DAVID OLABISI

(240)-273-6695 | davidolabisi133@gmail.com | linkedin.com/in/davidolabisi/

Senior Risk & Compliance Manager | CISM, CISA | Third-Party Risk • Data Privacy • Sanctions Investigations

Certified Information Security Manager (CISM) and seasoned risk leader with 8+ years of experience driving enterprise third-party risk, data privacy compliance, and technology risk programs in regulated environments. Proven success building third-party governance programs and leading complex compliance reviews, including vendor data privacy, AWS cloud controls, and regulatory investigations. Background in criminal justice with working knowledge of financial crime risk, sanctions-related screening, and cross-border compliance expectations (OFAC, EU, UN). Known for advising executives and legal partners on risk exposure and leading end-to-end audit and control processes.

SKILLS

Third-Party Risk Management • Data Privacy (CCPA/CPRA) • Cloud Governance (AWS) • Regulatory Compliance • Risk Control Self-Assessments (RCSA) • Issue Remediation • Audit Readiness • NIST 800-53 • RSA Archer • ServiceNow • SAS • Agile & Scrum • ISO Standards • Microsoft Excel (Pivot Tables & Automation) • Microsoft PowerPoint • Jira • Coupa • SharePoint

PROFESSIONAL EXPERIENCE

Sr Third Party Risk Analyst, Synchrony Financial (SYF), *Remote* **Sep 2022 – Present**

- Direct third-party data privacy and compliance programs across 500+ vendors, ensuring adherence to CPRA/CCPA, AWS controls, and enterprise risk frameworks.
- Led and mentor a team of 4 risk analysts responsible for third-party risk assessments, issue remediation, and regulatory reporting.
- Conducted high-impact security assessments for new and existing third-party vendors, with a focus on vendors handling PHI, PII, or financial data.
- Use HITRUST CSF-based controls and RSA Archer to review control maturity, identify deficiencies, and guide strategic risk mitigation planning.
- Lead drafting of third-party risk findings reports for executive consumption and align remediation timelines with internal risk appetite.
- Review vendor-provided artifacts, including SOC reports, information security policies, and penetration test summaries, to validate compliance posture.
- Contributed to quarterly reporting on third-party risk posture by summarizing trends, unresolved risks, and program improvements for leadership review and audit preparedness.
- Issued targeted security and compliance questionnaires to vendors, reviewing documentation such as SOC 1/2 Type II reports, PCI DSS attestations, ISO 27001 certifications, and internal policies to validate the effectiveness of controls.
- Evaluated administrative, physical, and technical controls against NIST 800-53, HITRUST, and internal frameworks, identifying security gaps and recommending action plans based on risk severity.

Third Party Risk Analyst, JP Morgan, *Remote* **Jan 2021 – Aug 2022**

- Oversaw onboarding and risk classification for high-risk third-party vendors; ensured compliance with global standards and internal controls.
- Led remediation tracking and resolution planning for third-party gaps, escalating unresolved issues to governance and legal teams.
- Maintain metrics for control effectiveness and support internal and external audit readiness efforts.
- Led full lifecycle third-party risk assessments across critical and high-risk vendors, using AACE and ProcessUnity to manage intake, workflow tracking, and assessment completion.
- Manage due diligence required for onboarding and recertification of risks and on-going monitoring of assigned third- party relationships.
- Perform continuous monitoring by assessing tools during onsite visits to validate the security questionnaires filled out by the vendors to ensure the protection of data at the vendor sites.

DAVID OLABISI

(240)-273-6695 | davidolabisi133@gmail.com | linkedin.com/in/davidolabisi/

Third-Party Risk Assessor, McLane Company, *North Carolina* **Jan 2019 – Dec 2020**

- Conducted detailed due diligence and on-site/virtual assessments of third-party vendors for operational, data, and cyber risks.
- Collaborated with internal stakeholders and vendors to address risk findings and validate control improvements.
- Supported vendor exit planning and offboarding strategies to reduce compliance and continuity risk.
- Mentored junior assessors by guiding them through assessment protocols, documentation reviews, and proper tool usage to maintain quality and compliance alignment across assessments.
- Maintained a live vendor risk register and tracked key performance indicators to ensure sustained compliance and escalate aging risks.
- Escalate issues of 3rd party vendor's non-compliance to the vendor risk management office (VMO).

IT Auditor, Nisus Technologies Corporation, *Maryland* **May 2017 – Dec 2018**

- Reviewed internal policies and procedures and existing laws, rules and regulations to determine applicable compliance and the adequacy of underlying internal controls.
- Conducted Sarbanes Oxley (SOX) testing in all the IT General Controls within the audit scope, to test their strength, effectiveness, and also weaknesses in their control environment.
- Documented control weaknesses related to testing exceptions and assisted in preparing draft audit reports to communicate findings and recommendations to senior management.
- Evaluated Change Management Control processes, Disaster Recovery Plans, and Business Continuity Plans.
- Assisted in IT management in identifying gaps between policy and process, developing recommendations to remediate control weaknesses and responsible for developing and maintaining IT control metrics related to compliance activities. Strong background in all stages of the auditing process, including planning, fieldwork/execution /risk assessment, reporting and follow up.

EDUCATION

Bachelor of Science, Criminal Justice

North Carolina Wesleyan University, Rocky Mount, NC

CERTIFICATIONS

Certified Information Systems Auditor (CISA), ISACA
Certified Information Security Manager (CISM), ISACA
Actively pursuing CISSP certification.