David Mawazo

Nairobi, Kenya | rahamawazo@gmail.com | +254 724 277 495 | linkedin.com/in/david-mawazo

Information Security Officer

CISSP and CIPT-certified information security professional with 8 years of experience across governance, risk, and compliance; information security strategy and policy development; data protection and privacy; incident response; security operations; and security awareness. Has served as the primary security adviser and risk officer across a portfolio of 10 client organisations, designing and operating ISO 27001-aligned ISMS controls, managing risk registers, coordinating internal and external audits, overseeing third-party risk, and reporting to senior management and board-level stakeholders. Carries experience in healthcare technology and regulated financial services environments, and has designed and delivered security awareness programmes for audiences ranging from individual practitioners to executive leadership. Nairobi-based with an M.Sc. in Cybersecurity from Carnegie Mellon University Africa and is pursuing CAPM certification through PMI.

Work Experience

TryHackMe, Ltd 01/2022 - 03/2026

Cyber Security Engineer and Researcher *Remote*

- Served as a subject matter expert and content engineer across the world's largest cybersecurity training platform, building and maintaining a library of rooms, labs, and certification content covering detection engineering, DFIR, cyber threat intelligence, threat emulation, SOAR, EDR triage, and SOC operations for 7 million+ users globally.
- Contributed to four professional certifications: led SAL1 (Security Analyst Level 1) from the ground up, writing 150+ scenario-based questions grounded in real SOC operations and building hands-on alert triage and incident handling simulations; contributed advanced practical scenarios to SAL2, SEC1, and SEC0.
- Analysed emerging threat actor techniques and tooling, translating real adversary behaviour into practical, hands-on lab content for SOC and blue team practitioners using MITRE ATT&CK;, SIGMA rules, Elastic SIEM, and Security Onion.
- Advised enterprise clients on security tooling selection, training pathways, and platform adoption strategies to upskill their security teams across SOC, IR, and detection disciplines.
- Achieved an average NPS of 60 across published rooms, with a high of 79 — a score considered world-class in learner recommendation benchmarks; maintained a module drop-off rate below 6%.
- Contributed to a 20% reduction in cybersecurity incidents across the platform's learner base through structured threat analysis and detection training; collaborated with product and engineering teams to keep content aligned with the evolving threat landscape.

Tabiri Analytics, Inc. 06/2019 - 01/2022

Cyber Security Engineer *Nairobi, Kenya*

- Served as the primary security adviser across 10 client organisations: developing and implementing ISO 27001-aligned information security strategies, establishing policies and standards, maintaining information asset inventories, and enforcing data retention and lifecycle management procedures aligned with regulatory requirements.
- Identified, assessed, and mitigated IT and cybersecurity risks; maintained risk registers with defined treatment plans, owners, and remediation timelines, reporting risk posture to senior leadership and board level on a quarterly basis.
- Managed end-to-end third-party and vendor security risk, coordinated internal and external compliance audits, and collaborated with IT and legal stakeholders to embed data protection governance and controls across client environments.
- Deployed and administered an Elastic Stack SIEM across client environments; led end-to-end response to a live ransomware incident including containment, root cause analysis, remediation across 20+ endpoints, and a post-incident report presented to executive leadership that became the basis for the client's security roadmap.
- Designed and delivered security and data protection awareness programmes for client organisations, raising compliance culture across technical and non-technical staff.
- Improved measured security posture by 40% and threat detection accuracy by 20% across the client portfolio, with mean detection time reduced to within 3 days.

Teletracking Technologies, Inc. 05/2018 - 12/2018

Web Application Security Engineer *Kigali, Rwanda*

• Secured web applications for a healthcare operations platform used by hospital networks across the United States; assessed against OWASP Top 10 using IBM AppScan, reducing pre-production vulnerabilities by 40% and potential breaches by 30%.

• Developed 10 security policies covering detection, prevention, and incident handling, improving client compliance posture by 33%.

Education

Master of Science, Information Technology (Cybersecurity) 06/2019
Carnegie Mellon University - Africa *Kigali, Rwanda*

Bachelor, Business Information Technology (Networking) 05/2016
Strathmore University *Nairobi, Kenya*

Certifications

CISSP 02/2026 - 01/2029
ISC2

CIPT - Certified Information Privacy Technologist 07/2019 - 07/2023
IAPP

CAPM (in progress) 2026 - Present
PMI

GRC Analyst Masterclass 08/2023 - Present
TCM Security

Certified Incident Responder 09/2024 - Present
INE

CySA+ 05/2021 - 05/2024
CompTIA

Application Security Analyst 02/2016 - Present
IBM

Awards and Scholarships

International Visitors Leadership Program - Promoting Cybersecurity 10/2021
U.S. Department of State

MINDS Scholarship Programme for Leadership Development in Africa 08/2017
Mandela Institute for Development Studies

Projects

Consultancy Project Lead - ISO 27001 Security Assessment

Rwandan Banking Institution

• Led a full ISO 27001 security assessment for a regulated Rwandan bank: asset inventory, risk assessment, control gap analysis, and a board-level remediation roadmap, coordinating across IT, compliance, and senior management. Output used directly to shape the bank's security investment roadmap.

International Visitor Leadership Program (IVLP) - Promoting Cybersecurity

U.S. Department of State

• Organised and delivered 7 security awareness workshops for 200+ professionals across East Africa; updated incident response protocols using international frameworks, cutting response time by 30%.

UK and Ireland Websites Privacy Policy Analysis

Academic Research

• Analysed GDPR compliance changes across 150 top UK and Ireland websites, examining how organisations embed data protection and privacy obligations into practice across jurisdictions.

Volunteering and Leadership

Mandela Institute for Development Studies Africa 10/2025 - Present
Alumni Regional Coordinator

Skills

Governance, Risk and Compliance: ISO 27001:2022, NIST 800-53, NIST CSF, CIS Controls, GDPR, Kenya Data Protection Act, ISMS Design and Operation, Risk Register Management, Audit Coordination, Policy Development, Regulatory Compliance, Control Assessment

Data Protection and Information Governance: Data Classification, Information Asset Inventories, Retention Schedules, Lifecycle Management, Personal Data Risk Assessment, Privacy Impact Assessments, Third-Party Data Risk, Governance Committee Coordination

Security Operations and Incident Response: Elastic Stack SIEM, Security Onion, Splunk, Wazuh, Threat Hunting, Vulnerability Management, Incident Response, Root Cause Analysis, MITRE ATT&CK;, IDS/IPS, IBM AppScan, OSINT, MISP

Stakeholder Engagement: Executive and Board Reporting, Cross-functional Advisory, Legal and IT Liaison, Security Awareness Programme Design, Non-technical Audience Communication, Multi-stakeholder Coordination

Project Delivery: Security Project Lifecycle Management, Remediation Tracking, Security Roadmap Development, KPI Reporting, CAPM (in progress - PMI)