Job Seeker Houston, TX Work Experience DELOITTE - Houston, TX March 2019 to Present Contract) (Third party cyber risk assessment) Review and validates all controls of vendor to ensure data confidentiality. Validate security questionnaires during findings review to ensure up to date data protection on vendor. Provides risk management support for a line of business or staff agency in key risk identification, measurement and aggregation, Perform validation testing activities on third-party management processes and controls to confirm adherence with policies, procedures, regulatory requirements/guidance, and industry best practices Perform validation testing activities on third-party management processes and controls to confirm adherence with policies, procedures, regulatory requirements/guidance, and industry best practices. Assess remediation plans and non-compliance acceptances across multiple business lines where Information Security standards compliance cannot be achieved. Participate in planning and strategy discussions around program development and management priorities including generating ideas, identifying trends and developing recommendations to shape strategy and objectives. Third Party Information Security Risk Analyst USAA - San Antonio, TX September 2018 to March 2019 Contract) Plan and execute security risk assessments for all third-party vendors/suppliers Work with our Vendor oversight to ensure adequate tier-in of our vendors based on the level of data they have access towards. Design and constantly upgrading supplier's questionnaires to ensure all areas of new threat signatures discovered are covered. Administer questionnaires to all vendors. Conduct onsite and virtual risk assessment to continuously determine the security posture at the vendor sites. Review and validates all controls at the vendor site to ensure data confidentiality. Validate security questionnaires during onsite visits, to ensure up to date data protection on vendor site. Conduct on-site risk assessments based on agreed upon procedures guidelines. Review the physical and logical access control managements on the vendor site in other to ensure data entrusted with them as well protected. Perform data loss prevention analysis of applicable data held at vendor site. Review all essential security policies and procedures documentation. Provide detail reports of the assessment to business owners and the Vendor Management office. Manage communication with vendors to ensure risk discovered are remediated within reasonable time. Escalate issues of 3rd party vendor's non-compliance to the vendor risk management office (VMO). IT Auditor KPMG - Houston, TX July 2018 to August 2018 Performed detailed walkthrough reviews, identified, mapped and documented infrastructure and applications risks and controls through process narratives, flowcharts for various applications within the firm. Assessed ITGC, application controls, as per COSO/COBIT risk management framework. Conducted detailed review and testing of general computer controls, change control process, access control lists, Segregation of Duties template, BCP/DR procedures including incident response procedure. Reporting of control deficiencies with management responses and with external auditors and stakeholders SCI. HOUSTON, TEXAS Third Party Risk Assessor October 2017 to June 2018 Coordinate with stakeholders to initiate, scope and plan Vendor Security Risk Assessments of new and existing vendors. Perform Information Security remote assessments, and onsite when required. Standardized, improved and automated the process by adding new communication templates. Assigned standard security questionnaire (SIG) based on SharedAssessments.org to vendors. Coordinated with the vendor to provide all required documentation based on their Tier rankings, to revalidate vendor appropriate implementation of information security controls. Analyzed the information to identify information security weaknesses or non-compliance issues with industry standards. Generated Assessment Report at the end of each assessment process, showing gaps and findings identified. Communicate those gaps and findings to stakeholders, and Business Relation Manager. Escalate issues associated with vendors as needed to management. IT Auditor FRAC SHACK AMERICA - Denver, CO June 2015 to August 2017 Performed audit with IT general controls such as, access control, change management, IT operations, disaster recovery and platform reviews (Windows and UNIX OS). Performs internal and external IT risk assessments; conducted gap analysis against industry standards and provided recommendations on mitigation options. Participated in integrated audits for evaluating network related issues; identifies IT related risks assessments and updated various risk and controls files to ensure firm wide identified risks were adequately addressed by control activities. Evaluate segregation of duties over application security involving the company's ERP systems (Oracle Financials) and execute audit strategy. Knowledge of Control Objectives for information and related Technology (COBIT) framework developed by the information Systems Audit Control Association (ISACA). Communicates with the company's external auditors on general computer control related matters and SOX test procedures. Information gathered is reviewed and analyzed extensively, and then compiled into a written summary report. IT Compliance Analyst ACCESS BANK - LAGOS, NG August 2012 to January 2015 Coordinated operational controls effectiveness testing across the IT division and with teams outside of the IT division as required. Provided intake, review, oversight, and tracking in support of internal audit functions. Supported the remediation of results from IT Security reviews and tests. Supported a yearly cycle of policy and procedure reviews to ensure process currency. Ensured that IT quality and risk metrics are collected and compiled. Ensured that the Group Risk Management Framework, policies and procedures are adhered to by the IT division. Supported the development and execution of an annual schedule of application risk assessments, control objectives, and IT "risk theme" assessments including track mitigating actions and communicate results. Continually review and mature the key risk indicators being monitored by the IT divisions. Education BS in Finance University of Lagos - Lagos, NG 2009 Skills Security, Cobit, Disaster recovery, Hipaa, Itil, Nist, Pci, Sox, Access control, Authentication, Rsa, Iso27001, Oracle, Sap, Ms office, Risk management, Audit, Internal audit, Vulnerability assessment, Soc Additional Information TECHNICAL KNOWLEDGE: ITGCs, Management Directives - Policies, Standard and Procedures, Internal Audit, SOX, Disaster Recovery, SOC 1 and 2 Review, COBIT, OCC, HIPAA, PCI DSS, NIST RMF, NIST CSF, ITIL, ISO27001, OCTAVE- Allegro, TPRM, Authentication and Access Control, Vulnerability Assessment, System Monitoring & Regulatory Compliance, Risk Management and Segregation of Duty. TOOLS: Teammate, ARAVO, ACL, RSA archer, Aravo TPRM, ServiceNow, SAP, Oracle, AWS Security, MS Office.

Name: Robert Thomas

Email: fisherkevin@example.com

Phone: 990-547-4880x92348