knelpunt is natuurlijk dat er een veelheid aan AI tools inmiddels beschikbaar is. Maar, je wil niet met elke gratis beschikbare AI tool op internet zomaar bedrijfsspecifieke documenten gaan voeden, want je weet niet wat er met die inhoud gebeurt. Dus dat is een obstakel, hè. Dus ja, ik vind dat je AI-tools die je gaat gebruiken in je bedrijfsspecifieke context, dat die gecheckt moeten zijn, dat afspraken met de leveranciers gemaakt zijn, et cetera ja, dus het moet onder bepaalde randvoorwaarden gebeuren.

Rico Schilder
Daar moeten ook weer controls voor komen?

Participant 1
Daar moeten we ook controls voor opstellen. Hé, je kan natuurlijk prima bepaalde documenten anonimiseren, alle gevoeligheden uit te halen, om met verschillende AI tools te gaan experimenteren. Dus ik zou en ik hoop dat, bij ORGANISATIE A zijn we er ook wel mee bezig met zo een AI labs in te richten, waarbij we gewoon een stukje sharepoint pakken die gewoon helemaal geanonimiseerd hebben, waarvan we in ieder geval met elkaar vastgesteld hebben dat hier allemaal documenten in instaan en die zijn gewoon goed. Daar zou iedereen bij mogen. Hè dus gewoon publieke documentatie en die gebruiken we om nieuwe AI mogelijkheden te toetsen en te kijken of dat waarde toevoegt.

Rico Schilder
Ja, ja, exact dus dat is ook een stukje veiligheid vooral, wat daarbij komt kijken?

Participant 1
En het andere is natuurlijk het risico dat we te veel gaan vertrouwen op de output. “Hé AI zei dat het geen risico was, en dus hebben we hier geen maatregelen genomen." Je hebt natuurlijk gewoon je eigen verantwoordelijkheid en aansprakelijkheid op dat vlak. Hé vandaar dat ik ook elke keer zeg van: “nee, Het is een hulpmiddel”.

Rico Schilder
Dus dus, wat voor problemen zou dat dan kunnen leveren als er te veel vertrouwen is in de output van de AI?

Participant 1
Nou ja, vertrouwen is prima mits je maar gevalideerd hebt en je zegt: “Ook al heeft de AI output het verkeerd gedaan. Dan aanvaard ik daarvan de consequenties. En dan ben ik daar ook voor gewoon aansprakelijk als bestuurder van een organisatie en, op de lagere niveaus als manager, ben ik verantwoordelijk voor mijn afdeling. Ik ben verantwoordelijk voor goed risicomanagement. Ja, ik laat AI mij ondersteunen, helpen, maar ik kan nooit de schuld geven aan AI omdat hij risico's verkeerd heeft ingeschat en mij niet gewezen heeft op bepaalde risico's of een verkeerd control framework heeft voorgeschoteld”.

Rico Schilder
Dus dit zou ook een beetje terugkomend op dat stukje waar we het eerder over hadden, over dat mensen wel handig moeten zijn en ook gewoon echt getraind moeten zijn in het gebruik van die AI. Daarnet hadden we het over hoe je moet vragen en moet prompten. Dus iemand zou wel echt AI-vaardig moeten zijn?

Participant 1
Ja, je moet het op waarde kunnen schatten.

Rico Schilder
Ja exact, maar zal dat niet lastig zijn? Want hoe kan je dat testen?

Participant 1
Ja, wat wil je testen? Testen of de output goed is of testen of mensen AI-savvy genoeg zijn om het op waarde te kunnen schatten?

Rico Schilder
Nee of de output goed is, want je had het over het valideren daarvan van de output.
Maar dat moet ook wel goed en secuur gebeuren, denk ik?

Participant 1
In het in de huidige in het hier en nu zeg ik van, we hebben gelukkig voldoende oude rotten in het vak rondlopen die het al 20 jaar gedaan hebben. He, die dan ja, de output op waarde kunnen schatten. Ik zit al wel 20 jaar verder te denken. Hé, zijn er dan nog steeds mensen die dan de output op waarde kunnen schatten? Daar kan je vraagtekens bij zetten.

Rico Schilder
Maar misschien is het dan wel niet meer nodig, omdat die modellen dan zodanig verbeterd zijn.

Participant 1
Ik vraag me af of de student van tegenwoordig nog zelf een scriptie zou kunnen schrijven.

Rico Schilder
Ik wilde zelf literatuur vinden over een bepaald onderwerp en toen vroeg ik aan ChatGPT om bronnen voor me te vinden over dit onderwerp, maar de bronnen had hij compleet verzonnen, want de auteurs bestonden, maar de titels waren niet te vinden. Hij had het gewoon compleet verzonnen

Participant 1
Heb je de betaalde versie gebruikt?

Rico Schilder
Nee, dat niet. En misschien dat daar nog wel een verschil in zit.

Participant 1
Ja, want je kan dus ook andere modellen gebruiken. Andere ChatGPT's, want er is ook ScholarGPT en ConsensusGPT. Hé, waar volgens mij is de ScholarGPT eigenlijk op Google Google Scholar gebaseerd. Dat gebruik je denk ik wel, hè?

Rico Schilder
Ja, Google scholar wel ja.

Participant 1
Die daarop is ingeprikt en consensus is weer op een andere database met allemaal literatuur is ingeprikt. Ook probeer ik weleens dezelfde prompts in die verschillende modellen te zetten en dan te kijken wat het verschil is qua output.

Rico Schilder
En levert dat veel verschil?

Participant 1
Ja, afhankelijk van de vraag die je stelt. Bij sommige vragen is dat een op een. Nou, er zitten hier en daar een paar woorden verschil in. Dan ga je hele gerichte vragen stellen, en dan kunnen die antwoorden ook wel enorm uiteenlopen. En dat is natuurlijk ook weer, hè? Hoe ga je AI toepassen in dit verhaal? Ik kan me inderdaad voorstellen dat er op een gegeven moment speciale control framework GPT's zijn die al dusdanig getraind zijn dat ze puur op control frameworks fantastisch goed werk doen. En zolang dat er nog niet is, kan je natuurlijk, de reguliere gebruiker, die zal in de gratis versie van ChatGPT of een ander model, het proces erin plotten, en de geavanceerde gebruiker die gaat betaalde versie gebruiken. Ik ga eens een aantal andere GPT's die speciaal getraind zijn, ga ik eens gebruiken en ik ga dan eens antwoorden vergelijken. En ik gebruik het beste antwoord.
En ik als mens heb nog steeds voldoende vertrouwen in mezelf dat ik het beste antwoord uit de verschillende antwoorden kan destilleren. En je kan ook weer aan een GPT vragen van:

“Ik heb nu aan 10 GPT’s een antwoord gevraagd. Adviseer mij wat nou het beste antwoord is”.

Rico Schilder
Nou interessant. En zie je dan ook nog bijvoorbeeld ethische problemen ook voor je wanneer je zoveel documenten gebruikt bij het opstellen van die controls.
Want we hadden het net over veiligheid.

Participant 1
Nou, ja, ik zit al direct te denken van ja, hè? Je zou het natuurlijk aan de AI kunnen vragen van: “gegeven dit control framework, ik wil fraude plegen. Hoe dan? Of nou, gegeven dit control framework. Ik wil onder de radar inbreken in dit systeem. Kan je me helpen, hoe dan? Ik wil gegeven dit control framework met maar een bepaalde autorisatie limiet, hoe kan ik de situatie dusdanig gamen?” En binnen het Financial Control Framework hebben we bestellingen boven bepaalde bedragen, en die moeten eerst goedgekeurd worden door een budgethouder. Dat je medewerkers dan in de gelegenheid stelt van: “Nou ja, weet je, ik wil iets inkopen, maar ik wil geen goedkeuring vragen van wat mijn budgethouder, hoe kan ik daar nou op slimme manier een omweg voor bedenken?” Dat zou een ethisch bezwaar kunnen zijn. Het AI model dat we dan gebruiken om een control framework vorm te geven, heeft zicht op de belangrijkste risico's, dat heeft zich op de belangrijkste controles en zou dus ook theorie kunnen adviseren hoe daar misbruik van gemaakt kan worden.

Rico Schilder
Daar zeg maar een maas in de wet vinden?

Participant 1
Ja.

Rico Schilder
Ja exact. Nou ja, zo heb ik er ook nog niet tegenaan gekeken.

Participant 1
Maar wat voor ethische bezwaren zat jij zelf te denken dan?

Rico Schilder
Nou er is best wel veel onderzoek naar ethiek en AI. Dat AI bijvoorbeeld ook wel zogenaamd fair moet zijn, dus dat de gebruikte data zeg maar traceerbaar is en dat het niet discrimineert op basis van historische data. Zou zoiets ook van toepassing kunnen zijn wanneer je een heleboel documenten gebruikt om een control te formuleren of voor risicoanalyse?

Participant 1
Ik vertelde je net even in de introductie over de data science initiatieven, bijvoorbeeld om het betaalgedrag te voorspellen ten aanzien van debiteuren. AI modellen kunnen ook inprikken op data om uiteindelijk je control framework vorm te geven. En, wij zagen op basis van data dat er in bepaalde postcodegebieden slechter betaald wordt. En dat hangt samen met inkomen. Dat hangt samen met opleidingsniveau en dat hangt ook samen met etnische afkomst in de wijken, waar veel arbeidsmigranten wonen en waar het opleidingsniveau nog niet zo hoog is en waar de inkomens niet zo hoog zijn. Daar zijn de betalingsachterstanden

over het algemeen ook hoger. En AI zou een model kunnen bedenken met een afhankelijkheid van de achternaam. "Heet jij schilder? Dat klinkt als een Nederlandse achternaam, dan zal jij wel goed betalen en heet jij Mustafa, weet ik veel. Dat klinkt als een niet Nederlandse achternaam, dus dan zal je wel niet zo goed betalen". En als je daar dan in inderdaad heel je control framework onderscheid in gaat maken, en het control framework komt met controls van nou mensen met dit soort achternamen zou je niet moeten accepteren als klant, want die betalen slechter en dan heb je straks last van in je liquiditeitsrisico. En daar moet je voor waken. Dat mag niet gebeuren.

Dat is pas meer aan de hand wanneer je het AI gaat gebruiken op daadwerkelijke data dan wanneer je AI gaat gebruiken om vanuit doelstellingen, wet- en regelgeving, procesdocumentatie, en beleidskaders een control framework vorm te geven. Maar ja, daar zitten natuurlijk risico's in.

Rico Schilder
Hoe zou dat het best voorkomen kunnen worden? Heb je daar, heb je daar een visie op?

Participant 1
Nou ja, dat je AI gebruikt als tool om je controle framework op te bouwen en actueel te houden en te toetsen, maar dat je uiteindelijk zelf nog gewoon in de lead bent om je control framework vast te stellen.

Rico Schilder
Ja oké ja dus die menselijke controle moet sowieso blijven?

Participant 1
En, ik denk ook dat je je ethische normen kader je ethisch kader eigenlijk ook wel weer als input kan gebruiken. Waarbij het AI model daar ook weer rekening mee houdt. Ik denk dat het AI model zelf dan niet met dit soort controles komt. Als je dat maar goed meegeeft.

Rico Schilder
Ja, dat is een goeie inderdaad. Dat je echt verschillende normenkaders en doelstellingen laat combineren.

Participant 1
Ja. Hè, dus eigenlijk zou het AI model wat je gebruikt om je control framework te definiëren een soort ethisch kompas mee moet geven in de prompt, en dan loop je dit risico een stuk minder. Kijk en volgens mij, in ChatGPT is dat er al. Daar kan je ook bepaalde dingen niet aan vragen, hè? Als je vraagt: "Hoe bouw ik een bom?" Dan is het best wel lastig om daar antwoord op te krijgen. "Hé, hoe kan ik mijn kinderen het beste mishandelen?" Dat is ook een vraag die je kan stellen aan ChatGPT, maar waar je dus een antwoord op krijgt wat wel binnen de kaders past van het ethisch kompas dat aan zo'n model is meegegeven.
En nu, zijn er natuurlijk allerlei internetfora waar mensen elkaar gaan vertellen hoe je ChatGPT dusdanig kan prompten, waardoor GPT wel vertelt hoe je een clusterbom in elkaar zet. Het kan dus wel, maar het is wel. Het wordt wel moeilijk gemaakt, laat ik het zo zeggen.

Rico Schilder
Ja exact, in principe dan zegt hij gewoon niets van: “Sorry, dat kan ik hier niet zomaar vertellen, toch?"

Participant 1
Ja ja ja.

Rico Schilder
En wat is dan essentieel voor het gebruikers aspect wanneer AI wordt geïmplementeerd binnen het proces?

Participant 1
Nog een keer de vraag?

Rico Schilder
Dus wat is essentieel voor het gebruikers aspect? Dus als ik als gebruiker AI wil gebruiken voor het opstellen van zo'n controlewerk.

Participant 1
Oké, dus de gebruiker is degene die een opdracht krijgt om een control framework te bouwen?

Rico Schilder
Ja exact en daarvoor gebruikt die een AI tool. En wat is dan voor die gebruiker ook echt essentieel?

Participant 1
Ja, control framework GPT. Wat is dan? Nou ja, ik denk dat we heel veel van die elementen geraakt hebben. Dat de organisatiecontext mee wordt gegeven en eigenlijk al die input documenten dat het model daarop is ingeprikt. Hè, dat je dus als gebruiker niet ellenlange prompts moet schrijven om overal rekening mee te houden. Dus dat het AI model al een framework bouwt vanuit een bepaald kader. Dat kader moet helder zijn, want anders heb je dus een hele geavanceerde gebruiker nodig die weet hoe je dat kader meegeeft en weet hoe je kan prompten en heel erg veel dialoog voert en met veel verschillende GPT’s gaat werken om uiteindelijk tot een het beste control framework te komen. Maar vanuit het gebruikersperspectief en gebruikers gemak, dan moet de AI snel zijn, kwalitatief goede antwoorden geven, en er moet weinig interactie nodig zijn. De output moet volledig zijn. Je wilt zeker weten dat dat enorme kader volledig is afgedekt, en je wilt zeker weten dat met die set aan controls een bepaalde doelstelling wordt gehaald. Dus er zullen wat parameters meegegeven moeten worden, maar puur een control framework is afhankelijk van de doelstellingen van de organisatie, he?

Ik bedoel, je kan een control framework opbouwen met alleen de key controls, maar je kan ook zeggen van nou, weet je, ik wil wat redundantie in mijn control framework hebben, dus ik wil naast mijn key controls ook mijn non key controls hebben. Dus hè, op het moment dat bepaalde key controls falen, dat ik nog ergens op kan terugvallen. Een andere organisatie zal zeggen van: “nee, ik wil hem echt beperken tot het essentiële". Dus je wilt bij het opstellen van je control framework wel een aantal parameters meegeven rondom risico en

risicobereidheid. En je kan aan een model vragen: “Ik wil mijn top 3 risico’s of mijn top 5 risico’s, of ik ben heel risicoavers, en ik wil al mijn risico’s in kaart brengen.” En er is een verschil tussen het soort organisatie, er is een verschil tussen NASA, een bank, of de bakkerij op de hoek. Maar ook dat is weer context natuurlijk. Je moet dus eigenlijk een soort requirementsanalyse doen op de AI tool die een control framework gaat bouwen, en dan kan ik me voorstellen dat dit soort requirements uitkomen, die je als gebruiker verwacht van zo’n tool. Dat het rekening houdt met context, risicobereidheid, het type organisatie, de mate detail die ik als gebruiker erin wil hebben. Ik kan me ook zo heel veel voorstellen dat een gebruiker van een multinational waarin ze volledig op SAP over zijn qua ERP systeem, en je hebt nog een paar aanpalende systemen, maar het totale systeemlandschap is heel beperkt en overzichtelijk. Dat de gebruiker in dat geval verwacht dat die AI die SAP tool gewoon heel goed kent, versus een andere organisatie waarbij en nauwelijks standaard pakketten en applicaties zijn en dus die verwachting helemaal niet heeft. Beetje in de oude wereld nog. Wij kochten 10 jaar geleden Oracle ABS, en daar kon je ook Oracle GRC bij kopen. En in dat Oracle GRC stond eigenlijk dat hele control framework. Wat helemaal gebaseerd was op de standaard inrichting van Oracle, met alle risico's en alle controls erin en die waren er ook al rechtstreeks ingeprikt. Als jij gewoon een organisatie hebt die alles in Oracle ABS deed, ja, dan hoeft hij eigenlijk helemaal geen control framework meer op te bouwen hè? Dan kocht je dat gewoon aan. En voor SAP is dat ook zo. Als je gewoon standaard in SAP zit, dan is jouw control framework ‘dat’. Dat kan je nog wel beetje tweaken, beetje tunen. Maar gebruik je al dat soort standaard die systemen niet of heb je nog heel veel andere systemen erbij? Dan moet je veel meer zelf nadenken over je control framework dan bij andere organisaties en dan gaat AI jou juist daarbij heel erg helpen.

Rico Schilder
Ja, dus het is juist in die scenario's waarbij je een vrij complexe context hebt, waar AI je heel erg kan helpen?

Participant 1
Ja.

Rico Schilder
Oke, en hoe zou dan het beste die context overgebracht kunnen worden op AI? Zou dat kunnen of of heb je daar alsnog echt die mens voor nodig? Of, zou je dat kunnen doen door een aantal documenten erin te gooien en dan…

Participant 1
Nou ja, in best practice is het zo dat veel organisaties relevante kaders ook gepubliceerd zijn op het internet. En bij ORGANISATIE A nog niet hoor, maar een volwassen organisatie heeft zijn… Nee trouwens, ik denk dat het taalmodel ook wel documenten kan scannen en classificeren, als zijnde van “Dit is beleid, want ik zie hier in dit beleidsstuk staan dat iets is goedgekeurd door een directie, en ik zie dat het als een beleidsstuk wordt gecommuniceerd, versus iets anders”. Op internet zweven nog allerlei soorten werkdocumenten, dus dat onderscheid kan het model ook zelf al aangeven. Ik denk dat je met een standaard koppeling met het internet of een confluence site of een aantal van dat soort dingen, al noem je dat samenwerk tools binnen organisaties, dat je daarmee die tool met context kan voeden.

Rico Schilder
Oké ja, top. Ja, dan denk ik dat we al mijn van tevoren bedachte vragen zo een beetje wel hebben gehad.

Participant 1
Wat heb ik niet geraakt? Waarvan jij dacht van nou dat zou die wel geraakt hebben? Of heb je zelf nog ideeën waarvan je denkt van hé?

Rico Schilder
Nou ik dacht vooraf wel echt dat generative AI kan helpen bij het maken van controls, helemaal in zo'n GRC tool. Dat je daar documenten in doet als input, en op basis daarvan een aantal controls opstelt, waarin staat hoe de control het best aangepast kan worden, en misschien zelfs wie er het best verantwoordelijk kan zijn voor de control, en dat hij dat soort dingen dan op een rijtje zet. Een risicoanalyse is iets dat al best veel gebeurt in financial risk, maar in IT risk wat minder. Of tenminste, ik heb het nog niet heel veel voorbij zien komen. Misschien hier en daar in wat LinkedIn posts, maar dat is vrij moeilijk om in mijn scriptie te verwerken natuurlijk. En ik loop wel een paar maanden stage nu, en ik pik hier en daar wel wat op van collega's, en we praten veel over het onderwerp, maar ik weet nog niet alle ins en outs van het risico-proces. Dus dat is heel interessant om te horen hoe dat zo samenhangt en hoe AI daar eventueel in te pas kan komen en wat jouw visie daarop is. Want het zou cool zijn inderdaad, als het gewoon in zo een GRC tool gewoon geïntegreerd is, toch?

Participant 1
Ja ja tuurlijk. Je koopt je GRC tool in de beloftes dat je eigenlijk niks meer hoeft te doen. Je hoeft dan niks meer in te vullen met proces risk en controls. Je installeert het, je geeft aan waar je sharepoint staat, je geeft aan wat je er ongeveer in wilt hebben, en 'generate the framework'. Het wordt zo ingevuld. En by the way, dit is je netto risico en daar zitten je verbeterpunten. Klik hier en dan informeren we de toezichthouder erover.

Rico Schilder
Ja, dat is wel het Utopia, zeg maar.

Participant 1
Ja, het zou mooi zijn.

Rico Schilder
Ja. Nou, in ieder geval heel erg bedankt voor je tijd. Ik vond het een interessant interview! Je hoort van me hoe verder.