AKANDU I. UKOHA CISM, CRISC, Sec+

Email: akukoha1@gmail.com Phone: 443.939.0570

EXPERIENCE SUMMARY

Information Technology professional with 10+ years' experience in Information Security Audits/Assessments, Third Party Risk Management (TPRM) and Governance, Risk and Compliance (GRC). Proven track record in leading compliance audits, developing risk management frameworks, and securing sensitive information for federal government agencies and Fortune 500 companies.

KEY SKILL AREAS

- Vendor Risk Management
- CISO Office Liaison
- Governance, Risk and Compliance
- ISO 27001/SOC2/ PCI-DSS/NIST 800-53/SOX/FedRAMP
- Information Security Assessments and Audits
- Cyber Security Policy Development
- Information Security Compliance
- Risk Assessment and Vulnerability Management
- Information Assurance/Certification and Accreditation
- Experience with tools such as Splunk, Tenable, Okta and Carbon Black
- SDLC – Agile/Waterfall

PROFESSIONAL EXPERIENCE

UBS, Remote **(05/2021- present)**

Associate Director

- Proactively identified process and control deficiencies and helped to execute process improvement initiatives.
- Ensured controls are in place to provide and maintain a secure and regulatory compliant technology environment by focusing on all aspects of compliance, including Sarbanes Oxley (SOX), CCPA, GDRP.
- Coordinate internal compliance audits and risk assessments, including documentation, artifacts submission, process flows, and testing.
- Provided subject matter expertise for quality assurance programs, including attestation, vendor questionnaire design, and management reporting.
- Successfully led, organized and completed ISO 27001, SOX, HIPAA and SOC 2 audit activities which resulted in the assignment of the certificate to various UBS business divisions and services.
- Developed and updated information security policies, standards and procedures as necessary.
- Worked with System Engineering and Security Teams to improve the Vulnerability Management process. This led to development of scope, categorization and remediation timelines of vulnerabilities. Also developed VM metrics to be presented weekly to senior information security staff to show status of VM tasks.
- Developed the Vendor Assessment and Third Party Risk Management Program using OneTrust to identify high risk vendors, perform due diligence to ensure alignment with UBS security standards and gain business acceptance before onboarding.
- Ensured vendor questionnaires and regulatory exams are completed promptly. Provided accurate and timely responses which included direct engagement with examiners.
- Developed a remediation plan and coordinated with teams to ensure all audit findings or corrective actions are remediated as required. These activities led to the closure of all audit related control deficiencies.
- Developed monthly security metrics/reports on behalf of the team to be presented at Senior Management Review Meetings.

Peraton (DHS Contract), Washington DC **(05/2020- 09/2021)**

Information System Security Officer (ISSO)

- Ensure that selected security controls are implemented and operating as intended during all phases of the Information Security (IS) lifecycle.
- Develop Plan of Actions and Milestones (POA&Ms) to evaluate and track discovered security weaknesses.
- Develop, maintain, review, update and route documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages, System Requirements Traceability Matrices (SRTMs) and other documents in order for the Program to obtain an ATO.
- Researches, evaluates and recommends new security tools, techniques, and technologies and introduces them to the enterprise in alignment with IT security strategy.
- Updating and Tracking POA&M's, developing Security Plans, Contingency Plans, System Categorization, Security Assessments, Disaster Recovery Plans, and Business Continuity Plans Reviewing scan results, working with system owners, writing security documentation, including Security plans, SSP's, SOP's, IRP'S, DRP's, and Contingency Plans
- Maintain operational security posture for system(s) through customized Risk Management Framework (RMF) to ensure established security processes and procedures are followed.
- Perform vulnerability scanning, risk assessment analysis using NIST 800-53 and prepare responses to Plan of Action and Milestones (POA&Ms).
- Provide configuration management and documentation for system software, hardware, networks, enclaves, etc.
- Evaluate security solutions to ensure they meet security requirements for processing classified information; perform vulnerability/risk assessment analysis to support certification and accreditation.

Department of Commerce (NOAA), Silver Spring MD **(12/2019- 03/2020)**

Information Technology Security Officer (ITSO)

- Coordinate and document an annual risk assessment as well as ad hoc project risk assessments.
- Review risk assessment documentation for completeness and appropriate selections of controls.
- Assist in enforcing a company-wide security awareness program that is tailored to the needs of specific roles within the organization and is measurable and auditable.
- Design and implement a program to collect and report information security related performance metrics and key risk indicators.
- Work collaboratively with all NOAA office lines to ensure that their practices are consistent with corporate information security policies and standards.
- Identify compliance objectives and mapped program deliverables to the requirements
- Assess organization-wide compliance with NOAA's policies and standards and take action to remediate non-compliance.
- Recommend controls to reduce risks to levels that align with the organization's risk tolerance.
- Ensure that NOAA is properly evaluating security risks through the NIST framework that assesses the potential impact of threats to the organization's information systems.
- Provide updates to senior management concerning any policy or documentation required for compliance to FISMA guidelines.

Housing Authority of Baltimore City, MD **(01/2018- 12/2019)**

Information Security Officer

- Conducting meetings with the client to discuss client's material weaknesses identified in an audit to gain an understanding and develop mitigation strategies for the findings.
- Conduct POA&M management by tracking and addressing weaknesses, as needed.
- Coordinate with POCs to request artifacts to close out POA&Ms.

- Meet with system point of contacts to discuss and provide guidance on remediation strategies.
- Communicate complex technology and security concepts and methodologies to senior leadership to support development of enterprise security strategy implementation.
- Serve as a subject matter expert in governance and leadership by reviewing and developing effective structure for communicating, decision making and responding to security threats across an organization
- Update security configurations by routinely reviewing vendor sites, bulletins, and notifications for security information.
- Provide technical advice on access control, security models, disaster recovery, business continuity planning, and security awareness training.
- Plan, implement and monitor internal information technology security policies, application security, access control, and corporate data safeguards
- Discuss and develop security strategies with CIO after weekly review of network vulnerability assessment results.
- Wrote and updated detailed guides on procedural implementation of security controls in the agency.
- Subject Matter Expert for security policy and privacy related questions.
- Manage responses to all IT and security and compliance related inquiries from 3rd parties.

Morgan Stanley

Information Security Analyst **(12/2013 – 12/2017)**

- Initiated and established a Role Based Access Control (RBAC) method for finance divisions to define controls for managing access and reducing risk.
- Managing role certification campaigns to confirm access controls and ownership.
- Coordinate meetings with senior officers of Morgan Stanley to determine privileges and access requirements relating to their departments.
- Developed materials to educate staff on the benefit of Role Based Access Control policy for the firm.
- Trained junior analysts on the daily tasks associated with provisioning appropriate access.
- Processed user access requests, modifications, terminations.
- Communicating status across the firm charting progress against the Identity Access Management program roadmap.
- Assist Project/Audit Lead with Semi Annual Access Review process for financial divisions.
- Work with various business and IT application owners to define Role-based access templates for implementing RBAC for multiple applications.

CERTIFICATIONS: Certified Information Security Manager (CISM)
CompTIA Security+
Scrum Master
Certified in Risk and Information Systems Control (CRISC)
Certified Information Security Auditor (CISA) - **In Progress**

EDUCATION:
University of Baltimore, Baltimore MD
BSc Finance