VICTOR TANDOH

Phone: (614-424-2594) | E-Mail: victortandoh2@gmail.com

PROFESSIONAL SUMMARY

Diligent Cybersecurity Professional with a robust vendor risk assessment and system administration background. Strong expertise in PCI-DSS, Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), National Institute of Standards and Technology (NIST), and Risk Management Framework (RMF) processes. I am Seasoned in assessing and managing risks in vendor and system environments. Skilled in conducting comprehensive system and vendor risk assessments, implementing risk mitigation strategies, and ensuring compliance with industry standards like PCI DSS; seeking a role where I can bridge the gap between technical systems and risk compliance, ensuring security and adherence to regulatory frameworks.

CYBER SECURITY TRAINING/SKILLS/STANDARDS/SOFTWARE

- **Compliance & Frameworks**: AICPA Standards, NIST Guidelines Publications, PCI DSS, ISO 27001, IT Security Compliance, NIST SP 800-53, SP 800-53A, SP 800-37, NIST SP 800-171, FIPS, FISMA, FedRAMP, Risk Management Framework (RMF), NISPOM.
- **Assessment & Authorization**: Certification and Accreditation (C&A), Assessment and Authorization (A&A), Vulnerability Assessment, Network Vulnerability Scanning, Information Assurance, System Risk Assessment, HIPAA & PRIVACY ACT training.
- **Tools & Software**: Nessus Vulnerability Scanner, ACAS, HBSS, SCAP, Splunk, SharePoint, Nexpose, Power BI, Archer.
- **Documentation & Procedures**: PTA, PIA, SSP, CP, SAR, POA&M, ATO, ISA, MOU/A, IDS, IPS.
- **Office Tools**: Microsoft Office.

PROFESSIONAL EXPERIENCE

Chipotle Mexican Grill
01/2023 - Present

Sr GRC Analyst

- Conduct a thorough review and assessment of the controls in place within the organization, focusing on the Service Organization Controls (SOC) framework established by the American Institute of Certified Public Accountants (AICPA).
- Stay current on developments and updates to AICPA standards and guidance related to SOC assessments and incorporate any changes into the assessment process.
- Participates in the development of security awareness training and phishing campaigns for whole organization. Collect the data for analysis and improve the security posture of the organization.
- Leads and coordinates audit-related tasks specifically for PCI-DSS 4.0 to ensure the readiness for audit testing with both internal personnel and external auditors. Contributes to the development of audit process improvements.
- Leads the roadmap and transition from PCI-DSS 3.2.1 to PCI-DSS 4.0, imbibing the changes and educating stakeholders.
- Stay up to date with industry trends and best practices, including monitoring for changes in PCI-DSS and recommending necessary adjustments to the compliance program.
- Conduct readiness assessments of service organization controls based on the SOC 2 framework.
- Assist with third-party vendor management programs utilizing tools like CyberGRX and BitSight.
- Performs risk assessments, audits and tests to ensure Chipotle systems and processes remain in compliance with applicable regulations, PCI-DSS, SOX and internal information security management policies, ensuring that required evidence is collected and maintained as required to meet compliance objectives.

Columbia Bank

05/2020 - 12/2023

IT Risk Manager-Third Party Vendor Risk Management

- Conduct readiness assessments of service organization controls based on the SOC 2 Framework.
- Spearheaded **vendor risk management**, ensuring thorough documentation of relationships and upload of related contracts for outsourced services.
- Conducted comprehensive **3rd Party Vendor Risk Assessments**; reported on vendor risk management activities, emphasizing the criticality of ensuring compliance and security.
- Delivered actionable recommendations for identified security exceptions and defined remediation strategies, emphasizing **PCI compliance**.
- Identified and addressed system vulnerabilities, recommending countermeasures and solutions for risk mitigation; played an active role in **vulnerability management, control mapping, gap analysis**, and remediation of findings from penetration tests.
- Regularly performed internal and focused risk assessments for existing and emerging technologies and services, ensuring the organization stays ahead of potential threats.
- Actively collaborated with cross-functional teams like IT, HR, contracts, and security to navigate potential compliance issues, ensuring adherence to **PCI, SOC2, and other regulatory requirements**.
- Contributed to **GRC reporting**; presented cyber assessment metrics to senior management, influencing strategic decisions on risk management.
- Cultivated and maintained robust working relationships with key stakeholders, ensuring consistent alignment on information risk management strategies across the organization.

NETWORK CENTER INC

05/2016 – 04/2020

Senior Security Assessor (IT Risk & Compliance)

- Led comprehensive security and privacy control assessments for IT processes, analyzing the overall effectiveness of controls including service organization controls, and identifying vulnerabilities across system components, applications, and databases.
- Participated in training and professional development activities to enhance knowledge and skills related to SOC readiness assessments.
- Drove vulnerability/risk assessment analyses to support Assessment & Authorization (A&A) activities, facilitating swift remediation and ensuring compliance.
- Orchestrated developing and implementing security solutions addressing weaknesses identified in the Requirement Traceable Matrix (RTM) and Security Assessment Report (SAR). Managed POA&M remediation and Corrective Action Plans (CAP).
- Conducted assessments on FedRAMP by analyzing customer responsibility documentation and controls provided by Cloud providers.
- Maintained comprehensive Security Authorization and Assessment packages, including System Security Plans (SSP), Contingency Plans (CP), SAR, and other vital security documents.
- Spearheaded risk assessments and recommended effective mitigating controls. Kept abreast of developments impacting assurance levels.
- Collaborated with the IT Controls Manager to enhance the efficiency and efficacy of IT audit testing procedures and processes.
- Deeply involved in the A&A process, offering security control assessor (SCA) services, including A&A scanning, documentation, threat analysis, and security system reporting.
- Demonstrated proficiency in NIST 800-53 security controls, ensuring thorough and timely documentation of assessment results.
- Strictly adhered to the NIST Risk Management Framework (RMF), supporting the A&A process and performing ongoing continuous monitoring in alignment with NIST 800-137 Rev 1.

- Conducted application controls testing focusing on data protection, logical access, data transmission, and contingency planning.
- Ensured organizational readiness and compliance concerning PCI, IT policy, and emerging regulatory requirements.

OHIO HEALTH **06/2013- 05/2016**

Third-Party Vendor Risk Manager

- Provided analysis and recommendations for identified security exceptions; participated in defining remediation efforts.
- Ensured all vendor relationships are documented and all contracts related to vendors that provide outsourced services are uploaded in the system.
- Performed 3rd Party Vendor Risk Assessments & assist in the reporting of vendor risk management activities.
- Ensured all vendors were classified and assessments completed by the VRM policy.
- Ensured all vendor relationships are documented in the VRM system and all contracts related to vendors that provide outsourced services are uploaded by the VRM policy.
- Managed the functionality of the VRM system which is VCI's central repository for vendor contracts and related documents and is the record of all vendor's due diligence and issue management.
- Influenced, and provided leadership and guidance to the business, Legal, Compliance, Purchasing, and other stakeholders to ensure requirements of VRM are fully understood.
- Worked with the Legal, Compliance, Information Risk Management, Purchasing, and Internal Audit to ensure consideration of third-party risk within their risk domain framework.
- Monitored compliance with VRM Policy and General Procedures
- Maintained detailed VRM Policies and Procedures
- Provided senior leadership reporting of the "Risk Based" vendor evaluation, identifying all areas of material risk and the potential source of the identified risk.
- Provided to senior leadership reporting that covers all vendors which provide "Core Process" to the organization, identifying those vendors and/or processes which represent the greatest threat of risk to the organization.
- Develop and provide reporting of all unresolved conflicts, misunderstandings, and differences in contractual interruptions, as well as the planned course for resolution, including the source of dispute; the parties involved, anticipated timelines, measurable milestones, and expected resolution date.

SKILLS & QUALITIES

Good interpersonal communication skills, Results-oriented, Initiative and Creativity, Fast Learner, Ability to adapt, Critical Thinking, integrity, multi-tasking, strong organizational skills, Strong attention to detail, Team builder and player.

EDUCATION

- Kwame Nkrumah University of Science and Technology August 2005 - May 2009
- Bachelor of Science, Computer Science

CERTIFICATIONS

- CISM – Certified Information System Manager
- CompTIA Security +