

# Raha Mawazo

Nairobi, Kenya (open to remote and relocation) | rahamawazo@gmail.com | +254 724 277 495 | linkedin.com/in/david-mawazo

---

## Information Security and GRC Professional | CISSP, CAPM

Information security and GRC professional with eight years across ISMS ownership, risk governance, and security enablement. CISSP, CISM in progress, with an M.Sc. in Information Technology (Cybersecurity) from Carnegie Mellon University. Ran ISO 27001 assessment and audit cycles across 10 client organisations, maintained risk registers with named owners and quarterly review reported to board level, and led third-party assurance across the supplier base. Led a live ransomware response end to end. Teaching application security since 2016, from IBM AppScan certification delivery through four years designing training and certifications for a 7M-user platform. Currently building Lighthouse, a GRC platform built around living control registers and explicit, documented risk acceptance.

## Work Experience

---

**Lighthouse** | 04/2026 - Present

**Founder and Builder (Independent)** | Nairobi, Kenya

- Building a GRC platform that unifies ISO 27001, NIST CSF and Secure Controls Framework requirements into a single living control register.
- Designed the exception workflow around explicit risk acceptance: every deviation carries an owner, a rationale, a compensating control and an expiry date.
- Built vendor and third-party risk modules covering tiering, onboarding assessment and ongoing assurance.

**TryHackMe, Ltd.** | 01/2022 - 03/2026

**Cyber Security Content Engineer and Researcher** | Remote

- Authored security framework training on ISO 27001 and 27002, NIST CSF and MITRE ATT&CK for a SaaS platform serving 7M+ users.
- Led design of the SAL1 defensive security certification, 150+ scenario-based questions and simulations; contributed to SAL2, SEC0 and SEC1.
- Designed security training across SOC operations, SIEM, detection engineering and DFIR; built 4 modules in one year with drop-off below 6%.
- Authored Sigma detection-rule content mapping log sources and IOCs to MITRE ATT&CK techniques; contributed to 4 consecutive Advent of Cyber editions.
- Worked in Agile cycles with product, engineering and curriculum teams, translating security requirements into things people would actually adopt.

**Tabiri Analytics, Inc.** | 06/2019 - 05/2022

**Cyber Security Engineer** | Nairobi, Kenya

- Maintained risk registers with named owners, treatment plans and quarterly review cycles; drove mitigations to completion rather than to documentation.
- Coordinated internal and external compliance audits across 10 client organisations; kept exception records under review and tracked non-conformities to closure.
- Led ISO 27001, NIST 800-53 and CIS Controls assessments and control reviews.
- Authored company-wide security policies and standards covering access, data handling, vendor risk and incident response.
- Ran vendor and third-party risk: due diligence, onboarding assessments and ongoing supplier assurance.
- Led end-to-end response to a live ransomware incident: containment, classification, root cause analysis, remediation across 20+ endpoints, and the post-incident report presented to client executives.
- Built and operated an Elastic Stack SIEM across client environments of 5 to 80 endpoints; mean detection time within 3 days.
- Reported security posture, top risks and audit outcomes to executive and board level.

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

**Web Application Security Engineer** | Kigali, Rwanda

- Defined security specifications and countermeasures for a telemedicine platform, embedding security requirements into the development lifecycle.
- Ran OWASP Top 10 assessments of production web applications with IBM AppScan, the platform certified in and taught since 2016; developed 10 security policies covering detection, prevention and response.

**Carnegie Mellon University Africa** | 08/2018 - 05/2019

### **Graduate Teaching Assistant** | Kigali, Rwanda

- Supported two graduate courses including Introduction to Information Security: recitations, assignments, grading and office hours.
- Built the course lab: Security Onion IDS, Elastic Stack log management and a Domain Controller for user access and Active Directory management.

### **Strathmore University** | 03/2016 - 08/2016

#### **IBM AppScan Course Trainer** | Nairobi, Kenya

- Delivered the IBM AppScan certification course to two consecutive cohorts, covering web security concepts, the OWASP Top Ten and the installation, configuration and customisation of application security scans.
- Ran hands-on labs and mock examinations preparing students for the IBM-proctored certification exam; covered scan-result review, vulnerability management, fix reporting and AppScan integration into CI/CD pipelines.
- Served as liaison between the cohort and IBM's University Relations and Digital-Nation Africa lead for East Africa.

## **Education**

---

### **M.Sc. Information Technology (Cybersecurity)** | 06/2019

**Carnegie Mellon University - Africa** | Kigali, Rwanda

### **B.Sc. Business Information Technology (Networking)** | 05/2016

**Strathmore University** | Nairobi, Kenya

## **Certifications**

---

**CISSP, Certified Information Systems Security Professional, ISC2** | 02/2026 - 01/2029

**CISM, Certified Information Security Manager, ISACA** | In progress

**CAPM, Certified Associate in Project Management, PMI** | 05/2026 - Present

**Certified Incident Responder, INE** | 09/2024 - Present

**GRC Analyst Masterclass, TCM Security** | 08/2023 - Present

**Application Security Analyst Mastery Award, IBM** | 02/2016 - Present

**CySA+, Cybersecurity Analyst, CompTIA** | 05/2021 - 05/2024 (expired)

**CIPT, Certified Information Privacy Technologist, IAPP** | 07/2019 - 07/2023 (expired)

## **Projects**

---

### **ISO 27001 Security Assessment, Rwandan Banking Institution**

#### **Consultancy Project Lead**

- Ran the full cycle: asset inventory, risk assessment and control gap analysis against Annex A across the institution's technology estate.
- Delivered a board-level remediation roadmap; coordinated IT, compliance and senior management throughout.

### **Promoting Cybersecurity**

#### **International Visitor Leadership Program, U.S. Department of State**

- Delivered 7 security awareness workshops for 200+ professionals across East Africa; updated incident response protocols using international frameworks.

## **Volunteering and Leadership**

---

### **Mandela Institute for Development Studies Africa** | 10/2025 - Present

**Alumni Regional Coordinator**

## **Skills**

---

**ISMS Ownership:** ISO 27001 and 27002, NIST CSF, NIST 800-53, CIS Controls, internal audit and evidence cycles, management review, corrective actions, external audit readiness, policy and standards authorship, exception and non-conformity management.

**Risk Governance:** Living risk registers with named owners, treatment plans and review cycles, explicit and documented risk acceptance, vendor and third-party risk tiering and due diligence, leadership reporting on posture, top risks and audit outcomes.

**Incident and Operations:** Incident classification, escalation, containment, root cause analysis and post-incident learning loops, Elastic Stack SIEM design and operation, Security Onion, Sigma detection rules, threat hunting, vulnerability assessment, OWASP Top 10.

**Enablement and Communication:** Security awareness and training design, certification and assessment design, translating security into decisions for engineering and leadership audiences, influencing without authority across product, engineering and compliance teams.

**Languages:** English (fluent; all education and professional delivery conducted in English). French (conversational).