James Gerrior

Information Security & AI Governance Leader

Email: james@jamesgrc.com

LinkedIn: James Gerrior | Website: jamesgrc.com | GitHub: github.com/jamesgrcghub

PROFESSIONAL PROFILE

Information Security and AI Governance Leader with 11 years leading enterprise ISMS programs, and 3 years building and directing corporate AI Management Systems (AIMS) in an AI company.

Experienced CISO-level leader with a record of translating complex requirements — ISO 27001, ISO 42001, EU GDPR, EU NIS 2 Directive, EU AI Act, NIST AI RMF — into fully customized and measurable programs. I have designed and managed security and governance programs in North America, EU, East Africa, and Asia for multinational organizations, transforming management systems into KPI-driven models with current posture measurements and maturity forecasting.

Open to Information Security and AI Governance leadership roles.

CORE COMPETENCIES

Governance: Information Security Management Systems (ISMS) | AI Governance / AI Management Systems (AIMS) | GRC Strategy & Leadership | Enterprise Risk Management | Compliance Program Management | Board & Executive Reporting

Risk & Privacy: Data Privacy & EU GDPR Compliance | AI Ethics & Responsible AI | Third-Party Risk Management

Operations: Incident Management | Security Awareness Programs | Agentic AI Implementation | Threat & Vulnerability Management

International Program Leadership: North America | EU | East Africa | Asia

DOMAIN EXPERTISE

Information Security: ISO 27001 | NIST Cybersecurity Framework (CSF) | EU NIS 2 Directive | TISAX | OWASP Projects and Top 10s | OWASP AI Exchange

AI Governance: ISO 42001 | NIST AI RMF | EU AI Act | OECD AI Principles

Risk & Compliance: ISO 31000 | ISO 9001 | ISO 22301 | EU GDPR

Emerging & Specialized: Agentic AI Governance & Security | Non-Human Identity (NHI) | Post-Quantum Cryptography (PQC) | AI Trust, Risk, and Security Management (AI TRiSM) | Continuous Threat Exposure Management (CTEM)

PUBLIC WORK

Live Demo Governance Dashboards: Controls, KPI scoring, trends, forecasting, compliance tracking, and management system data analysis – using synthetic data

- Interactive ISMS Dashboard: jamesgrc.com/isms
- Interactive AIMS Dashboard: jamesgrc.com/aims

ISMS & AIMS Control Libraries: Customized, multi-framework-mapped control libraries as used in the above Dashboards — versioned and open on GitHub — github.com/jamesgrcghub

EMPLOYMENT HISTORY

Director of Information Security & GRC — Sama *March 2023 — Present*

- Designed, implemented, and managed a customized Information Security Management System built upon ISO 27001, NIST CSF, OWASP materials, TISAX, EU NIS 2 Directive, and client requirements
- Matured company security posture using a method of customized quarterly KPI measurements across all ISMS controls and domains
- Served as Chairperson of the Security Council – conducting monthly Exec Team meetings, and providing quarterly Board reports
- Designed and implemented a customized AI Governance Framework built upon ISO 42001, NIST AI RMF, EU AI Act, and OECD AI Principles
- Served as Chairperson of the AI Governance Council and led ISO 42001 certification preparation process – conducted monthly AI Governance Council meetings focused on maturing AI Governance posture
- Designed, implemented, and managed a customized Enterprise Risk Management Framework built upon ISO 31000, ISO 9001, and applicable legal and regulatory requirements
- Directed Global GRC team; matured enterprise risk management and compliance practices across all regional operations
- Implemented agentic AI tools for enterprise Information Security and GRC task automation, content creation, and data analysis using Anthropic models

Information Security Director — One Acre Fund *December 2016 — March 2023*

- Designed, implemented, and managed the first enterprise ISMS covering operations across 10+ countries
- Designed Technical Governance and Data Governance Frameworks, establishing foundational policies, standards, and controls
- Founded and led the internal Risk Advisory Group, aligning enterprise risk management practices across all business units
- Designed Risk Management Assessment processes for projects and assets, establishing a repeatable and auditable risk evaluation methodology
- Implemented Vulnerability Management and Incident Response programs

IT Operations Director — One Acre Fund *December 2014 — December 2016*

- Created the first company IT Operations strategy spanning 10 countries, 7,000+ staff, and 800,000 farmers
- Designed the company's initial Information Security strategy in 2015, establishing governance structure and baseline controls
- Managed departmental KPIs and OKRs, driving structured maturity reporting to executive leadership

Technical Director — NetIQ – Novell Africa *December 2012 — November 2013*

- Coordinated SIEM, IDM/IAM, and BCP/DR proof-of-concept engagements for prospective clients in financial and government sectors across East Africa

---

CERTIFICATIONS

ISACA CISM — Certified Information Security Manager

IAPP AIGP — AI Governance Professional (Expected Q3 2026)