RAFIU OLANREWAJU BABATUNDE

Senior Audit and Compliance Analyst

**Location:** Houston, TX **| Email:** babatunderafiu68@gmail.com**| Phone:** +1 (832) 660-1087

# Professional Summary:

As a certified and seasoned expert in Information Technology Risk and Security, I bring a wealth of experience to the table. My proficiency lies in adeptly managing risks, implementing cybersecurity measures, overseeing IT General Controls, and meticulously documenting third-party security and information assurance. My fervor for conducting comprehensive information systems security control risk assessments and IT audits, coupled with my skills in vulnerability management, threat modeling, and application security, set me apart. I have also led projects ensuring meticulous security documentation, compliance adherence, and regulatory alignment, consistently upholding industry best practices. I excel in collaborative team environments, valuing transparency and cooperative work dynamics. Grounded in profound knowledge of industry frameworks and optimal strategies for both IT systems and business processes, I am primed to make a strategic impact.

# Professional Expertise:

* **Audit & Security Expertise:** Internal Audit, COBIT, SOX Compliance, Risk Management, NIST SP, ISO 27001, COSO, ISO 27002, NIST 800-53, NIST CSF, PCI-DSS, SOC Controls, IT Change Management, Internal Control, Organization Restructuring, Cultural Transformation.
* **GRC Proficiency:** Utilize GRC tools to centralize compliance management, track activities, and generate reports.
* **Application & ERP Insight:** Review Application Controls, Third-Party Security, ERP systems, Office 365, SAP, JDE, Oracle DB.
* **SOC Understanding:** Familiar with SOC 1, SOC 2, SOC 3 for service organization controls, financial reporting, security, and privacy.
* **Risk Assessment:** Diligently assess DLP solutions, configuration, and data loss risk.
* **Effective Communication:** Bridge business-tech gap, excel in documentation, scope management, and C-suite interactions.
* **Relationship Building:** Skillfully build relationships while addressing challenging inquiries.
* **Cybersecurity Proficiency:** Well-versed in NIST Framework, CSA, STRIDE, Merger & Acquisition security, Threat Modeling, Penetration Testing.
* **Broad Security Knowledge:** Infrastructure, Risk, Cloud, Cryptography, IAM, EDR/XDR/MDR, Amazon Web Services (AWS), Network Segmentation, Firewalls.
* **Vulnerability Management:** Utilize tools like Veracode, Nexus, Nessus for effective vulnerability management.
* **Technical Aptitude:** Expertise in network security tech, identity management, and technical controls implementation.

# Education:

* **Bachelor of Science in Banking and Finance**

Lagos State Polytechnic **2000**

# Certification:

* Certified Information Systems Auditor (CISA)
* Certified Information Security Manager (CISM)
* Certified In Risk and Information Systems Control (CRISC)
* Certified Ethical Hacker (CEH)
* Project Management Certified
* Computer Hacking Forensic Investigator (CHFI)

# Skills:

|  |  |
| --- | --- |
| **Audit and Compliance:** | Internal Audit, COBIT, SOX Compliance, Risk Management, NIST SP, ISO 27001, COSO, ISO 27002, NIST 800-53, NIST CSF, PCI-DSS |
| **GRC Tools:** | Centralized Compliance Management, Compliance Tracking, Reporting |
| **Application and ERP:** | Application Controls Review, Third-Party Security, ERP Systems, Office 365, SAP, JDE, Oracle DB |
| **Service Controls (SOC):** | SOC 1, SOC 2, SOC 3 Understanding, Financial Reporting Controls, Security & Privacy Controls |
| **Risk Assessment:** | DLP Solution Assessment, Risk Evaluation, Data Loss Risk Mitigation |
| **Communication:** | Bridging Business-Tech Gap, Documentation Excellence, Scope Management, C-Suite Interaction |
| **Relationship Building:** | Building Rapport, Handling Challenging Inquiries |
| **Cybersecurity:** | NIST Framework, CSA, STRIDE, Merger & Acquisition Security, Threat Modeling, Penetration Testing |
| **Broad Security Knowledge:** | Infrastructure Security, Risk Management, Cloud Security, Cryptography, IAM, EDR/XDR/MDR, AWS, Network Segmentation, Firewalls |
| **Vulnerability Management:** | Veracode, Nexus, Nessus, Vulnerability Identification & Mitigation |
| **Technical Aptitude:** | Network Security Tech, Identity Management, Technical Controls Implementation, Endpoint Security, Incident Response |

# Experience:

## Dell Technologies

## Role: Senior Audit and Compliance Analyst Jan 2022 - Current

## Responsibilities:

* Conducted 25+ comprehensive internal audits using frameworks such as COBIT and NIST SP, ensuring alignment with industry standards and regulatory requirements.
* Managed end-to-end SOX compliance activities, overseeing 15 key controls and contributing to the completion of 3 successful audit cycles.
* Led a cross-functional team to implement and document controls for ISO 27001 certification, resulting in a successful audit outcome and improved information security posture.
* Collaborated with IT department to assess and enhance IT general controls, resulting in a 20% reduction in potential vulnerabilities.
* Coordinated the review of 35+ application controls within ERP systems, identifying and addressing security gaps to ensure data integrity and privacy.
* Facilitated the implementation of a centralized GRC tool, streamlining compliance management, tracking activities, and generating monthly compliance reports.
* Orchestrated the evaluation of third-party security requirements for vendors, contributing to a 15% reduction in vendor-related security risks.
* Executed thorough risk assessments of 3 DLP solutions, recommending policy adjustments that led to a 25% reduction in data loss risks.
* Collaborated closely with technical teams to conduct 13 threat modeling sessions, enhancing proactive security measures and aligning them with business objectives.
* Utilized tools such as Veracode and Nessus to identify vulnerabilities, leading to the successful mitigation of 40+ critical security risks.
* Spearheaded the implementation of network segmentation strategies using Firewalls and AWS security groups, bolstering security by isolating critical assets from potential threats.

## Omerta Global Consult

## Role: Senior Security Consultant Jul 2017 – Dec 2021

## Responsibilities:

* Lead IT security review and application security assessments, work with application owners and external vendors to remediate vulnerabilities and deficiencies.
* Lead and manage team to mitigate information technology and security risks within agreed policies, procedures, standards, and risk limits.
* Create Threat Models and Identify Security overlays for overlays for architecture to identify gaps and work with project teams to improve security.
* Help identify risks and design controls around applications.
* Facilitate team meetings and discussions with management.
* Communicate actively and efficiently with seniors, managers, and clients throughout an engagement.
* Proactively interact with POC to gather security evidence, resolve audit-related problems, and made recommendations for business and process improvements.
* Multi-task and work with a sense of urgency to allow for on time delivery of high-quality audit reports.

## The Home Depot

## Role: Governance Risk and Compliance (GRC) & Third-Party Security Consultant Nov 2014 – Jul 2017

## Responsibilities:

* Helped clients identify IT risks and ensure controls implemented are well designed and working as intended. This includes the evaluation of the efficiency and effectiveness of IT General Controls, application controls, Security controls, while leveraging on ISO 27001, COSO and COBIT frameworks.
* Performed audit procedures, including risk-based controls, through various means- inspection, observation, and re-performance.
* Performed Sarbanes-Oxley (SOX 404) audit and review of service organizational controls SOC 1, Type 2 review.
* Worked with external auditors during the annual audit, SOX audit and the SSAE 16 audits (SOC 1 Type 2).
* Interpreted technical procedures to validate compliance with maintenance practices and program management guidance.
* Tested the design and effectiveness of internal controls by completing walk-throughs of complex business processes and analyzing results.
* Diligently tracked remediation plans to confirm proper resolution.
* Performed Security risk assessment of vendors and third parties and ensure data protection objectives.
* Performed review of security evidence like SOC 2, vulnerability assessment report, penetration tests and policies and procedures.
* Interpreted technical procedures to validate compliance with maintenance practices and program management guidance.
* Diligently tracked remediation plans to confirm proper resolution.

## EY, Nigeria

## Role: Security Advisor Dec 2012 – Oct 2014

## Responsibilities:

* Assisted in the development, implementation and maintenance of policies, procedures, standards, and guidelines in accordance with applicable regulations including ISO 27001, NIST 800-53 Framework Controls and HIPAA.
* Created information security documentation and workflows to assist with incident response, audits, and vendor requirements.
* Assisted management in overseeing security incident handling efforts in response to a detected incident and coordinated with other stakeholders as directed.
* Directed the creation and organization of a comprehensive workflow, training, and security awareness for the department.
* Negotiates with suppliers the supplier security contract language. This includes commenting on parent contract language regarding backup and recovery, audit rights, business continuity, disaster recovery, termination, offshoring and outsourcing, and other information security concerns.
* Perform security control assessment as part of Assessment and Authorization (A&A) and continuous monitoring.
* Conduct risk assessments regularly to make sure system weaknesses are well documented and mitigating processes are put in place.
* Assesses SOC Reports & SIG to make sure it complies with company’s Control Standards.

## EY, Nigeria

## Role: Internal Audit Advisory Dec 2012 – Oct 2014

## Responsibilities:

* Performed assessment of IT internal controls over financial reporting (ICFR) at client’s place.
* Implemented process improvements to SOX testing, resulting in efficiency in review time and desirable financial reporting.
* Work with the Vendor Management Office and Head Strategic Sourcing & Vendor Management to formulate holistic strategy around key third parties.
* Reviewed SDLC, manual and automated controls, and oversaw the implementation of corrective action plans while maintaining communication with all levels of management
* Met with process owners and other point of contact to remediate audit findings/exceptions and as follow up to ensure system and process security.
* Led and managed testing of controls and ensured controls were adequately designed (TOD) and working effectively (TOE) to mitigate information technology and security risks within agreed policies, procedures, standards, and risk limits.
* Performed assessments of application controls and IT general controls such as access control, change management, operations, disaster recovery and job scheduling.
* Share bi-weekly IT SOX status dashboards with Project lead so that we can all be on the same page and know the overall status of our work, key milestones, and remediation breakdown.
* Part of the buy-side programmed management team for the post-merger integration of two Major Privatized Power Distribution Companies in Nigeria.

## KPMG, Nigeria

## Role: Senior Security Assessor Apr 2010 – Dec 2012

## Responsibilities:

* Responsible for conducting application and security risk assessments, with a focus on Information Security and Privacy.
* Reviewed vendor security from a BCP/DR and Data Security perspective.
* Worked with the appropriate business users and technology owners to ensure that for any identified risks that require mitigating actions are plans, developed, and executed.
* Reviewed services provided by vendor and defined scope of assessment based on the Standard Information Gathering (SIG) questionnaire.
* Identified the top human risks to the organization and the behaviors that need to change to mitigate those risks.
* Assessed operational fitness of assigned third parties through due diligence reviews.
* Articulate writing skills to support development content and communicating information security principles at all levels from executives to non-technical employees.
* Reviewed and analyzed SOC 1, SOC 2 reports of third parties/vendors and other evidence provided during a risk assessment.
* Reviewing vendor contracts, onboarding, and monitoring vendors performances.
* Daily activities include performing vendor risk assessments, reviewing attestation documentation (e.g., SOC 2), and completing vendor/supplier security questionnaires.
* Coordinate audit activities with audit clients and interact with store support and management staff while maintaining departmental goals, policies, and initiatives.
* Assesses and reports on IT and information risk for key initiatives.
* Coordinated, supported, and maintained activities for Vendor Risk Assessment (VRA) Repository and related support tools.
* Work and assist vendor relationship managers and business partners to address and respond to risks in compliance with organizational risk policies and procedures.
* Provide recommendations to address control deficiencies and improve security posture of supplier providing services to the organization.

## KPMG, Nigeria

## Role: Audit Senior Associate. Apr 2010 – Dec 2012

## Responsibilities:

* Worked with different clients successfully to perform testing of Internal control over financial reporting.
* Planned and executed operational audits of various business areas using risk-based audit methodology.
* Performed risk assessments for application systems and other information technology audits
* Led and managed testing of controls and ensured controls were adequately designed (TOD) and working effectively (TOE) to mitigate information technology and security risks within agreed policies, procedures, standards, and risk limits.
* Performed thorough reviews of logical security and control features with emphasis placed on vulnerability to internal fraud and external computer hackers.
* Through the focused use of modern audit methodologies audited the adequacy of internal system/application controls, to assess the integrity of financial reporting, efficiency of operations, as well as compliance with approved policies and procedures.
* Assessed and reported on the effectiveness of systems development controls, change management procedures and network security administration.