BOLA MABAWONKU

Senior GRC Manager | Cloud Security Architect

CISM · CRISC · CISSP · CCSP

Edmonton, AB, Canada · bmabawonku@bolamabawonku.com · linkedin.com/in/bolarinwa-mabawonku · bolamabawonku.com · github.com/Bolamabx

PROFESSIONAL SUMMARY

Senior cybersecurity professional with over five years of experience designing and delivering governance, risk, and compliance frameworks and cloud security programs across financial services, healthcare, and technology sectors. Demonstrated track record of building enterprise security programs from the ground up, achieving regulatory compliance, and delivering measurable risk reduction. Combines board-level communication and regulatory engagement experience with hands-on technical delivery across AWS, Azure, and GCP, including emerging AI governance frameworks for managed service environments. Holds four active certifications, CISM, CRISC, CISSP, and CCSP, reflecting depth across both the governance and technical dimensions of cybersecurity. Career spans Nigeria and Canada with cross-regulatory experience across FFIEC, OCC, HIPAA, CBN, NDPA, ISO 27001, NIST CSF 2.0, NIST AI RMF, and SOC 2 frameworks.

CORE COMPETENCIES

- Cybersecurity strategy & program development
- Regulatory engagement: OCC, FFIEC, CBN, NDPA
- Third-party & vendor risk management (TPRM)
- Incident response planning & tabletop exercises
- SIEM detection engineering: Sentinel, KQL
- SOAR automation & cloud IR playbook development
- AI risk governance: NIST AI RMF, EU AI Act
- Enterprise risk management & risk registers
- Board & executive cybersecurity reporting
- Compliance automation: SOC 2, ISO 27001
- Cloud security posture management (CSPM)
- Policy-as-code & infrastructure-as-code security
- Multi-cloud security: AWS, Azure, GCP
- Information security policy framework authoring
- Vulnerability management program governance
- Security awareness & human risk management
- IAM governance & least-privilege architecture
- MITRE ATT&CK for Cloud mapping & detection
- NIST CSF 2.0 implementation & assessment

TECHNICAL SKILLS & TOOLS

Cloud Platforms	AWS (IAM, Config, GuardDuty, CloudTrail, Security Hub, Lambda, Organizations, SCPs) · Azure (Defender for Cloud, AD, Monitor, Policy, Sentinel) · GCP (Security Command Center)
Security Tools	Prisma Cloud · Microsoft Sentinel · CyberArk PAM · SailPoint IIQ · Tenable/Nessus · AWS GuardDuty · Vanta · Drata · BitSight · SecurityScorecard · KnowBe4
GRC Platforms	ServiceNow IRM · OneTrust · NIST CSF Workbook (v1.1 & v2.0) · Microsoft Purview
Automation & IaC	Terraform · Python (boto3, azure-sdk) · AWS Lambda · GitHub Actions · KQL · Logic Apps (SOAR) · AWS Config Rules
Frameworks	NIST CSF 2.0 · NIST AI RMF 1.0 · EU AI Act · ISO 27001:2022 · ISO 27005 · FFIEC CAT · CIS Benchmarks · MITRE ATT&CK · SOC 2 TSC · HIPAA · PCI DSS · CBN Cybersecurity Framework 2024 · NDPA 2023 · NIST SP 800-

Keywords: *AWS, Azure, GCP, Terraform, Python, KQL, Prisma Cloud, Microsoft Sentinel, CyberArk, SailPoint, Tenable, Vanta, Drata, ServiceNow IRM, NIST CSF 2.0, NIST AI RMF, EU AI Act, ISO 27001, ISO 27005, FFIEC, OCC, HIPAA, PCI DSS, SOC 2, CBN Cybersecurity Framework, NDPA, MITRE ATT&CK, IAM governance, least privilege, CSPM, TPRM, vulnerability management, security awareness, incident response, SOAR, board reporting, AI governance.*

PROFESSIONAL EXPERIENCE

Senior GRC Manager / Cloud Security Architect — 2022 – Present

Financial Services & Technology Sector — *Canada*

- Designed and deployed a multi-cloud CSPM program across AWS, Azure, and GCP covering 570+ assets at a regional financial services firm, reducing critical and high misconfigurations by 78% within 90 days and achieved a clean internal audit result for the first time in three years
- Built an end-to-end third-party risk management program assessing 120+ SaaS and IaaS vendors in a HIPAA-regulated environment, achieving HIPAA Security Rule compliance and receiving SOC 2 Type II audit credit as a key compensating control
- Engineered a continuous compliance automation pipeline reducing manual SOC 2 and ISO 27001 evidence collection from 12 weeks to 9 business days, enabling concurrent certification within a single 12-month audit window with zero auditor exceptions
- Led a full-scale cloud IAM governance remediation across 18 AWS accounts, consolidating 340+ individual IAM users into federated SSO, eliminated all standing privileged access via CyberArk JIT, and cleared the top ITGC audit finding
- Built a cloud-native incident response capability integrating AWS and Azure telemetry into Microsoft Sentinel with 18 custom KQL detection rules mapped to MITRE ATT&CK for Cloud, reducing MTTD by 65% and automated 40% of alert responses via SOAR
- Authored a Cloud Incident Response Plan for an AWS environment aligned to NIST SP 800-61 Rev 3, defining a six-member IRT structure, six-phase IR lifecycle with formal decision gates, and external notification obligations covering OCC, FFIEC, card brands, and cyber insurers
- Designed and built a NIST CSF 2.0 implementation workbook covering all six functions including the new Govern function, spanning 108 subcategories with a 37-artifact evidence register. Used as the governance and assessment instrument across program delivery and regulatory examination engagement
- Authored cloud IAM governance playbook and eight-tier RBAC matrix governing an 18-account AWS Organizations estate, achieving a 98% quarterly access review on-time rate and reducing access exception requests by 70%
- Designed and delivered a next-generation security awareness program addressing AI-era threats, deepfake social engineering, AI-generated phishing, and business email compromise, with an 8-KPI human risk dashboard aligned to NDPA and PIPEDA; achieved 97% completion and reduced phishing click rate from 34% to under 6% within two simulation cycles
- Built an enterprise AI risk governance framework for a managed services provider, inventorying 15 AI-enabled features across RMM and PSA platforms with no prior oversight. Classified all use cases under NIST AI RMF 1.0 and EU AI Act risk categories and cut client AI-governance questionnaire turnaround from three business days to same-day

Head of Information Security (CISO) — 2019 – 2022

Community Financial Institution — *Canada*

- Built the institution's first cybersecurity program from zero as the sole security leader, designing and delivered the cybersecurity strategy, 3-year program roadmap, and KRI/KPI framework presented to the Board of Directors for approval and funding
- Authored 30+ information security policies and procedures and implemented the NIST Cybersecurity Framework across all five functions with formal control ownership assigned to IT and business stakeholders
- Designed and implemented an ISO 27001-aligned ISMS including formal risk assessment (ISO 27005), Statement of Applicability, and full Annex A control mapping, built to certification-ready standard
- Managed OCC cybersecurity examination process end-to-end, coordinating exam logistics, producing all evidence packages, presented remediation status to examiners, and closed all prior findings with zero material findings at examination
- Launched the institution's first vulnerability management program, deploying Tenable/Nessus, established asset inventory, defined risk-tiered remediation SLAs, and remediated 200+ findings in the first scan cycle

- Established board-level cybersecurity governance through quarterly Board Risk Committee reporting on program status, KRIs, and regulatory posture, giving the Board first-ever visibility into cyber risk
- Launched security awareness program achieving 95%+ staff completion rate and reducing phishing simulation click rate from 34% to under 6% within two simulation cycles

Information Security Analyst / GRC Analyst **2017 – 2019**

Financial Services Sector *Nigeria*

- Conducted information security risk assessments, gap analyses, and control evaluations across banking and financial services environments aligned to ISO 27001 and CBN regulatory requirements
- Developed and maintained information security policies, procedures, and standards supporting regulatory compliance with CBN Framework, NDPA, and internal audit requirements
- Supported compliance monitoring activities, security controls implementation, and third-party vendor assessments across multiple business units
- Delivered security awareness training and supported incident response activities including investigation, documentation, and post-incident reporting

CERTIFICATIONS

CISM Certified Information Security Manager
ISACA | Active

CISSP Certified Information Systems Security Professional
ISC2 | Active

CRISC Certified in Risk and Information Systems Control
ISACA | Active

CCSP Certified Cloud Security Professional
ISC2 | Active

EDUCATION

Master of Business Administration (MBA)
UNICAF University, Malawi | 2020

Bachelor of Science, Computer Science
Olabisi Onabanjo University, Nigeria | 2008

Academic credentials evaluated by World Education Services (WES); Canadian equivalency confirmed.

KEY PROJECTS & PORTFOLIO

Full project documentation, evidence artifacts, and detailed case studies are available at bolamabawonku.com/projects. The portfolio includes eleven documented projects with problem statements, measurable outcomes, lessons learned, and downloadable evidence artifacts.

- Greenfield Cybersecurity Program Build: Community Financial Institution (Flagship)
- Enterprise Cloud Security Posture Management Program: Multi-cloud, AWS / Azure / GCP
- Third-Party Cloud Risk Assessment Framework: HIPAA-regulated healthcare technology
- SOC 2 & ISO 27001 Compliance Automation Pipeline: concurrent certification, 12 weeks to 9 days
- Cloud IAM Governance & Least-Privilege Program: 18 AWS accounts, 340+ users consolidated
- Cloud IR Playbooks & SIEM Detection Engineering: Microsoft Sentinel, 18 custom KQL rules
- Cloud Incident Response Plan: AWS environment, NIST SP 800-61 Rev 3, 6-phase lifecycle
- NIST CSF Implementation Workbook (v1.1 & v2.0): 108 subcategories, Govern function, evidence register
- Cloud IAM Governance Playbook & RBAC Matrix: 8 tiers, 18 accounts, exception requests down 70%
- Next-Generation Security Awareness & Human Risk Management Program: AI-era threats, 8-KPI dashboard, 97% completion
- AI Risk Governance Framework: managed services provider, 15 AI use cases, NIST AI RMF 1.0 / EU AI Act

PROFESSIONAL AFFILIATIONS

ISACA, active member, CISM and CRISC credential holder

ISC2, active member, CISSP and CCSP credential holder

References available upon request · Portfolio: bolamabawonku.com · GitHub: github.com/Bolamabx · Last updated: August 2026