Henk Jan Jansen

CIPM, CISSP, ITILv4, SFPC, CISM, CSAM, IPMA-A Digital Transformation & Cybersecurity

Introduction

A highly experienced and results-oriented program management professional with 30 years of extensive experience in successfully leading and delivering complex, large-scale programs. Expertise includes program management, SAP implementations, Identity and Access Management (IAM) and Cyber Security, complemented by a strong foundation in Law & Regulation, Compliance and Digital Transformation Strategies.

Possesses in-depth knowledge of IT operations security frameworks, compliance mandates, and regulations, with a comprehensive understanding of both national and international legal landscapes. Adept at navigating the intricacies of security, compliance, and regulatory requirements to ensure the success of the program and mitigate potential risks.

INTERPERSONAL SKILLS

- Fast and efficient learner.
- Good team leader and team player.
- Proficient in 3 languages: English, German and Dutch.
- Result-oriented.
- A punctual worker.
- Reliable and responsible with all tasks

Security Tech Enthusiast | Bridging the Gap Between Ideas, Execution & Innovating for a Better Tomorrow

Summary

Hello, I'm Henk Jan,
Strategic IT and cybersecurity professional with 30+ years of global experience guiding national and international organizations in developing and implementing robust security strategies. Expertise in risk management, compliance (DORA, NIS2, ISO 2700x) and incident response. Proven ability to align security initiatives with business objectives and drive significant improvements in security posture. CIPM, CISSP, ITILv4, SFPC, CISM, CSAM, IPMA-A.

A seasoned hands-on and hands-on ICT and cybersecurity professional with over 30 years of experience designing frameworks, implementing risk and vulnerability assessments, and leading initiatives to secure digital assets. Performing Treat and Risk Assessment. Recognized for leading complex IT and cybersecurity projects, managing cross-functional teams, and providing leadership at the executive level. Knowledge of laws and regulations, government frameworks and policies on privacy, and information security (such as VIR, BIO and GDPR). Proficient in aligning organizational goals with advanced security frameworks and regulatory standards, including ISO2700x/3000x, DORA, and NIS2.

Education

1981-1986 Bachelor of Business Information Science,
University of Twente, The Netherlands
1981-1987 Doctor of Science (D.Sc.)
University of Twente, The Netherlands

Languages

- English - Expert
- German - Expert
- Dutch – Main language
- Tagalog - Intermediate
- French - Intermediate

Security Tech Enthusiast | Bridging the Gap Between Ideas, Execution & Innovating for a Better Tomorrow

Key competences

- DPO Data Protection Officer
- CISO Head of Information Security
- Director of Information Security
- SOC Security Center
- User awareness, security awareness and training
- Different components such as Phishing
- Security awareness campaigns
- IAM by Privilege Access Management
- Security of deliverables, milestones, and schedule
- Security Analyst/Security Engineer
- Security architect
- Computer Security Incident Responder
- Vulnerability management
- Security Architecture
- Security process monitoring
- Infrastructure security
- Security of the Cloud
- IAM/PAM/CIAM
- Application security
- Endpoint security
- Incident response
- Email Security
- Threat intelligence
- Threat modeling
- Security by Design
- DLP Data Loss Prevention
- Vulnerability assessment
- Disaster Recovery (DR)

Laws & Regulations, Compliance:

- DORA
- ISO 2700x series
- BIO
- SOX
- AVG
- Operational Resilience Regulations
- DNB Good Practical
- EBA Guidelines
- NEN + NEN-EN
- PRA, ESMA Regulation
- NIS2

Work experience

Kadaster
Senior Business Architect
Apeldoorn January – May 2026.
Description of the assignment:
Business Architect CIAM (Services & Processes)

- Drafting and updating the CIAM solution architecture for service provision and
- business processes, with specific attention to the relationship with API management;
- Establishing and updating the CIAM domain architecture
- The recording and maintenance of architectural models in the agreed
- Architecture repository
- Identifying and weighing relevant dependencies and interests within the CIAM
- Domain
- Providing improvement recommendations for processes and architecture
- Advising project managers on phasing, prioritization and planning from the perspective of
- architectural perspective.

Business Architect CIAM (Applications & Technology)
CIAM solution architecture for applications and technology, with a particular focus on custom UI development based on APIs;

- Developing the CIAM design in consultation with the selected CIAM
- Supervising the implementation by means of architectural advice, appropriate within
- Applying and substantiating modern CIAM concepts and patterns such as FIDO,

- passwordless authentication, verified credentials, PBAC/ReBAC en ID-wallets;
- Recording architecture products in the architecture repository;
- Proposing improvement proposals and advising on phasing and prioritization.
- A demonstrably architecturally realized CIAM implementation within the
- An updated architecture repository with solution and domain architecture;
- Documented solution architecture and CIAM designs.

Ministry of Infrastructure and Water · Freelance (Part-time)
Interim DPO
Den Hague, South Holland, Netherlands· Feb 2025 – Present
Description of the assignment:
▪ Responsible for the provision of information and independently advises on the structure of all Ministeries based on UAVG, AVG, WPG.

Brand New Day · Freelance (Part-time)
Interim Information Security Officer
Amsterdam, North Holland, Netherlands· Mar 2024 – Nov 2024

Primarily:
Led a comprehensive self-assessment and gap analysis against EBA guidelines and DORA, identifying 46% of critical security gaps in existing policies and procedures. Developed a detailed roadmap for recovery to achieve full compliance, prioritizing critical areas such as EBA and DORA regulations.
Secondary:
- Conducted comprehensive gap analysis against EBA guidelines and DORA, identifying 85% of critical security gaps in existing policies and procedures.
- Developed a detailed roadmap for remediation, prioritizing critical areas such as data protection and incident response, achieving 95% compliance within 6 months.
- Implementation of phishing awareness training, which has reduced successful phishing attempts by 70% across the organization.

Key Components:
- Configuration Management
- DORA, EBA, DNB, PRA, ESMA regulation and Operational Resilience regulatory
- IT Asset Management
- IT Service Delivery
- Change Management
- Quality Assurance
- Risk Management / Security and Compliance
- Incident Management
- Entra ID (Intune) and Microsoft Security tools

Municipality of Amsterdam · Partime
Interim Architect/DPO Cloud solution
Amsterdam, Netherlands Jan 2023 - Mar 2024
Implementation is technical as well as functional Technical design made for an IV organization.
Description of the assignment:
▪ Responsible for the provision of information and independently advises on the structure of the IV management organization
▪ Develops a multi-year innovation agenda and brings the organization to the IV organization of the future.
DPO role:
1. Led digital transformation initiatives, resulting in a 30% improvement in operational efficiency and a 25% reduction in IT-related costs.

2. Implemented a comprehensive suite of security technologies, including SIEM and UEBA, preventing 99.9% of potential data breaches.
3. Developed and enforced GDPR-compliant data protection.

Regional Education center · Part-time
Interim Chief Information Security Officer
Utrecht, Netherlands Sep 2023 – February 2024
Implementation is technical and functional
Task:

- Developed and implemented a 3-year plan for improving security maturity, in accordance with the NIST Cybersecurity Framework, resulting in a documented 55% improvement in the organization's security posture within 6 months.
- Implemented IAM/PAM solution, reducing unauthorized access attempts by 85% and reducing user provisioning time by 60%.
- Design and execution of a Crisis Management (BCM) plan, reducing incident response time by 50% during simulated breach scenarios.
- NIST Cybersecurity Framework and ISO 27001 Standards

OCBC bank & BDO bank Singapore/Philippines
Project manager/Architect IAM solution
IAM / PAM - Zero trust environment
Philippines Jun 2023 – Oct 2023
Implementation is technical and functional

- Spearheaded the implementation of NetIQ Identity Manager, establishing a zero-trust environment for 50,000+ users across multiple countries, reducing unauthorized access attempts by 92%.
- Alignment of operational technology (OT) cybersecurity with ISO 27001 and IEC62443 standards, achieving 100% compliance within 4 months.
- Optimized processes for managing the identity lifecycle, reducing provisioning time by 75% and deprovisioning time by 60%.

Municipality of The Hague
Project manager/Architect IAM solution
Nov 2022 - Aug 2023
The Hague, South Holland, Netherlands · Hybrid
Implementation is technical and functional

- This included a complete overhaul of the existing identity infrastructure to improve security, efficiency, and compliance.
- This ensured that sensitive data was protected and that employees had the right levels of access based on their role. This implementation resulted in a 30% reduction in the number of attempts at unauthorized access to systems.
- This agenda included initiatives in the areas of cloud computing, cybersecurity, data analytics, and citizen engagement. The agenda has been approved by the CIO and is expected to lead to a 30% increase in citizen satisfaction with online services over the next three years.
- This included implementing Multi-Factor Authentication (MFA), 2FA, Single Sign-On (SSO), and role-based access control (RBAC) policies. This resulted in a 50% reduction in the risk of data breaches and ensured compliance with relevant regulations.
- This included recommendations on cybersecurity best practices, data management policies, and IT risk management.
- This resulted in 99.9% uptime for critical IAM services.
- This framework covered key areas such as information security, data architecture, and privacy.

Interim CIO/DPO February 20 21-October 2023

Federal Government (EU) Brussels Belgium

- Led digital transformation initiatives, resulting in a 30% improvement in operational efficiency and a 25% reduction in IT-related costs.
- Implemented a comprehensive suite of security technologies, including SIEM and UEBA, preventing 99.9% of potential data breaches.
- Developed and enforced GDPR-compliant data protection policies, achieving 100% compliance and avoiding potential fines of up to €20 million.

Interim Architect Cloud solution
Municipality of Amersfoort · Freelance January 2022 - March 2023
North Holland, Netherlands
Implementation is technical and functional
Technical design made for an IV organization
Description of the assignment:

- Responsible for the provision of information and independently advises on the design of the IV management organization and implementation of NIS-2.
- Have developed a multi-year innovation agenda and bring the organization to the IV organization of the future
- Responsible for the strategy in the field of information provision (including information security, architecture and privacy)
- Advising on the optimal safeguarding and organisation of the tasks and responsibilities of the CIO in the organisation.
- Drafting the I-vision, framework, strategic responsibility for information provision, design IV organization and the overarching architecture.
- Quality assurance
- The design is based on the BISL framework.

Energie Data Services Nederland (EDSN) B.V. Freelance

Security Program Manager March 2022 – October 2022
Amersfoort, The Netherlands
Implementation is technical and functional

- Here, I led the security program that improved EDSN's security posture, resulting in a 65% reduction in identified vulnerabilities within 6 months.
- Upgraded to ISO 27001:2022, improving IAM/PAM workflows and ensuring GDPR and NIST 800-53 compliance, improving overall security audit scores by 50%.
- Implemented security awareness training program, which increased employee security competency scores by 55% and reduced security incidents by 70%.

The points that had all the attention was:

- Upgrade IEC ISO 27001 2022
- Upgrade policy
- Procedures for upgrades
- 24/7 Monitoring of the entire infrastructure onside and in the Cloud
- Upgrade IAM/PAM workflows, processes, and protocols.
- IAM/PAM (OKTA & NetIQ)
- Quality assurance
- VGA, NIST 2 Privacy and Security Compliance
- Expansion of Crisis Management (BCM)
- CIS-Hardening Framework
- Level 1 profile "benchmark"
- Level 2 profile "defense in depth"

Leaseplan, CarNext

Senior manager/Architect OKTA SME Aug 2021 – March 2022
Amsterdam, North Holland, Netherlands
Implementation is technical and functional

I was able to carry out the separation from LeasePlan to CarNext. I split off the IT infrastructure from LeasePlan, so that there would be a completely new IT environment. I also took care of the migration of AD connected applications, all third parties and all user data to the new CarNext IT environment. Below is the next step on the sidelines of CarNext.

Tasks:

- Design and implementation Okta (Workforce Identity and Access Management/ Consumer Identity and Access Management) SSO/MFA/WMA/2FA. Lifecycle management and patch management.
- Setting up a foundation for Identity and Access Management within CarNext. Implementation of crisis management (BCM). At that time, the company was in the middle of an IT carve out and there was still a lot of legacy to be cleaned up before the foundation could be laid.

⇒ My 2nd role within CarNext was Manager Cyber Security to build a new ICT/Cyber security team.
I am responsible for the strategic and operational leadership of CarNext's Security & Compliance department, which includes both compliance and security engineering capabilities. Responsibilities include: threat and risk management, vulnerability management, security engineering, application and cloud security, access management, endpoint security, the information security management system, compliance with security and privacy regulations, standards and best practices such as ISO27001, NEN7510, NIS2, DORA, HIPAA and SOC 2.

Me and my team help our business grow by complying with norms and standards in new regions such as the UK and the US and in new sectors. We also enable growth by ensuring the security of CarNext secure e-mail products. I also enjoy public speaking at conferences, webinars, or podcasts.

As CISO, I am also part of the management team of CarNext and I am responsible for strategic and operational leadership. In addition to my responsibilities for security and compliance, I take care of the OKR (Objective & Key Results) setting and management and I play an active role in further structuring the MT meetings.

- Quality assurance
- Implementation of security technologies, such as network equipment, firewall, Active Directory, IAM, PAM, SIEM, UEBA, AV, IDS/IPS, Saas, Iaas, Paas, BIO, ISFM, SAML, OIDC, user environment management, implementation of crisis management, including desktop/laptops, profile management, access control, and MDM solutions.

- **Program Manager RP International for DarkMatter LLC** Feb 2019 to Mar 2021
  - Program Manager Cyber range Expo2020
  - Department of Economic Development (Chamber of Commerce)
  - Emirates Nuclear Power Corporation
  - Cyber Security Range Manager, Cyber Academy (hybrid)
  - Training RFID (Digital Forensics and Incident Response Distribution)
  - Min. of Foreign Affairs Headquarters, Abu Dhabi
  - Min. of Finance, Abu Dhabi
  - Ministry of Economic Development, Abu Dhabi
  - Emirates Nuclear Corporation
  - Ayjal Education Management UAE

- Training RFID (Digital Forensics and Incident Response Distribution)
- ADNOC Digital Transformation – AI – ML – RPA
- Cyber Education DarkMatter - DigitalE1 UAE
- Program Manager Cyber Range, Security Awareness training
- Bootcamp related to IT/Cyber Security Awareness

Technical Program Manager Gfi Informatique, Dubai, UAE Jan 2018 - Feb 2019
Managing Program Manager Camelot ITLab, Mannheim Germany Feb 2018 - Oct 2018
Project Director Comyerse Inc. Boston / London / Dubai Sep 2016 - Oct 2018
IT Program Manager BNP Paribas, Nuremberg Area, Germany Aug 2017 - Jul 2018
Security Consultant Passport Business Engineering BV, The Netherlands May 2018 - Aug 2018
IT Program Manager ITERGO, Düsseldorf Germany Jun 2017 - Sep 2017
Global Chief Information Officer IMI Precision Engineering Birmingham, UK Jun 2016 - se 2018
Principal Product Delivery Manager Vodafone GmbH, Germany July 2015 - June 2017

Key competences

- **Cybersecurity Architecture & Implementation**

1. Expert in developing and implementing comprehensive cybersecurity strategies aligned with the organization's goals and regulatory requirements (ISO 2700x, BIO(2), NIST, DORA, NIS2). Skilled in designing and implementing robust security architectures that incorporate security by design principles, zero-trust models, and defense-in-depth strategies. Adept at conducting thorough risk assessments, threat modeling, and vulnerability assessments to identify and mitigate potential security weaknesses. Experience establishing and managing Security Operations Centers (SOCs) for proactive threat detection and incident response. Designing a cloud-native security architecture for a financial institution migrating to AWS, implementing a zero-trust network segmentation strategy for a factory, and developing a comprehensive incident response plan for a government agency.

- **IAM/PAM Solutions**

1. Extensive experience in the design, implementation, and management of IAM/PAM solutions to control access to sensitive data and systems, prevent unauthorized access, and enforce the principles of least privilege. Expertise includes directory services (Active Directory, Azure AD), authentication protocols (SAML, OAuth, OpenID Connect), multi-factor authentication (MFA), single sign-on (SSO), and identity management. Proven ability to integrate IAM/PAM solutions with various applications and platforms, including cloud environments (Azure, AWS, GCP), on-premise systems, and SaaS applications (Salesforce, Office 365). Hands-on experience with leading IAM/PAM tools such as OKTA, NetIQ, CyberArk, and Zero Trust. Deploy OKTA for a global enterprise with 50,000+ users, deploy CyberArk to secure privileged access to critical infrastructure systems, and develop an automated identity lifecycle management process using NetIQ.

- **Cloud Security**
  - Proficient in securing cloud environments (AWS, Azure, GCP) using native cloud security services and third-party security tools. Expertise includes cloud security architecture, cloud identity and access management, cloud data security, cloud network security, and cloud application security. Knowledge of cloud security best practices and compliance standards (e.g., CIS benchmarks, SOC 2, ISO 27017). Experience implementing cloud security solutions such as cloud workload protection platforms (CWPPs), cloud security posture management (CSPM) tools, and cloud access security brokers (CASBs). Designing and implementing a secure cloud infrastructure for a healthcare provider migrating to Azure, implementing a cloud security monitoring solution using AWS CloudWatch and CloudTrail, and conducting a security assessment of a cloud application using OWASP guidance.

- **Incident response & Threat Intelligence**
  - Experience developing and executing incident response plans to effectively detect, contain, eradicate, and recover from cybersecurity incidents. Skilled in conducting incident investigations, conducting forensic analysis, and identifying root causes. Knowledge of resources, techniques, and tools for identifying and mitigating emerging threats. Experience working with law enforcement and other stakeholders during incident response. Leading the incident response to a major data breach at a financial institution, developing a threat intelligence program for a government agency, and conducting a tabletop exercise to test an incident response plan.

- **Compliance & Governance**
  - In-depth knowledge of regulatory frameworks and security standards, including DORA (Digital Operational Resilience Act), ISO 2700x series, BIO (Dutch Baseline Information Security), SOX (Sarbanes-Oxley Act), GDPR (Dutch implementation of GDPR), NIS2 directive, DNB Good Practice, EBA guidelines, NEN + NEN-EN standards, PRA, ESMA regulations, SWIFT CSCF and

NIST frameworks. Ability to translate regulatory requirements into actionable security policies and procedures.

- **Infrastructure & Network Security**
  - Extensive knowledge of network security principles and technologies, including firewalls, intrusion detection and prevention systems (IDS/IPS), virtual private networks (VPNs), and network segmentation. Skilled in designing and implementing secure network architectures that protect against unauthorized access, data breaches, and denial-of-service attacks. Experience configuring and managing network security devices from leading vendors such as Cisco, Palo Alto Networks, and Fortinet. Designing and implementing a secure network architecture for a multi-site distributed enterprise, configuring a firewall to block malicious traffic based on threat intelligence feeds, and conducting a penetration test to identify network vulnerabilities.
- **Incident response & Forensics**
  - Incident response planning, incident detection and analysis, malware analysis, digital forensics, threat hunting, security incident management, and data breach response.
- **Application Security**
  - Secure SDLC (software development lifecycle), application security testing (SAST, DAST), web application firewalls (WAF), API security, mobile application security, and secure encryption practices.
- **Other Technical Skills**
  - SAP Security, BiSL Framework, Quality Assurance, machine learning (ML), artificial intelligence (AI), Robotic Process Automation (RPA), knowledge of operating systems (Windows, Linux), scripting languages (Python, PowerShell).

Cyber Security certifications

Cybersecurity Certifications

- Certified Information Security Manager (CISM)
- Certified Information Privacy Manager (CIPM)
- Information Security Foundation, (based on ISO/IEC 27002)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Systems Security Professional (CISSP) (ISC2, SA)
- EU General Data Protection Regulation Practioner (GDPR-P)
- CyberArk Defender
- CyberArk Sentry
- CyberArk Guardian
- IP3Security Design and Implementation, Strategy to reality Security Design Specialist
- Cisco Managing Network Security, Cisco Managing Support CCEA + CCNA
- NetIQ Identity Manager 4.0.2
- CA Identity Manager
- CA Governance Less
- CA Governance
- EC-Council Certified Security Analyst
- OKTA
  - OCP Okta Certified Professional
  - OCA Okta Certified Administrator
  - OCC Okta Certified Consultant
- SABSA = Sherwood Applied Business Security Architecture
  - F1 & F2 SABSA Foundation Modules
  - A1 – Advanced SABSA Risk, Assurance & Governance
  - A2 – Advanced SABSA Architecture Program Management
  - A3 – Advanced SABSA Architecture Design
  - A4 – Advanced SABSA Incident, Monitoring & Investigations Architecture
  - A5 – Advanced SABSA Business Continuity and Crisis Management

Security Tech Enthusiast | Bridging the Gap Between Ideas, Execution & Innovating for a Better Tomorrow

Professional certifications

- Certified Chief Information Security Officer (CCISO)
- Organizational Development Manager (SHRM)
- ArchiMate® 3.1 Training Course: Combined Level 1 and Level 2
- Certified Master Data Management (MDM -CMA)
- PRINCE2 @ Agile AXELOS Global Best Practice
- Lean Six Sigma Black Belt
- IT Infrastructure Library ITIL (v4)
- Togaf Enterprise Architect
- ArchiMate® 3 Foundation & Practitioner Enterprise Architecture
- ArchiMate® 3.1 Training Course: Combined Level 1 & Level 2
- Certified IT Asset Manager (CITAM)
- Certified Associates Asset Management (SAAM)
- Certified Senior Practitioner Asset Management (CSAM)
- IPMA-level A Program Director
- IPMA-level B, C, D (ICT- Project Management)
- Prince2 PM, Foundation, Practitioner, Essentials & Problem Management
- Certified IT Asset Manager (CITAM)
- Certified Senior Practitioner Asset Management (CSAM)
- Cisco Certified Design Associate (CCDA)
- Certified ISO 27001 Lead Auditor (PECB), Lead Implementer (PECB)
- Project Management Institute (PMI) Professional Certification (PMP)
- Scrum Foundation Professional Certificate