

FELICIA AWAZI | (713) 505-4204 | awazifelicia4@yahoo.com | Rosenberg, Texas

PROFESSIONAL SUMMARY

Cybersecurity Governance, Risk, and Compliance (GRC) professional experienced in risk management, regulatory compliance, and internal controls. Background spans healthcare, banking, insurance, and retail sectors. Skilled in leveraging GRC platforms to conduct risk assessments, support audits, and translate regulatory requirements into actionable controls that strengthen security, privacy, data protection, and organizational resilience. Lead cross-functional initiatives that enhance compliance, reduce risk exposure, and align security with business goals.

SKILLS AND COMPETENCIES

- **Risk & Compliance:** Enterprise Risk Management (ERM), ISO 31000, Regulatory Compliance (FISMA, HIPAA, PCI-DSS, GDPR, SOX, CCPA, NYDFS, GLBA)
- **Frameworks & Controls:** HITRUST, COBIT, ISO 27001, NIST CSF, SOC 2, Internal Controls
- **Governance and Operations:** Policy Development, Risk Assessment, Incident Response, Business Continuity Planning, Compliance Metrics and Reporting
- **Project Tools:** RSA Archer, ServiceNow, MetricStream, OneTrust, Jira, Confluence, SharePoint, Power BI, Microsoft Sentinel
- **Productivity:** Microsoft Office Suite (Word, Excel, PowerPoint)

PROFESSIONAL EXPERIENCE

Governance, Risk and Compliance (GRC) Analyst | SAIC, Reston, VA | Sep 2022 – Present

- Develop and implement GRC frameworks to support critical IT systems, ensuring cloud migration projects comply with FISMA and NIST SP 800 series requirements
- Conduct security control assessments and internal audits, identifying gaps and driving remediation to improve compliance scores by 75%
- Perform identity and access management (IAM) assessments, including access reviews and role-based access control (RBAC) evaluation, enhancing access governance
- Maintain and report on the enterprise risk register, reducing high-risk findings by 20% through proactive mitigation
- Collaborate with development teams to integrate risk controls into the System Development Life Cycle (SDLC), improving compliance and reducing vulnerabilities
- Streamline incident response by documenting cases and collecting evidence within 24 hours, reducing audit findings by 25%, and maintaining regulatory compliance

Information Security Compliance Analyst | Wex Health, Portland, ME | May 2020 – Aug 2022

- Implemented HIPAA and HITRUST-aligned GRC frameworks, integrating risk controls into production systems to protect PHI
- Collaborated with IT to develop, update, and maintain PCI DSS security policies and procedures, ensuring compliance and remediating deficiencies
- Maintained the enterprise risk register and generated detailed reports and Power BI dashboards highlighting key risks, vulnerabilities, and mitigation strategies

- Led audit preparation by validating technical evidence, ensured proper system configuration, and supported third-party assessments
- Leveraged GRC tools, compliance platforms, vulnerability management solutions, and cloud security technologies to strengthen organizational risk posture
- Partnered with IT and cross-functional teams to monitor 75+ controls and deliver KPI/KRI dashboard reports that informed executive decisions

Information Security Risk Compliance Analyst | USAA, San Antonio, TX | Mar 2018 – Apr 2020

- Reviewed and enhanced security policies to align with industry standards, strengthened governance, and supported Material Risk Identification (MRIA) reviews
- Integrated GRC frameworks into the SDLC and maintained a centralized IT risk register, ensured compliance with NIST SP 800-53 and supported scenario analysis activities
- Validated controls and documented evidence for PCI-DSS, GDPR, and SOC 2 assessments, maintained the risk register and supported audit readiness
- Executed Risk Control Self-Assessments (RCSA) and supported regulatory oversight activities, ensuring control design and effectiveness were tested and documented
- Led implementation and monitoring of security controls, improving compliance posture and establishing measurable KRIs for continuous oversight
- Reduced operational risk exposure by 20% through proactive mitigation and delivered executive-level risk reports for governance committees

Cybersecurity Risk Analyst | Kroger, Cincinnati, OH | Feb 2015 – Jan 2018

- Performed risk assessments across enterprise retail systems, identifying vulnerabilities and driving PCI-DSS-aligned mitigation plans
- Developed and updated security and data protection policies, strengthening PCI-DSS and privacy compliance
- Collaborated with IT and operations teams to identify, assess, and remediate risks, aligning efforts with company policies and compliance objectives
- Supported audit readiness by gathering documentation, preparing evidence, and participating in internal and external audits to ensure compliance
- Monitored security alerts, incidents, and vulnerability findings, working with operations teams to track remediation efforts and strengthen overall security posture

EDUCATION & CERTIFICATIONS

Bachelor's Degree in Business Administration, University of Buea

Certifications: Certified in Risk and Information Systems Control (CRISC) | AWS Certified Cloud Practitioner (CCP) | Project Management Professional (PMP) | SAFe 6.0 | Professional Scrum Master (PSM) | Security Clearance