Januarius J. Asongu

Townsend, DE 19734
Tel: 302-546-9700 ▪ Email: asongu2@gmail.com

IT Governance, Risk & Compliance Professional

Risk Management and Information Technology professional with extensive experience in risk management and assessment, infrastructure, network, cloud, and application security, IT security architecture, IT auditing, IT controls and compliance, third party/vendor management, and data governance. Over 20 years of experience working with Big Banks like JPMorgan Chase (JPMC), Sumitomo Mitsui Banking Corporation (SMBC) and City National Bank (Royal Bank of Canada); and leading consulting firms like Ernst & Young (EY) and Boston Consulting Group (BCG Platinion). Industry certifications include ***CCIO, CISA, CISM, CRISC, CDPSE, CGEIT, CISSP, AWS-SCS*** *etc.*

Professional Experience

City National Bank (Royal Bank of Canada) / Akraya, Los Angeles, CA (Remote)
CYBER & TECHNOLOGY RISK ANALYST, January 2022 - Present

- Identify, analyze and report enterprise technology risks for executive level business, Cyber, Technology and information security leadership; sharing work product with the Audit and Risk Committee, Royal Bank of Canada, and CNB's regulators.
- Perform quantitative and qualitative analysis to support the prioritization of risk mitigation projects, measure progress of technology risk reduction initiatives, and identify areas with high residual risk.
- Provide challenge and oversight of the First Line of Defense as a member of the Second Line of Defense, and develop, collect and report metrics and Key Risk Indicators (KRI) which provide effective, proactive identification of technology risks.
- Contribute to the governance of Information Technology Framework, Policy and Standards; translate complex regulations into clear, easily understood regulatory requirements and desired outcomes; and perform gap analysis.
- Support the implementation of a data risk and oversight function as a key component of CNB's second line of defense strategy; and engage with key stakeholders to complete deep dive assessments and achieve MRA compliance.
- Ensure risk assessments are completed, are appropriately scoped, and provide assurance through independent review and challenge of management control testing, including applications, data centers, databases, and infrastructure.
- Perform independent categorization and aggregation of technology risks identified by the first line of defense, and provide a thematic view of risk across the enterprise.
- Map regulatory requirements across regulations to identify overlapping requirements and compliance efficiencies; and track regulatory compliance and maintain up to date records of requirements and corresponding mitigating controls.
- Manage the IT Framework, Policy and Standards governance process as new and revised materials progress through their lifecycle, including work with relevant committees and Bank stakeholders.

JPMorgan Chase & Co, Newark, DE
VICE PRESIDENT, SUPPLIER ASSURANCE / THIRD PARTY RISK MANAGEMENT, March 2019 – January 2022

- Accountable for executing the global comprehensive risk management and assessment programs for all in-scope suppliers within JPMC's Corporate Third-Party Oversight (CTPO) program.
- Accountable for driving several programs that support the Cybersecurity and Technology Controls (CTC) function, including implementing and operating controls and processes that further enhance the security posture of JPMC's supply chain.
- Leading team in identifying, evaluation and reporting on legal and regulatory, IT, and cybersecurity risk to information assets, while supporting and advancing business objectives, and displaying broad cybersecurity experience.
- Supporting the onboarding of new suppliers and/or technologies by performing risk assessments of the suppliers/technologies and ensuring compliance with corporate policies and industry regulations and standards.
- Contributing to the development/improvement of the Third-Party Risk Management governance framework and developing and executing firm-wide risk assessments of processes, products, or programs, with focus on consistency.
- Assessing remediation plans and non-compliance acceptances across multiple business lines where technology standards' compliance cannot be achieved; and publishing reports, risk scores, and other data on daily, weekly, and/or monthly basis.
- Identifying opportunities to improve third party risk posture, developing creative solutions for mitigating risks, and driving compliance to adhere to best risk management practices throughout the organization.
- Work in close collaboration with Legal, Compliance, Product, Customer Support, IT/INFOSEC, Procurement, and Human Resources teams to instill trust in the integrity of the Supplier's products and/or services.

continued…

- Received recognition for successfully conducting a complex high-stake assessment that paved the way for JPMorgan Chase launching it cryptocurrency (JPM Coin).
- Serving as a subject matter expert on COBIT, ITIL, COSO, NIST CSF/RMF, ISO 27000/31000/26000, HIPAA, GDPR, FFIEC, PCI-DSS, SOX, SOC, ISO 2700X etc.

Ernst & Young LLP, Tysons Corner, VA
IT RISK / INFORMATION SYSTEMS SECURITY OFFICER, October 2018 - March 2019

- As a member of the Technology Risk (IT Audit) team, I served as a key resource in delivering quality client services on financial statement audits, attestation engagements and IT control projects.
- Provided information assurance, information security, and risk management using leading standards (e.g., COSO, ERM, FISCAM, FISMA, NIST), and prepared written materials, presented project results to clients as well as formal feedback.
- Led the Information Security team on a high-stake Department of Defense (DoD) cloud-based (Azure) project (Leadership Dashboard), which integrated various databases and made use of Artificial Intelligence (AI), data mining, statistics, machine learning, search, and data analytics solutions.
- Responsible for securing a high-classified system by providing technical guidance and completing tasks leading to the Authorization to Operate (ATO) including developing policies and procedures for onboarding, data access, use, and reporting.
- Developed the System Security Plan, POA&Ms, BCP/DRP, IRP, SAP and other critical NIST RMF documentation.
- Implemented the NIST Risk Management Framework, complying with applicable Federal regulations including OMB Circular A-123, FISCAM, FISMA, FedRAMP, NIST and FIPS.
- Selecting security controls, documenting the implementation of security controls, assessing the implementation of security controls, assembling security authorization packages, and managing POA&Ms.
- Assisted in the implementation of platform, application, storage, network, virtualization, and cloud security best practices and enforced HIPAA, NIST 800-53, FedRAMP and other Compliance Program policies.

AspireLogy, Dover, DE
MANAGING DIRECTOR – CYBERSECURITY ADVISORY SERVICES, August 2013 - October 2018

- Led a small team of cybersecurity policy and compliance experts to expand the business in several cybersecurity advisory service areas.
- Developed technology roadmaps, project and budget plans, service and support models, manage risk assessments, and developed service delivery updates to communicate / present to senior leadership teams.
- Conducted research as needed, tested IT general and application controls, prepared for and led client meetings, established relationships with client personnel at the appropriate levels, and deepen sector and client knowledge.
- Worked across a wide spectrum of computing environments, including simple and complex on-premises corporate environments, modern commercial cloud-hosted applications, hybrid deployment models etc.
- Worked with new technology and explored industry best practices for security compliance to better deliver advice and credible recommendations to a growing company and our valued clients.
- Developed Audit plans and conducted Audits and Risk Assessments for various clients in diverse industries including Financial Services, Education, Healthcare, IT etc.
- Collaborates with key stakeholders in the identification of risks through risk assessments and measuring the risks utilizing the risk rating methodology.
- Monitors and follows up on the operational risk events submitted by management to ensure corrective actions including a root cause analysis on identified operational risk events.
- Provides control oversight to ensure compliance with laws and regulations; advises senior management on the status of their control environment related to risk identification and control weaknesses.
- Develops and maintains processes, procedures and tools for managing exception alerts as they occur, including monitoring of resulting exception cases.
- Implementing action plans identified from management self-reported issues and risk assessments and perform a quality assurance review of evidence to support issue management regarding closure or completion of remediation plans.

continued…

- Build customized professional development plans for new staff based on their strengths, weaknesses, and evolving market demands.
- Perform team management to ensure project deliverables meet quality standards and are delivered on time and within budget.
- Develop standardized and repeatable assessment templates and tools to enhance the Team's ability to perform advisory services using a mix of available staff with high quality results.
- Develop security implementation roadmaps and guide customers through prioritized action plans.
- Serve as the technical advisor to organizational leaders and decision-makers as it relates to cost-effective security implementation.

IRGB, Rockford, IL
IT AUDIT LEAD / THIRD-PARTY RISK MANAGER, August 2008 – July 2013

- Developed internal audit and TPRM policies and procedures, and established relationships with internal business partners by executing efficient audit work and enhancing risk management based on an enterprise-wide view of risk management.
- Developed valuable and positive relationships with internal business partners by executing efficient audit work and offering suggestions to enhance risk management based on an enterprise-wide view of technology risk management.
- Led the execution of the audit process and vendor risk assessments, including performing IT Audit fieldwork and provided subject matter knowledge/skills and/or to designed and conducted tests of internal controls.
- Evaluated business impact and significance of audit findings, identifying mitigating controls and other factors, and assessing whether residual risks are consistent with risk tolerance and prudent risk management.

GTC, Hyattsville, MD
INFORMATION SECURITY ANALYST / IT AUDITOR, May 2002 – August 2008

- Led and mentored project teams focused on advisory projects and assisted engagement management to successfully complete engagement objectives.
- Scheduled and oversaw the work of audit teams and based on the work performed, drafted strategic, business focused audit reports to identify and communicate issues.
- Performed and documented work such as audit scoping, procedure development, walkthroughs and controls testing of higher risk and/or complex areas in accordance with Internal Audit standards.
- Assessed systems to determine system security status and ensured adherence to security policy, procedures, and standards.
- Performed upgrades, patches, and other general security measures to better secure systems.
- Analyzed network traffic to identify anomalies and test controls for weakness and identified security threats.

Education

- **PhD in Cyber Security & Business Administration,** Charisma University, Turks & Caicos Islands
- **Master of Science (MS) in Information Technology,** University of Maryland, Adelphi, MD
- **Bachelor of Philosophy (BPhil),** Pontifical Urban University, Rome

IT Certifications

Amazon Web Services Certified Security - Specialty **(AWS-SCS),** Certified Information Systems Security Professional **(CISSP),** Certified in the Governance of Enterprise IT **(CGEIT),** Certified Data Privacy Solutions Engineer **(CDPSE),** Certified in Risk and Information Systems Control **(CRISC),** IBM Blockchain Essentials, Certified Information Security Manager **(CISM),** Certified Information Systems Auditor **(CISA),** Chief Information Officer **(CIO)** Certificate etc.

IT Tools

Microsoft Office Suite (Word, Outlook, PPT, Excel, Publisher etc), MS Visio, MS Project, MS Teams, G-Suite, CyberArk, Keychain, SailPoint IdentityIQ, ServiceNow, Slack, Salesforce, IBM Lotus Notes, RSA Archer, ProcessUnity, Audit Board, eMASS, CSAM, DISA STIGs, Qualys, Nessus, Veracode, Jira, GitHub, SharePoint, AWS & Azure native tools, Splunk, Confluence, Tableau, InfoSec IQ, Rapid7, Banker's Academy LMS, Google Analytics etc.

continued…