Resume

Ir.drs. Jurgen van der Vlugt CISA CRISC

Profile

I have been a consultant focused on advice and implementation of GRC frameworks and processes, increasing privacy and security awareness, quantifying operational risks and resilience to cyber threats. Before that, I worked as an independent professional or on short-term contracts in the risk and security domain, sometimes in team lead roles, via Xebia, Securesult, Marsh Risk Advisory, Secura, BDO Advisory, the International Criminal Court, at ministries and multinationals up to and including small SMEs.

I have also been an IT auditor and advisor on permanent contract at various organizations such as Noordbeek, Achmea, ABN AMRO Bank and KPMG. Initially as an IT auditor, but increasingly leaning towards not-just-ticking assessor/advisor on the breadth of IT management and control issues, latterly mainly involved in general ERM/ORM, BCM, privacy and (audit of) OT.
In the course of my career, I transitioned from auditing only, to portfolio management, team leadership and relationship management with clients and other stakeholders.

In addition, I have had my own wine import and trade for many years, with excise duty permit, stock administration, logistics matters, etc. – with attention and as an auditor, of course, by the book...

Knowledge and power

My professional heart lies in researching the applicability of everything that is New in our fields. Setting up strategy, tactics and operational implementation and, stern but friendly, assessing in the wider scope of that.

And actively contributing to the profession is (should be) a logical part of working life. I have contributed to the committees and working groups of NOREA, ISACA, ISSA, PvIB and PRMIA, I have taught and examined at colleges and universities, I have published regularly in national and international journals and conferences, and I hope to continue with that.
I was also a board member of the Netherlands-Canada Chamber of Commerce for many years, including for business /academic exchange in the IT/AI field and of course for the wine trade.

About the person

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

Contact

See:

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

What I'm looking for

Is a role in GRC advisory leading and managing assignments, with a sufficiently broad area of responsibility but still substantive involvement in content. With:

- Advising, deciding and managing improvements and innovation, from small to transformative, on (Enterprise / Operational / Information) risk management (beyond 3LoD, including quantitative and appreciative) – from business continuity to technology implementation and back;
- The same, on effective, business-driven implementation of and control over (the risks of) 'Artificial Intelligence' / Machine Learning and the business process re-engineering that comes along with that;
- Effective (balancing) communication styles, from Board-level discussions to operational level; relation-ship-oriented diplomacy to evidence-based rigour – whatever fits. That, in an open culture, not bureaucratic, not boring, no 'Dutch' bureaucracy;
- Not: more of the same, bureaucracy, pure-compliance auditing, writing procedures, ISAE3402, getting excited about IIA “quality assurance”. Doing that at most every now and then, but otherwise minimizing reporting-without-impact and ticking-boxes-for-the-sake-of-ticking is a pretty strict requirement;
- Keeping your eyes and ears open and working pre-sales with Sales is great, but I'm not a rain maker. I don’t do Sales nor billability targets period

Environment

- Working/writing/reporting in English: Preferred;
- Leading: Certainly. Although not from behind a large desk, but by demonstrating and working together;
- (Helping with) organizational development: Preferred;
- An international angle is a plus (regularly working in English and/or with international colleagues);
- Humour: Yes please.

Formalities

- Rate – quick transparency builds trust; ambiguity breaks it! – €8500 per month as a basis; of course you can make a switch even more pleasant. The 8% Holiday, 13th et al., and car (allowance) on top of that;
- Perm contract. One-year contract(s), I’m getting tired of them;
- With a preference for Randstad-Noord (North Holland, North-South Holland, Utrecht West side) as a location;
- If public transport or car travel time (at relevant hours) would be more than 75 minutes one-way, that would count as time at work;
- Traveling abroad for jobs: Yes, please! Provided 5% to a maximum of 15% of your working hours; Western Europe, North America, and some ME.

The above was promised at my current employer. But if a considerable number (sic) of points go the other way, with a weak customer acquisition skill and portfolio, then the above is no longer feasible. Without any prospect of improvement, because the strategy continues to go in a completely different direction, I am now drawing up some procedures and filling tools with yet another 'implementation' that a junior should also be able to do.

That is why I am looking for a good place in an internal position with sufficient trade challenges. With all my pent-up flexibility and energy: Who offers the right opportunity to use that in full positivity?

Work experience

Organization: **Maverisk Consultancy, IS Audit and Advisory services**
[January 2020 – via BDO Advisory Risk Services, Secura, Marsh, Securesult and Xebia]
Position: **Independent Professional, part-time (AP-registered) FG, Principal and Team Leader**
Period: **January 2012 –**

Leading and performing various audit and advisory assignments, including:

- Advising on the implementation of structural resolution of pentest results;
- Advising on and coordinating the implementation of new 'guardrails' controls for a VC/incubator company, introducing Policy-as-Code and Controls-as-Code;
- Designing compliance controls for new managed services.

- Hands-on making a small real estate investor DORA-compliant, from, let's say, a less advanced stage of management to now, in six months, suitable compliance with a sound ISMS and tooling;
- Supporting a Directorate-General of a Ministry with the formation of information management and security and privacy management of files containing extremely sensitive (and socially and politically very sensitive) data, including extensive formal (legal) considerations in this regard;
- Consultancy in various forms in higher education on information security, risk management and roadmaps for implementation of organizational improvements;

- Drafting, implementing and initially executing as CISO an ISMS in a fast-moving agile/DevOps scale-up organization (full stack security);
- A number of audit and advisory assignments on cybersecurity from an ISO 27001 perspective (including integration of NIST, BIO and NEN7510) in combination with IEC 62443 (including NIS/WBNI compliance), resulting in agile but organization-wide In Control status;
- A study of the organization and management of cybersecurity at a large construction company. The risk- prioritized advice ranged from management of organizational change capacity to details of internal vulnerability scans and the prioritization in follow-up;

- Setting up and helping to initiate an organization-wide information security strategy and associated policy for a large organization in the mechanical engineering industry, with a focus on IT supplier management;
- Supporting the implementation of maturity-enhancing measures under DNB regulation at one of the largest pension funds;
- Implementing and assessing control frameworks for GDPR compliance and BIA-driven GDPR implementations at a large healthcare institution and a medium-sized construction company;

- Setting up and initially implementing the CISO function at a network organization in the IT sector;
- Advisory services for a range of public organisations (national and local governments) on information security certification, privacy issues, integrating information and privacy secure behaviour into daily work, securing networks and IoT/Operational Technology infrastructures (up to PLC level); the emphasis was on translating GRC requirements into practical, feasible implementations throughout the organisations;
- Advising the ABN AMRO ISO department on the global information security risk-control framework (global guidelines, local implementations);

- Setting up and temporarily filling a CISO role at a smaller healthcare institution;
- Audit, review and advisory assignments on issues of operational and information risk management against various industry standards (incl. NIS/WBNI-comparable standards) at government institutions;
- At the International Criminal Court, act as Auditor Information Technology: managing the IT audit portfolio and relationship management (at all levels), conducting and leading statutory IT audits on IT, on the IT organization, on the information risk management strategy and implementation and on information security; acting as an independent advisor on security of communications infrastructures and technology innovations.

Organization: **Achmea/ Eureko Internal Audit**
Position: **Senior IT auditor**
Period: **January 2011 – December 2011**
Performing internal audits, including healthcare organisation issues; audit objects varied from IT processes to Information GRC processes but mainly related to assessment and advice on operational and information security risk management framework implementations within the Lines of Business and at Holding levels.

Organization: **Noordbeek Consultancy**
Position: **Senior Manager IT Audit/ Advisory services**
Period: **June 2006 – December 2010**
Leading and executing various implementation, audit and consultancy assignments in the areas of strategic IT management, information security and risk control, IT management frameworks, GRC implementations, and full-stack technical security for clients ranging from ministries (Defense and others) and multinationals, to smaller public and private (SME) organizations. Integrating ISO 27001 and IEC 62443 frameworks into integrated strategic and tactical In Control processes. A small selection of completed assignments:

- Leading and conducting an audit of, and urgently advising on, an organization-wide implementation of a management control framework for information management at a Defense organization;
- Leading and conducting (assurance/compliance-oriented) audits for a range of clients;

Organization: **ABN AMRO Bank, Group Security**
Function: **Group Information Security Coordinator**
Period: **October 2004 – May 2006**
Responsible for the global integration of physical and information system security including coordination of global policy development for this, and the development of anti-cybercrime strategies. Various (forensic) projects and implementations of highly confidential communication tools.

Organization: **ABN AMRO Bank, Group Audit Corporate Center**
Position: **Manager IS Audit**
Period: **May 2001 – September 2004**
Leading and performing various (global) audit and advisory roles, mostly related to information strategy, security and management frameworks for information and IT management, and GRC compliance. Advising in a broad relationship management role from SVP to Board level, on the integration of banking processes (at tactical and strategic levels), information and general risk management, audits on IT change processes and tactical / operational IT matters. A selection of assignments carried out:

- Leading and conducting an audit on a consolidated global HR system (for 180k FTE);
- Leading and conducting an audit on an Asset-Backed Securities system;
- Leading and conducting an audit of the consolidated financial reporting system.

Organization: **IQUIP (now Sogeti)**
Function: **Information Systems Auditor and Consultant**
Period: **April 2000 – May 2001**
Leading and executing various audit and advisory assignments in a broad IT field related to information security and the quality of IT management (control).

Organization: **KPMG EDP Auditors**
Position: **IT Audit Manager**
Period: **March 1995 – April 2000**
Leading and executing various audit and advisory assignments in a broad IT field, mostly related to technical information security. A selection of assignments performed:

- Development and roll-out of the Security and Audit of Windows NT line of business, same as the Y2k business;
- Performing information and IT security audits (in teams, sometimes solo) for several dozen customers;
- Conducting a global second opinion survey on Y2k projects for a well-known brewer.

Organization: **322 sqn RNLAF**
Position: **Lieutenant Intelligence/liaison officer**
Period: **1990-1991**
During military service, assigned to Leeuwarden Air Base as Ground Liaison Officer / Intell Officer at an F16 squadron from the Staff of the 1st Army Corps; duties included management of cryptographic materials and NATO strategy documents. NATO CTS Atomal clearance.

Trainings

Year	Course	Diploma
2019-2020	Journalistic Writing; University of Applied Sciences Utrecht	n/a
2002	Certified Information Systems Auditor (CISA); ISACA	•
2025	Champagne Connoisseur (level 2) also beta tester; Comité de Champagne	•
2023	Short course in Wine Writing; Wine Academy	•
2016	Bourgogne Terroir and Wine; Wine Institute	•
2014	Short MBO Basic Gastronomy; Wine Academy	•
2011	SDEN 2/3 (WSET3); Wine Institute	•

Languages

	Reading	Writing	Speaking
German	Advanced (Kant, Nietzsche, Heidegger, Schopenhauer, Canetti, Musil)	Reasonable	Good
English	Excellent (Hume, Joyce)	Excellent (business)	Excellent
French	Fair (wine authors)	Basic; fair with LLM usage	Fair (about wine)

Training courses

Year	Course	Trainer	Diploma
1995-1998	Postgraduate IT Auditing	Free University of Amsterdam	•
1992-1995	Engineer, Technical Computer Science	Delft University of Technology	Cum Laude [+]
1990-1991	Various Electronic Warfare courses	Ministry of Defense	n/a
1984-1990	Doctorate in Business Economics	Erasmus University Rotterdam	•

Side and volunteer activities

Organization	Rolls
NOREA	Member, Education Committee; previously lead writer of the Advisory Services Working Group, member and chair of the Education Committee, member of the Professional Technology Committee, the Revision of Professional Rules Committee and the Editorial Team
NEN	Former Member, Cybersecurity & Privacy Standards Committee
ISSA	Former Chairman and Secretary of the Dutch Chapter, Member of the Global Ethics Committee
PvIB	Former chairman of the iB Magazine article prize jury
ISACA NL	Former Board member
PRMIA	Formerly Subject Matter Expert
MSM Maastricht	Formerly Adjunct Professor of Executive MBA Program
Higher education	(Formerly) teaching at a majority of Dutch universities and colleges
The Hague University of Applied Sciences	Formerly External Commissioner for final exams
Miscellaneous	Conference, guest and roundtable presentations and chairing in the Netherlands and worldwide
Miscellaneous	Publish articles and posts about technical developments
Various Charities	Various support activities

Passion

I'm excited about:

- Our profession. I have been working with punch tape, teletype and 2's complement binary arithmetic since 1979, and over the years I have also dealt with organizational design issues, accountancy and audit, information security in all its facets, information risk governance and project risk management, and in recent years also operational and quantitative risk management. I like to publish about this, and I am very happy to be on stage for course, seminar, conference and lecture groups.
- Wine and gastronomy – with many years of its own wine import and trade (with excise permit, etc.), now mainly focused on wine/food combinations, and biochemical and organoleptic research plus wine (tasting) writing.
- Modern architecture (Jugendstil / Art Nouveau, New Building, Frank Lloyd Wright, Calatrava, etc.).

Knowledge and Skills

		Basic	Experienced	Expert
Governance	Accountancy	•	•	
	Advisory services	•	•	•
	Artificial Intelligence / Machine Learning	•	•	•
	Auditing	•	•	•
	Business Administration	•	•	•
	Business / Marketing	•	•	
	Business Impact Analysis	•	•	•
	COBIT®	•	•	
	COSO ERM	•	•	
	Cyber Insurance	•	•	•
	Data Governance	•		
	Enterprise Risk Management	•	•	•
	Information Management	•	•	•
	Internal Audit	•	•	•
	ISO 27001 – ISMS	•	•	•
	ISO 27014 – Governance of information security	•	•	
	IT Governance	•	•	•
	IT Management	•	•	•
	IT Strategy	•	•	•
	Ownership (Risk, Asset, Process, System ownership)	•	•	
	Privacy	•	•	•
	Defining roles/responsibilities (RACI)	•	•	
	Writing strategy and policies	•	•	•
Risk	Awareness (security and 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	•	•	•

		Basic	Experienced	Expert
Compliance	EU AI Act	•	•	
	EU Cyber Resilience Act	•	•	•
	General Data Protection Regulation (GDPR)	•	•	
	Baseline Information Security Government (BIO)	•	•	
	CIS Controls V7.1, V8.0	•	•	•
	The Dutch Central Bank (DNB) standards	•	•	
	Digital Operations Resilience Act (DORA)	•	•	•
	ECB-standaarden	•	•	
	IEC 62443	•	•	•
	ISF controls	•	•	•
	ISO 27002 –Information Security Controls	•	•	•
	ISO 27701 – Privacy information management	•		
	NBA/LIO Maturity / Audit framework 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	•		
	SURF Audit framework	•	•	•