**Mogoi Matongo**

**Email:** mematongo@gmail.com

**Summary**

Experienced Information Security Systems Security, Cybersecurity Analyst with 2 years in the IT industry with extensive knowledge in Information Security, Data Analytic and reporting, Incident Response and Software Development Lifecycle (SDCL) project within domains such as Government Healthcare, Finance, and the educational sector. Dynamic team player for agile project with expertise managing large enterprise software development projects that meet demanding time restraints and exceed all expectations.

**CONTROLS & FRAMEWORKS**

NIST RMF (FISMA), FedRAMP, NIST SP 800-53, 800-53A, 800-60, 800-18, 800-37, 800-30, 800-137, PCI DSS, ISO 27001:2013/27002:2013 SOC 1 & 2, HITRUST, Third Party Risk Management.

**SOFTWARE AND PLATFORM**

RSA Archer, Hiperos, OneTrust, ServiceNow, Security Scorecard, Microsoft Suite, Google Suite, Tenable Security Center, Microsoft Word, Excel, Project, Access, Power Point, SharePoint, Smartsheet. Tableau

**EDUCATION AND CERTIFICATIONS**

⮚ Bachelor of Computer Science-Graduation May-2025

**PROFESSIONAL EXPERIENCE**

**IT SECURITY Internship- May-August 2023 General Dynamics Information Technology, VA**

⮚ Completed remediation plans for all POA&Ms.

⮚ Developed FISMA compliance and privacy documentations to support the migration of legacy and mainframe.

applications from datacenters to the cloud.

⮚ Completed and maintain the following SAP documentation at least annually or as their respective systems changes:

o FIPS 199, E-Authentication Worksheet, Privacy Threshold Analysis (PTA), Privacy Impact Assessment

(PIA) & System of Records Notice (SORN) – as required, Security Plan (SP), Contingency Plan (CP) &

Contingency Plan Test Results (CPTR), and all other required security documentation.

⮚ Ensured security controls are met at inception and throughout system development cycle.

⮚ Ensured systems are properly patched and hardened according to organizations requirements.

⮚ Ensured Rules of Behavior are signed for all system users.

⮚ Completed Waivers and Accepted Risks (WEAR) as required to be presented to the Authorization Official.

⮚ Reviewed Audit Logs on a weekly basis and recording the findings in an Audit Log Review Tracker.

⮚ Reviewed system accounts monthly and recording the findings in an Account Management Review Tracker.

⮚ Uploaded Plan of Action and Milestones (POA&M) into Cyber Security Assessment and Management (CSAM) tool

and validated artifacts provided to remediate respective POA&M items.

**IT SECURITY Internship May 21 – August 2022 Raag Solutions Raleigh, NC**

⮚ Engage with other information security risk personnel across the organization to help identify enterprise-level.

risks.

⮚ Ensure the implementation of information risk programs that identify, measure, track and remediate risks with

business owners.

⮚ Lead annual audits for industry specific reports, including ISO27001, ISO 27701 and SOC 2 Type II reports.

⮚ Coordinate with external auditors and internal control owners through kickoff meetings, interview requests,

closing meetings and evidence gathering to accomplish operational task.

⮚ Documents findings and assesses risk where deviations exist resulting from internal and external testing.

⮚ Performs assessment and provides feedback by defining appropriate risk levels and corrective actions for issues.

identified to ensure compliance.

⮚ Performs risk and control assessment for all high-risk third-party service providers to evaluate effectiveness of

control system.

⮚ Write and edit policies and reports whiles testing the operation of general, contractual controls.

⮚ Performs IT & Risk Security Risk & Control Assessments for new products/initiatives.

⮚ Reviews services provided by Third-Party vendors and ensured adherence to standards and risk tolerance.