RITA ASHTON

240-921-7174 | neyahru@gmail.com |

Information Technology professional with 8 plus years of progressive technical and Knowledgeable IT security professional with years of experience designing and implementing security plans and initiatives. Experienced in Risk Management Framework, Systems Development Life Cycle (SDLC), Audits and Compliance, Security Life Cycle, Risk assessment, vendor risk management, data privacy, audit and Vulnerabilities Management, cloud compliance and applicable standards. Organized, Solutions and deadline-focused with in-depth knowledge and understanding of numerous frameworks and regulations. Specialized in providing IT security expertise and guidance in support of security assessments and continues monitoring and contract reviews, NIST CFS, HIPAA, HITRUST, PCI-DSS, Incident and Contingency Planning. Job-oriented with excellent attention to detail, team player, excellent ability to lead and work with diverse populations, dependable, multi-tasking, and time management proficient to accomplish tasks. Equally, motivated, and always seeking challenges for improvement, problem-solving, and career enhancement.

SKILLS/TOOLS

Assessments & Compliance: SOC 2 - Type 1 & 2 Reports, PCI-DSS, GRC, CAIQ, SSAE 18, SIG, HITRUST, HIPAA, ISO 27001/2, NIST 800 series, ITGC, Vendor/Supplier Security Audit, FIPS 199, ITCG, FISMA, ITIL.
IT Program Directorship & Management: Cybersecurity Technical Writing (Policies, Standards, and Procedures), Third-Party Risk Management, Business Continuity & Disaster Recovery (BC/DR), SDLC Security Controls, Policies and Procedures, Implementation, Incident Response, Supplier Risk Assessment and Risk Mitigation Analysis, Access Control Management, Contingency Plan, Policy Review, Continuous Monitoring, Artifacts gathering, Remediation, SSP, SCRM,SAR, SAP, CMP.
IT Security Tools: RSA Archer, Vanta, One Trust, Knowbe4,
Productivity Tools: Microsoft 365, ServiceNow, Jira /Confluence, SharePoint, Slack, Teams, Google Docs, MS Teams, BOX.
Soft Skills: Teamwork, Problem Solving, Interpersonal Communication, Conflict resolution.

CERTIFICATIONS

Certified Information System Auditor (CISA)

Certified Risk Information Security Control (CRISC)

Certified CompTIA Security

Certified Information System Security Professional (CISSP)- In-View

PROFESSIONAL EXPERIENCE

GRC Consultant
|US Tech Solutions | **November 2020 - Present**
City/State

- Oversee comprehensive compliance programs (NIST-853, SOC 2, HITRUST, HIPAA, PCI), conducting detailed assessments and continuous testing.
- execute and perform lead audit function during internal audit to ensure compliance with applicable regulations and international laws and standard, standards, guidelines and procedures implement, manage and track effectiveness of corrective action plans and provide management with regular updates.
- Using GRC tools like Practical Threat Analysis (PTA) and The GRC Stack, which aims at synchronizing information and activity across governance, risk management and compliance to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps. Perform Scanning: Run port Scanning using tools like Nmap to obtain the list of open/active ports and services; and Vulnerability Scanning using tools like Nessus to identify weaknesses in the software and review Security Audit Logs: using SIEM tools like Splunk to verify that the Access Control.
- Responsible for reviewing and assessing supplier evidence as related to the information security aspect like SIG, SOC 1 and 2 reports, Visa and Mastered certified, compliance certified.
- key performance indicators (KPIs) and key risk indicators (KRIs) to measure and monitor program performance for the program strategy and supporting initiatives. Manages third party vendor management programs by defining security controls based on tiers of vendors, performing risk assessments for new and existing vendors, and partnering with legal to review contracts for new and existing vendors. Delivers and manages a security awareness & education program and monitors and measures compliance and performance
- Review Information Security Audit reports such as SOC 1 or SOC 2 Reports & SIG questionnaire to make sure it complies with company's control standards.
- Analyze the information to identify information security weaknesses or non-compliance with industry standards such as NIST CSF. PCI-DSS, ISO 27001, NYDFS, etc.
- Ensure all vendor relationships are documented in the VRM system and all contracts related to vendors that provide outsourced services are uploaded in the system in accordance with the VRM policy.
- Manage the functionality of the VRM system which is the central repository for vendor contracts and related documents and is the record of all vendors due diligence and issue management and remediation.
- Work with the Legal, Compliance, Information Risk Management, Purchasing, and Internal Audit to ensure consideration of Third-party risk within their own risk domain framework.
- Ensure all vendors are classified and assessments completed in accordance with the VRM policy.
- Coordinate with stakeholders to initiate scope and plan controls assessments of new and existing vendor engagements.
- Responsible for analyzing all new vendor contracts and pointing out areas of improvement to management.

- Assess completed questionnaire and supporting documentation to validate vendor appropriate implementation of information security controls.
- Communicate vendor information security issues to stakeholders, ensuring their understanding of associated risks and actions needed to remediate those risks.
- Validate evidence from vendors before remediation plans are closed.
- Responsible for managing and reviewing the employee entitlement access to internal systems of the company.
- Support the VRM Program to effectively manage vendor risk in accordance with internal policy and regulatory requirements, ensuring strong oversight of all vendor risks and provide visibility of existing and emerging risks.
- Perform weekly user access reviews to identify and mitigate risks from inactive and unsecured accounts, focusing on accounts approaching 60 days of inactivity without MFA enabled.

Vendor Risk Analyst
| Signify Health | **January 2016 – October 2020**
City/State

- Conducted comprehensive vendor risk assessments evaluating security, financial stability, operational practices, regulatory compliance, and ethical standards.
- Review Information Security Audit reports such as SOC 1 or SOC 2 Reports & SIG questionnaire to make sure it complies with company's control standards.
- Analyze the information to identify information security weaknesses or non-compliance with industry standards such as NIST CSF. PCI-DSS, ISO 27001, NYDFS, etc.
- Ensure all vendor relationships are documented in the VRM system, and all contracts related to vendors that provide outsourced services are uploaded in the system in accordance with the VRM policy.
- Manage the functionality of the VRM system which is the central repository for vendor contracts and related documents and is the record of all vendors due diligence and issue management and remediation.
- Work with the Legal, Compliance, Information Risk Management, Purchasing, and Internal Audit to ensure consideration of Third-party risk within their own risk domain framework.
- Ensure all vendors are classified and assessments completed in accordance with the VRM policy.
- Coordinate with stakeholders to initiate scope and plan controls assessments of new and existing vendor engagements.
- Responsible for analyzing all new vendor contracts and pointing out areas of improvement to management.
- Assess completed questionnaire and supporting documentation to validate vendor appropriate implementation of information security controls.
- Communicate vendor information security issues to stakeholders, ensuring their understanding of associated risks and actions needed to remediate those risks.
- Validate evidence from vendors before remediation plans are closed.
- Responsible for managing and reviewing the employee entitlement access to internal systems of the company.
- Support the VRM Program to effectively manage vendor risk in accordance with internal policy and regulatory requirements, ensuring strong oversight of all vendor risks and provide visibility of existing and emerging risks.

IT Compliance Analyst
| Deloitte | **July 2014– December 2016**
City/State

- Led evidence collection efforts for annual NIST-853 assessments, ensuring alignment with all control requirements.
- Conduct thorough due diligence reviews on third party services providers.
- Identify and assess risk associated with third party relationships.
- Lay down a road map for obtaining compliance by developing a statistical graph of the various department that will be involved within the scope of the audit.
- Communicate identified risks to key stakeholders to initiate and drive risk remediation.
- Perform network vulnerability scans and security assessment.
- Ensure information security compliance with eternal federal regulations.
- Issue the final report to senior leaders and board of trustees, finance, infrastructure, or audit committee.
- Perform onsite security assessments on third party service providers.
- Provide secure design consulting services on application development projects
- Act as a facilitator between IT and internal or external audit teams.
- Identify the framework of certification program the organization will follow if not yet available. Recommend based on the business conducted by the organization.
- Ensure that all controls required to be implemented are identified from specific framework such as IS27001/NIST CSF and privacy regulations like GDPR/HIPAA/CCPA
- Coordinate with stakeholders to initiate scope and plan controls assessments of new and existing vendor engagements.
- Responsible for analyzing all new vendor contracts and pointing out areas of improvement to management.
- Assess completed questionnaire and supporting documentation to validate vendor appropriate implementation of information security controls.
- Communicate vendor information security issues to stakeholders, ensuring their understanding of associated risks and actions needed to remediate those risks.
- Validate evidence from vendors before remediation plans are closed.
- Responsible for managing and reviewing the employee entitlement access to internal systems of the company.

EDUCATION

BACHELOR OF SCIENCE: Computer Science
University of Buea, Cameroon

Master of Science in Cybersecurity-In-View
WGU