**SCHNEIDER FONCHAM**

IT Risk/Compliance/Audit Analyst

Email:Schneiderfoncham@gmail.com.

Tell: 202-913-5362

Enthusiastic with excellent skills in organizational, IT Audit, Risk and compliance professional with 8 years plus of experience directing complex projects, developing strategies and leading teams to further the enhancement of overall regulatory compliant operations. A motivational leader who can easily work in and navigate and environment committed to personal development and with the ability to learn quickly and multi-faceted operational division. Experience knowledge in implementing controls, policies, procedure, processes, Vendor management, Risk assessment and IT assessment focusing on the improvement of business operation, regulatory affairs, compliance and information security, risk management, strategic planning, Privacy and Data Protection. Penetration testing, Security Management & Operations, Vulnerability Scanning, NIST Family of Security Controls, Jira, Confluence, HIPAA, HITRUST, PCI DSS, Incident and Contingency Planning, and health information security technologies. Complete all projects on time with the highest level of scrutiny and attention to detail to ensure results exceed expectations. Strong Communication skills with experience working in a team environment, able to collaborate with individuals from diverse backgrounds in maintaining CIA.

**SPECIAL SKILLS AND TRAINING**

Microsoft Suit, Analytical skills, Documentation

Due diligence, SOC 1, 2 Audit, SIG Questionnaire,

Vendor Risk/ Third Party Security Risk Management

ISO 27000 / PCI DSS / HIPAA / NIST / FISMA / HITRUST / NYDFS

Plan of Action and Milestones (POA&M), Corrective Plan of action

Risk Assessment, Vulnerability Management , Archer eGRC Platform or any other Similar Platform, IT Audit, Privacy, / JIRA/ GDPR/CCPNA/AWS/CLOUD SERVICES/Splunk, New-York Financial Regulation/ Share point site, Experience in Application controls and risk assessments

**PROFESSIONAL EXPEREINCE**

**Risk/Audit/Compliance Analyst** July 2019 - Present

*BANK OF AMERICA (WTS).*

* Responsible for analyzing all new vendor contracts and pointing out areas of improvement to management. Develop, Implement, and maintain policies, procedures, standards, and guidelines per applicable regulations including NIST 800-171 Framework Controls, ISO 27001, GDPR, CCPA PCI DSS, and HIPAA
* 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. PCI-DSS, ISO 27001, NYDFS, etc.
* Acts as a liaison during organization internal and external audit Conducted reviews of security documents updated by the ISSO to ensure FISMA compliance, reviewing and validating of items uploaded into the POA&M tracking tool in support of remediated findings and work on mapping the SIG and control standards to the VRA Questionnaire
* Prior experience working with Data Management applications, Statistical Data Analysis systems, Clinical Data Entry applications, Electronic data capture systems. Familiarity with regulated systems (GxP, CFR 21 Part 11) and systems validation; Life Sciences, Biotech or pharmaceutical industry experience preferred Comfortable with project methodologies, and familiarity with tools including MS Project and Excel
* 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 vendor 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.
* Advise clients on software configuration recommendations, complete configurations, and lead the configuration efforts with staff completing the configurations Training the client team on their new software usage based on custom configurations completed and Take the lead in defining issues and ideas to be studied as well as the approach (methodological and technical) to be used in addressing studies and projects. Creates and/or develop new methods of analysis, database design and performance measurement or, in some cases, adaptation of existing solutions to new areas.
* Ensure all vendors are classified and assessments completed in accordance with the VRM policy.
* Familiar with sig tools such as JIRA, Splunk, and Bit sight,maintain effective communication with vendor relationship manager during continuous monitoring of vendors qualify application responses by facilitating meetings with business owners and third- party contacts. Assessed Vendor risk profile to determine the C.I.A rating, conduct assessment of vendors and prepare VRA Report.
* 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.
* 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 in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps.
* 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.
* Reviewed and update POA&Ms, security vulnerabilities and mitigation strategies; and develop security A&A artifacts, to include but not limited to, sensitivity assessments, SSP, and SAR. Stays current with regulatory knowledge and makes appropriate changes to the audit function in order to maintain compliance.
* 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.
* Experience and experience with cloud data security (FISMA/FedRAMP compliance) and working with public cloud solutions. Comfortable with IaaS, PaaS and SaaS Researched and Reviewed Vulnerability reports with Developers, System Admins, and Engineers to remediate Vulnerabilities identified from scans and create a risk register and risk treatment plan to track the remediation process per classification (Critical, High, Medium, and low)
* Reviewed vendor compliance from a BCP/DR and Data Security perspective. Responsible for conducting vendor risk assessments, with a focus on Information Security and Privacy. Conducts regular audits for all credit branches/departments to ensure compliance with regulatory requirements, policies, and operational procedures.

**Risk Analyst** Sept 2017 – July 2019

*Ebay (Remote)*

* Act as remediation analyst with vendors in remediating findings discovered during or after assessments.
* Making sure that vendors are following regulatory requirements and information security policy, applicable procedures, processes, and standards.
* Supports Third Party onboarding, ongoing monitoring, and Third Party off-boarding.
* Answering any internal stakeholder questions related to ongoing assessments.
* Create and institute policies and procedures to conduct Vendor Risk Assessments (VRA).
* Worked with the project leadership and technical team to develop strategies and plans to enforce security requirements and address identified risks.
* Ensured all identified gaps and results are documented.
* Ensured adherence to all federal, state and local laws regulations including but not limited to the FISMA, HIPAA and other compliance framework.
* Assisted in designing and implementing risk mitigation strategy to foster organization cyber resilience.
* Translated security vulnerabilities, assessed risks, developed mitigation plans, tracked and documented any accepted residual risks.
* Gather evidence for internal control assessment and also for ISO 27001 Audit.

**IT Compliance Analyst** July 2015 – August 2017

*Computer Information System Health Care*

*Maryland*

* Responsible for conducting vendor risk assessments, with a focus on Information Security and Privacy.
* Reviewed vendor compliance 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.

**Junior Security Analyst** Dec 2014 – July 2015

*AT&T*

* Assisted in the development, implementation and maintenance of policies, procedures, standards, and guidelines in accordance with applicable regulations including NIST 800-53 Framework Controls and HIPAA.
* Carried out HIPAA Risk Assessment on Third Party Vendors and identified gaps on these assessments.
* 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.
* Assisted the CISO with any ancillary projects needed, including creation of Visio workflows, document review and legal research.

**EDUCATION**

* Bachelor’s Degree in computer science - University of Buea – 2014

**CERTIFICATIONS**

* CompTIA Security+ Certified
* Certify Information System Auditor (CISA) Certified
* Certified Information Systems Security Professional (CISSP) in progress