AKILO A.

AI Governance and Technology Risk Leader | Information Security

Toronto, ON | akilo.a.ak@gmail.com | +1 (226) 386-1527 | linkedin.com/in/akilo | github.com/akiloakolu

PROFESSIONAL SUMMARY

Information Security and Technology Risk professional with 12+ years of progressive experience protecting regulated environments in financial services and healthcare. Proven track record executing enterprise GRC programs, supporting FCA and PHIPA regulatory engagements, and advising senior stakeholders on risk strategy. Hands-on specialist in AI governance with experience implementing and operationalizing governance frameworks, assessing generative AI and LLM risks, and aligning programs to the EU AI Act and NIST AI Risk Management Framework. Familiar with OSFI B-13 technology and cyber risk guidance, applying AI governance discipline built in regulated healthcare to the demands of regulated financial services. Skilled at maturing compliance functions, reducing residual risk exposure, and driving cross-functional security initiatives.

CORE COMPETENCIES

Information Security Management | Technology Risk and GRC | AI Governance and Ethics | Regulatory Compliance

OSFI B-13 | PIPEDA | PHIPA | PCI DSS | SOC 2 | ISO 27001 and 27002 | NIST CSF | COBIT 5

EU AI Act | NIST AI RMF | Generative AI Governance | LLM Risk Assessment | AI System Inventory | Responsible AI Frameworks

Cloud Security: Azure and AWS | Zero Trust Architecture | SIEM | EDR | IAM | PAM | Threat Modeling

Third-Party Risk Management | Enterprise Risk Assessment | BCP and DR | Incident Response | Board Reporting

AI AND EMERGING TECHNOLOGY SPECIALTIES

- Designed AI governance frameworks aligned to the NIST AI RMF and EU AI Act high-risk system requirements, producing an AI risk register covering 10 AI systems and vendors in a regulated environment
- Assessed generative AI and LLM security risks including prompt injection, training data poisoning, model hallucination, and AI supply chain exposure, and developed enterprise mitigation control libraries
- Built an AI System Risk Inventory and Compliance Gap Analyzer using React, FastAPI, Python, and the Anthropic Claude API as a practical AI governance portfolio tool
- Proficient with Anthropic Claude API, OpenAI API, Microsoft Azure AI Services, and Amazon Bedrock within secure deployment and data residency frameworks
- Authored internal AI governance policies covering bias auditing, explainability standards, model documentation, and human-in-the-loop control requirements

PROFESSIONAL EXPERIENCE

Technology Risk and AI Governance Manager | Integrated Occupational Health Service *Dec 2023 – Present*

London, UK / Canada | Remote | Healthcare

- Implemented and operationalized AI governance framework aligned to NIST AI RMF, achieving zero findings in 2023 regulatory review.
- Delivered quarterly stakeholder risk reporting to VP/CRO across 3 business lines, securing $250K SIEM budget approval.
- Extended AI governance standards to 10 AI systems and vendors, tiering risk ahead of EU AI Act enforcement.

Information Security Manager | Integrated Occupational Health Services *Apr 2021 – Dec 2023*

London, UK | Hybrid | Healthcare

- Led six-person cross-functional security team covering application security, third-party risk, vulnerability management, and incident response.
- Implemented cloud security controls for Azure migration covering 80% of workloads, maintaining PCI DSS Level 1 and ISO 27001.
- Cut critical and high vulnerability backlog 55% in 10 months via risk-prioritized sprints and SLA accountability.
- Built third-party risk program tiering 120+ vendors across 3 business lines by data sensitivity and PHIPA exposure.

Information Security Specialist | Access Bank UK Limited *Oct 2015 – Jan 2021*

London, UK | On-site | Financial Services

- Built SOC on Microsoft Sentinel SIEM, cutting detection time from 14 days to 72 hours banking-wide.
- Ran phishing simulation program, cutting employee click rates 65% over 18 months across high-risk roles.

- Led network segmentation initiative, remediating 200+ legacy devices to cut lateral movement risk in trading operations.

Technology Risk Analyst | Access Bank *Feb 2013 – Sep 2015*
Abuja, Nigeria | On-site | Financial Services

- Led CyberArk PAM deployment, onboarding 600+ accounts and cutting shared admin credentials 80% across core banking.
- Maintained 400+ control library mapped to COBIT 5 and NIST CSF, standardizing risk classification banking-wide.
- Led OWASP Top 10 reviews and threat modeling across 20+ applications annually, prioritizing remediation.

IT Risk and Access Analyst | Diamond Bank Plc *May 2011 – Jan 2013*
Abuja, Nigeria | On-site | Financial Services

- Reviewed access across 5,000+ systems and users, remediating excessive access to enforce least-privilege.
- Closed 700+ orphaned accounts through access provisioning and de-provisioning, cutting unauthorized access risk.
- Secured core network infrastructure, routers, switches, firewalls, VPNs, supporting 1,500+ sites and users.

EDUCATION

Post Graduate Diploma, Network Security and Architecture | Fanshawe College | 2025
Post Graduate Diploma, Information Security Management | Fanshawe College | 2024
Bachelor of Science, Computer Science | University of Benin | 2010

CERTIFICATIONS

CISSP (In view)
AIGP (In view)
CISM Certified Information Security Manager | ISACA
CRISC Certified in Risk and Information Systems Control | ISACA
CySA+ Cybersecurity Analyst | CompTIA

KEY ACHIEVEMENTS

- Reduced enterprise critical vulnerability exposure by 55% within 10 months at a Tier 1 financial institution
- Supported ISO 27001 certification for a multi-site health system, delivered on schedule and under budget
- Secured budget approval for a $250K SIEM upgrade through quarterly risk reporting to VP and CRO leadership
- Achieved a 65% reduction in employee phishing click rate over 18 months through a targeted security awareness program

PROFESSIONAL AFFILIATIONS

ISACA Toronto Chapter | ISC2 Canada | IAPP | Obsidi Network Member Advisory Group | Cloud Security Alliance