Curriculum Vitae

Ir.drs. Jurgen van der Vlugt CISA CRISC – exRE

Profiel

Ik ben sinds september 2025 consultant bij Xebia, gericht op advies en implementatie van GRC-frameworks en processen; beheersing van AI voor, tijdens en na het ‘maken’ ervan; kwantificering van operationele risico's en weerbaarheid tegen cyberbedreigingen.

Daarvoor was ik als zelfstandig professional of op kortlopend contract werkzaam in het risk- en security-domein, soms in team lead rollen, via onder andere Securesult, Marsh Risk Advisory, Secura, BDO Advisory, het Internationaal Strafhof, bij ministeries en multinationals tot en met kleine MKB.

Ik ben tevens IT-auditor en -adviseur geweest in vaste dienst bij diverse organisaties als Noordbeek, Achmea, ABN AMRO Bank en KPMG. In het begin als IT-auditor, maar steeds meer overhellend naar niet-alleen-maar-vinkende assessor/adviseur op de breedte van IT-management en beheersingsvraagstukken, laatstelijk voornamelijk bezig met algemeen ERM/ORM, BCM, privacy én (audit van) OT.

Hierbij heb ik, na een aantal snelle stappen, tevens snel de omschakeling gemaakt van alleen-maar uitvoerend naar opdrachtportefeuillebeheer, teamleiding en relatiemanagement met klanten en andere stakeholders.

Daarnaast heb ik jarenlang een eigen wijnimport en -handel gehad, met accijnsvergunning, voorraadadministratie, logistieke zaken et al. – met aandacht en als auditor natuurlijk volgens het boekje…

Kennis en kracht

Mijn hart ligt bij het onderzoeken op toepasbaarheid van alles wat Nieuw is in onze vakgebieden. Strategie, tactieken en operationele implementatie opzetten en, welwillend kritisch, beoordelen.

En actief zijn in het vakgebied hoort er bij. Bijna altijd heb ik een bijdrage geleverd in de commissies en werkgroepen van o.a. NOREA, ISACA, ISSA, PvIB en PRMIA, heb ik les gegeven en geëxamineerd aan hogescholen en universiteiten, en ik publiceerde regelmatig in nationale en internationale vakbladen en conferenties. Ook was ik jarenlang bestuurslid van de Netherlands-Canada Chamber of Commerce, o.a. voor business/academic exchange op IT/AI-gebied en natuurlijk voor de wijnhandel.

Over de persoon

Zie https://maverisk.nl/volledig-ik/

Contact

Zie:

- https://www.linkedin.com/in/jurgenvandervlugt/
- https://maverisk.nl/volledig-ik
- jvdvlugt@xs4all.nl / +31-(0)6-206.648.23 / Amstelveen

Wat ik zoek

Is een rol met voldoende breed verantwoordelijkheidsgebied maar toch ook nog inhoudelijke betrokkenheid, waarin de volgende aspecten aan bod komen:

- Adviseren en besluiten over, en managen van, verbeteringen en innovatie; van klein tot transformatief – Doorlopend (Enterprise / Operational / Information) risk management (voorbij 3LoD, inclusief kwantitatief), met de zo hard nodige helderheid over de vertaalslag van business continuity risico's naar controls en terug en implementatie van Policy-as-Code en Controls-as-Code;
- Idem, inzake effectief, business process re-engineering gedreven implementeren van 'Artificial Intelligence' / Machine Learning; tools inzetten waar die nuttig zijn én met de beheersing die daarbij hoort;
- Effectief (balanceren met) communiceren, van Board-level discussies tot operationeel niveau); relatiegerichte diplomatie t/m hard op de bal – wat past. Dat, in een open cultuur, niet ambtelijk, niet saai, geen 'Hollandsche' bureaucratie;
- Niet: meer van hetzelfde, bureaucratie, DigiD- of andere pure-compliance auditing, procedures schrijven, ISAE3402, blij worden van IIA/NOREA "kwaliteitszorg". Hooguit nog eens een keertje, maar verder is minimaliseren van rapporteren-zonder-impact en vinken-om-het-vinken een vrij harde eis;
- Geen Sales targets. Oren en ogen openhouden en pre-sales samenwerken met Sales kan uitstekend, maar ik ben géén rain maker. Billability targets hou ik ook niet van! maar ja.

Omgeving

- Werken / schrijven / rapporteren in het Engels: Voorkeur;
- Internationale angle is een pré (regelmatig werken in het Engels en/of met int'l collega's);
- Leiding geven: Zeker. Hoewel niet vanachter het grote bureau maar voordoen en samenwerkend;
- Organisatie- c.q. dienstontwikkeling: Zeer graag. Een halve stap voorlopen op de behoefte, tijdens projecten of opdrachten verder uitwerken (op maat van de behoefte, maar lerend), en daarna lichtjes standaardiserend;
- Humor: Ja graag, van het drogere soort.

Formaliteiten

- Tarief – snelle transparantie bouwt vertrouwen; onduidelijkheid breekt die af! – €8500 per maand als basis – u kunt een overstap uiteraard nog prettiger maken… De 8% Vakantie, 13e et al., en auto(vergoeding) erbovenop;
- Vast contract. Als 'het niet werkt' tussen mij en werkgever, ben ik professioneel genoeg om zelf wel weg te gaan – ik ben geen risico maar neem dat wel. Jaarcontract(en), dat is toch echt voltooid verleden tijd, en een teken van wantrouwen mede in het eigen beoordelingsvermogen – ik start liever gelijk positief;
- Met een voorkeur voor Randstad-Noord (Noord-Holland, Noord-Zuid-Holland, Utrecht) als standplaats;
- Indien de OV- of auto-woon-werkafstand op relevante tijden groter is dan 75 minuten, dan is woon-werkverkeer in werktijd;
- Buitenlands reizen voor klussen: Graag! Mits 5% tot maximaal 15% werktijd; West-Europa, Noord-Amerika, en wat ME.

Bovenstaande blijft mijn wens. Maar als er dan bij huidige werkgever een aantal (sic) punten de andere kant heen gaan, bij een zwakke klantwervingsvaardigheid en -portefeuille, dan komt er van bovenstaande inmiddels niet veel. Zonder zicht op verbetering, want de strategie blijft een geheel andere kant opstaan, zit ik nu wat procedures op te stellen en tools te vullen met de zoveelste 'implementatie' die een junior ook zou moeten kunnen. Zonde ik kan en wil zo veel meer…

Vandaar dat ik een goede plek zoek in de adviseringswereld of in een interne functie-met-voldoende-uitdaging. Met veel flexibiliteit en een energievoorraad.
Wie biedt de juiste mogelijkheid om die in volle positiviteit nuttig te kunnen inzetten?

Werkervaring

Organisatie: **Xebia**
Functie: **Consultant**
Periode: **September 2025 – heden**

Voor adviesdiensten en consultancy. Meest recente opdrachten:

- Advisering over de implementatie van structurele oplossingen van pentest-uitkomsten;
- Adviseren en coördineren van implementaties van nieuwe 'guardrails' controls voor een VC/incubatorbedrijf met gebruikmaking van Policy-as-Code en Controls-as-Code;
- Opzetten van controls voor compliance voor de managed service-diensten.

Organisatie: **Maverisk Consultancy, IS Audit and Advisory services**
[Januari 2020 – augustus 2025 via BDO Advisory Risk Services, Secura, Marsh en Securesult]
Functie: **Zelfstandig Professional, parttime (AP-geregistreerd) FG, Principal en Teamleider**
Periode: **Januari 2012 – augustus 2025**

Leidinggeven aan en uitvoeren van diverse audit- en adviesopdrachten, waaronder:

- Laatste opdracht: Het opstellen, implementeren en initieel als CISO uitvoeren van een ISMS in een snel bewegende agile/DevOps scale-up-organisatie (full stack security);
- Een aantal audit- en adviesopdrachten over cybersecurity vanuit een ISO 27001-perspectief (inclusief integratie van NIST, BIO en NEN7510) in combinatie met IEC 62443 (inclusief NIS/WBNI-compliance), resulterende in agile maar organisatiebrede In Control-status;
- Een onderzoek naar de organisatie en management van cybersecurity bij een groot bouwbedrijf. De risico-geprioriteerde adviezen varieerden van management van de organisatieverandercapaciteit tot details over interne kwetsbaarhedenscans en de prioritering in opvolging ervan;

- Het opzetten en helpen in gang zetten van een organisatiebrede informatiebeveiligingsstrategie en bijbehorend beleid voor een grote organisatie in de machinebouw, met een focus op IT-leveranciersmanagement;
- Ondersteunen bij het implementeren van volwassenheidsverhogende maatregelen uit hoofde van DNB-regulering bij een van de grootste pensioenfondsen;
- Het implementeren en beoordelen van control-frameworks voor Avg-compliance en BIA-gedreven Avg-implementaties bij een groot zorginstituut en bij een middelgroot bouwbedrijf;

- Het opzetten en initieel uitvoeren van de CISO-functie bij een netwerkorganisatie in de IT-sector;
- Adviesdiensten voor een reeks publieke organisaties (nationale en lagere overheden) over informatiebeveiligingscertificering, privacy-aangelegenheden, het integreren van informatie- en privacyveilig gedrag in dagelijks werk, de beveiliging van netwerken en IoT/Operational Technology infrastructuren (tot PLC-niveau); de nadruk lag op vertaling van GRC-vereisten naar praktische, haalbare implementaties door de hele organisaties;
- Adviseren bij de ABN AMRO ISO-afdeling over het global information security risk-control framework (wereldwijde richtlijnen, lokale implementaties);

- Opzetten en tijdelijk invullen van een CISO-rol bij een kleinere zorginstelling;
- Audit-, review- en adviesopdrachten op issues van operationeel en informatierisicomanagement ten opzichte van diverse industriestandaarden (incl. NIS/WBNI-vergelijkbare standaarden) bij overheidsinstellingen;
- Bij het Internationaal Strafhof, fungeren als Auditor Information Technology: het managen van de IT-audit portefeuille en relatiemanagement (op alle niveaus), uitvoeren en leidinggeven aan statutaire IT audits op IT, op de IT-organisatie, op de information risk-managementstrategie en -uitvoering en op informatiebeveiliging; fungeren als onafhankelijk adviseur over beveiliging van communicatie-infrastructuren en technologie-innovaties.

Organisatie: **Achmea/ Eureko Internal Audit**
Functie: **Senior IT auditor**
Periode: **Januari 2011 – december 2011**
Uitvoeren van internal audits, inclusief zorgorganisatie-issues; auditobjecten varieerden van IT-processen tot Informatie-GRC-processen maar vooral betrekking hebbend op beoordeling en advies op operationele en informatiebeveiligings-risicobeheer framework implementaties binnen de Lines of Business en op Holding-niveaus.

Organisatie: **Noordbeek Consultancy**
Functie: **Senior Manager IT Audit/ Advisory services**
Periode: **Juni 2006 – december 2010**
Leidinggeven aan en uitvoeren van diverse implementatie-, audit- en adviesopdrachten op de gebieden van strategisch IT-management, informatiebeveiliging- en risk control, IT-management frameworks, GRC-implementaties, en full-stack technische beveiliging bij klanten variërend van ministeries (Defensie en andere) en multinationals, tot kleinere publieke en private (MKB-) organisaties. Het integreren van ISO 27001- en IEC 62443-frameworks tot geïntegreerde strategische en tactische In Control processen. Een kleine selectie van uitgevoerde opdrachten:

- Leidinggeven aan en uitvoeren van een audit op, en dringend adviseren bij een organisatiebrede implementatie van een management control framework voor informatiemanagement bij een Defensieorganisatie;
- Leidinggeven aan en uitvoeren van (assurance/compliance-gerichte) audits bij een reeks van klanten;

Organisatie: **ABN AMRO Bank, Group Security**
Functie: **Group Information Security Coordinator**
Periode: **Oktober 2004 – mei 2006**
Verantwoordelijk voor de wereldwijde integratie van fysieke- en informatiesysteembeveiliging inclusief coördinatie van de wereldwijde beleidsontwikkeling daarvoor, en het opzetten van anti-cybercrimestrategieën. Diverse (forensische) projecten en implementaties van hoogvertrouwelijke communicatiemiddelen.

Organisatie: **ABN AMRO Bank, Group Audit Corporate Center**
Functie: **Manager IS Audit**
Periode: **Mei 2001 – september 2004**
Leidinggeven aan en uitvoeren van diverse (wereldwijde) audit- en adviesrollen, meestens gerelateerd aan informatiestrategie, beveiligings- en managementframeworks voor informatie- en IT-management, en GRC-compliance. Adviseren in een brede relatiemanagement-rol van SVP- tot RvB-niveau, over de integratie van bankprocessen (op tactische en strategische niveaus), informatie- en algemeen risicomanagement, audits op IT-veranderprocessen en tactische / operationele IT-aangelegenheden. Een selectie van uitgevoerde opdrachten:

- Leidinggeven aan en uitvoeren van een audit op een geconsolideerd wereldwijd HR-systeem (voor 180k fte);
- Leidinggeven aan en uitvoeren van een audit op een Asset-Backed Securities systeem;
- Leidinggeven aan en uitvoeren van een audit op het systeem voor geconsolideerde financiële verslaggeving.

Organisatie: **IQUIP (nu Sogeti)**
Functie: **Information Systems Auditor en Consultant**
Periode: **April 2000 – mei 2001**
Leidinggeven aan en uitvoeren van diverse audit- en adviesopdrachten op een breed IT-terrein gerelateerd aan informatiebeveiliging en aan de kwaliteit van IT-management (control).

Organisatie: **KPMG EDP Auditors**
Functie: **IT Audit Manager**
Periode: **Maart 1995 – april 2000**
Leidinggeven aan en uitvoeren van diverse audit- en adviesopdrachten op een breed IT-terrein, meestens gerelateerd aan technische informatiebeveiliging. Een selectie van uitgevoerde opdrachten:

- Ontwikkeling en uitrol van de Security en Audit van Windows NT line of business, idem van de Y2k business;
- Informatie- en IT-beveiligingsaudits uitvoeren (in teams, soms solo) bij enige tientallen klanten;
- Uitvoering van een wereldwijd second-opiniononderzoek op Y2k-projecten voor een bekende bierbrouwer.

Organisatie: **322 sqn RNLAF / St1Lk/G2Lucht**
Functie: **Luitenant Intell/ ground liaison officer**
Periode: **1990-1991**
Gedurende de militaire diensttijd vanuit de Staf 1e Legerkorps tewerkgesteld op vliegbasis Leeuwarden als Ground Liaison Officer / Intell Officer bij een F16-squadron; met als taken onder andere het beheer over cryptografische materialen en NATO-strategiedocumenten, missie-instructies / debriefing aan vliegers. NATO CTS Atomal clearance.

Trainingen

Jaar	Cursus	Diploma
2019-2020	Journalistiek Schrijven; Hogeschool Utrecht	nvt
2002	Certified Information Systems Auditor (CISA); ISACA	•
2025	Champagne Connaisseur (niveau 2) tevens bètatester; Comité de Champagne	•
2023	Korte opleiding Wijnschrijven; Wijn Academie	•
2016	Bourgogne Terroir en Wijn; Wijninstituut	•
2014	Kort MBO Basis Gastronomie; Wijn Academie	•
2011	SDEN 2/3 (WSET3); Wijninstituut	•

Opleidingen

Jaar	Opleiding	Opleider	Diploma
1995-1998	Postdoctoraal IT-auditing	Vrije Universiteit Amsterdam	•
1992-1995	Ingenieur, Technische Informatica	Technische Universiteit Delft	Cum Laude^{+}
1990-1991	Diverse Electronic Warfare cursussen	Ministerie van Defensie	nvt
1984-1990	Doctoraal Bedrijfseconomie	Erasmus Universiteit Rotterdam	•

Talen

	Lezen	Schrijven	Spreken
Duits	Gevorderd (Kant, Nietzsche, Heidegger, Schopenhauer, Canetti, Musil)	Redelijk	Goed
Engels	Uitstekend (Hume, Joyce)	Uitstekend (zakelijk)	Uitstekend
Frans	Redelijk (wijn-auteurs)	Basaal; redelijk met LLM-gebruik	Enigszins (over wijn)
Italiaans	Puzzelend met woordenboek (inzake wijn)	Niet	Met de hand

Neven- en vrijwilligerswerkzaamheden

Organisatie	Rollen
NOREA	Lid, Commissie Educatie; voorheen penvoerder Werkgroep Adviesdiensten, lid en voorzitter van de Commissie Educatie, lid Commissies Vaktechniek, Herziening Beroepsregels en Editorial Team
NEN	Voorheen lid, Normcommissie Cybersecurity & Privacy
ISSA	Voorheen voorzitter en secretaris Dutch Chapter, lid van het Global Ethics Committee
PvIB	Voorheen voorzitter iB Magazine artikelprijsjury
ISACA NL	Voorheen Board member
PRMIA	Voorheen Subject Matter Expert
MSM Maastricht	Voorheen Adjunct Professor Executive MBA Program
Hoger onderwijs	(Voorheen) lesgeven aan een meerderheid van de Nederlandse universiteiten en HBO's
Haagsche Hogeschool	Voorheen Extern Gecommitteerde bij slotexamens
Diversen	Conferentie-, gast- en roundtable-presentaties en -dagvoorzitterschappen in Nederland en wereldwijd
Diversen	Artikelen en posts publiceren over vaktechnische ontwikkelingen
Diverse Goede Doelen	Diverse ondersteunende activiteiten

Passie

Ik loop warm voor:

- Ons vak. Ben sinds 1979 al met ponsband, teletype en 2-complement binair rekenen in de weer geweest, en daar zijn in de loop der vele jaren organisatie-inrichtingsvraagstukken, accountancy en audit, informatiebeveiliging in alle facetten, information risk governance en project risk management, en de laatste jaren ook operationeel en kwantitatief risicomanagement bij gekomen. Daarover publiceer ik graag, en sta met veel zin voor cursus-, seminar-, conferentie- en collegegroepen op de bühne.
- Wijn en gastronomie – met vele jaren een eigen wijnimport en -handel (met accijnsvergunning et al.), nu vooral gericht op wijn/spijscombinaties, en biochemische en organoleptische research plus wijn(proef)schrijven.
- Moderne architectuur (Jugendstil / Art Nouveau, Het Nieuwe Bouwen, Frank Lloyd Wright, Calatrava e.a.).

Kennis en Kunde

		Basis	Kundig, ervaren	Expert
Governance	Accountancy	•	•	
	Adviesdiensten	•	•	•
	Artificial Intelligence / Machine Learning	•	•	•
	Auditing	•	•	•
	Bedrijfseconomie	•	•	•
	Bedrijfskunde	•	•	
	Beleid schrijven	•	•	•
	Boekhouden	•	•	
	Business Impact Analysis	•	•	•
	COBIT®	•	•	
	COSO ERM	•	•	
	Cyber verzekeringen	•	•	•
	Data Governance	•		
	Eigenaarschap (Risk, Asset, Process, System ownership)	•	•	
	Enterprise Risk Management	•	•	•
	Information Management	•	•	•
	Internal Audit	•	•	•
	ISO 27001 – ISMS	•	•	•
	ISO 27014 – Governance of information security	•	•	
	IT Governance	•	•	•
	IT Management	•	•	•
	IT Strategy	•	•	•
	Privacy	•	•	•
	Rollen/verantwoordelijkheden beschrijven (RACI)	•	•	
	Strategie schrijven	•	•	•
Risk	Awareness (security en privacy)	•	•	•
	Business Continuity Management / DRP	•	•	•
	COBIT® for Risk	•	•	
	Human Risk Management	•	•	
	Information Risk Management	•	•	•
	ISF IRAM	•	•	
	ISO 22301 – Business Continuity Management	•	•	•
	ISO 27005 – Information Security Risk Management	•	•	•
	ISO 31000 – Risk Management	•	•	•
	NIST 800-30 Conducting Risk Assessments	•	•	
	NIST 800-39 Managing Information Security Risk	•	•	
	NIST CyberSecurity framework	•	•	•
	NIST Risk Management Framework	•		
	Operational Risk Management	•	•	•
	OT Security	•	•	
	Resilience	•	•	•
	Risk Analysis	•	•	•
	Risk Assessment / DPIA	•	•	•
	Risk Management	•	•	•
	Risk Quantification	•	•	•
	Third Party Risk Management	•	•	•

		Basis	Kundig, ervaren	Expert
Compliance	Algemene Verordening Gegevensbescherming (AVG)	•	•	
	Baseline Informatiebeveiliging Overheid (BIO)	•	•	
	CIS Controls V7.1, V8.0	•	•	•
	De Nederlandsche Bank (DNB) standaarden	•	•	
	Digital Operations Resilience Act (DORA)	•	•	•
	ECB-standaarden	•	•	
	EU AI Act	•	•	
	EU Cyber Resilience Act (Cbw)	•	•	•
	IEC 62443	•	•	•
	ISF controls	•	•	•
	ISO 27002 –Information Security Controls	•	•	•
	ISO 27701 – Privacy information management	•		
	NBA/LIO Volwassenheid / Toetsingskader V2.0, V3.0	•	•	•
	NEN 7510 / 7512 / 7513	•		
	Network and Information Security directive (NIS2)	•	•	•
	NIS2	•	•	•
	NIST 800-53 Security and Privacy Controls for	•	•	
	NIST Privacy Framework	•		
	Payment Card Industry Data Security Standard (PCI DSS)	•		
	SURF Toetsingskader	•	•	•