Cyber Security Strategy, GRC, ESR RISK AND COMPLIANCE Cyber Security Strategy, GRC, ESR RISK AND COMPLIANCE Cyber Security Professional with extensive experience in all aspects of Cloud Security and Compliance, Cyber Security Strategy, Governance Risk and compliance, IT and Cyber Security Audit, Enterprise Cyber Security Risk Management, Regulatory Compliance, Change Management. Possess strong analytical skills to solve problems quickly and add value to stakeholder relationships, both internal and external to an organization Atlanta, GA Work Experience Cyber Security Strategy, GRC, ESR RISK AND COMPLIANCE SunTrust Bank - Atlanta, GA February 2019 to Present Serve as a technical subject matter (SME) on cyber security/systems security matters Develop and implement Cyber program, and information systems security Policy, Standards and Procedure/and guidelines per the respective department and federal requirements interpret and implement security policies requirements to ensure confidentiality, integrity, availability of information, systems, and network Perform compliance reviews of policies, procedures, and assessment reports to ensure compliance. Develop recommendations for remediating risk and compliance gaps Evaluate information security risk in for business environment controls and industry requirements ((NIST, FFIEC, SWIFT, CIS etc.) Experience in Risk Assessment, audit, and IT security assessments for the purpose of developing policies and procedures as needed Senior Cybersecurity Analyst SunTrust Bank - Atlanta, GA January 2017 to February 2019 Conducted self - Annual Assessment (NIST SP 800-53A): Performed IT risk assessment to identify system threats, vulnerabilities, and risks. Developed risk assessment reports; identifying threats, and vulnerabilities applicable to the system Performed Vulnerability Assessment making sure risks are assessed, evaluated and a proper action taken to limit their impact on the information systems Performed patch management as part of remediation process, and applied required security patches within NIST and enterprise guidelines Evaluated the likelihood that vulnerabilities would be exploited and assess the impact associated with this threat and vulnerabilities Conducted Security Control Assessment to assess the adequacy of management, operational, privacy and technical security controls implemented Prepared recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process Assisted in the development of an Information security continuous monitoring strategy. Helped maintaining an ongoing awareness of information security IT Auditor, Risk & Assurance Habif, Arogeti & Wynns LLP August 2014 to December 2016 Performed IT SOX compliance audits for public and private entities as well as SOC 1 Type 2 reviews using COBIT and COSO frameworks Audit SME for PCI security compliance, HIPAA testing for regulated entities, DLP, and SSAE 16 SOC1 technology controls Participated in the planning and execution of risk-based audits such as patch and vulnerability management Participated in patch management and vulnerability remediation process. Such gap analysis, and track deficiencies and review for systemic risk Conducted complex security related assessment and assisted with evaluation of compliance with cybersecurity regulations (SWIFT, NYDFS, etc.) Assessed scope of security issues and developed best practice approaches to remediation or mitigate and provide quality assurance to ensure risks are scoped and assessed appropriately Analyzed threat and vulnerability and recommend security controls and/or corrective actions for mitigating technical and business risk Performed cyber security risks assessment through remediation & recovery and audit risk assessments leveraging continuous monitoring to assess IT inherent and residual risks Associate Security Engineer Elevated Computing - Dallas, TX January 2013 to April 2014 Developed knowledge of Active Directory structures Managed and troubleshoot all Active Directory certificates services, events and errors Performed access provisioning: IAM, Privileged User Management, Public Key Infrastructure and Certificate management. Responsible for maintenance and patching of the identity and access management tool Provided assistance with application and network Access Control, implemented IDS/IPS Solutions and Authentication solutions Implemented technical security controls and technologies (e.g. DLP, IDS, IPS and Application Firewalls, Antivirus and Anti-malware Experienced with security Information and Event Management (SIEM, experience configuring, deploying, and maintaining Splunk IT Analyst Hospital Data August 2009 to December 2012 Participated in the Information Security strategy, technology control process strategy, security compliance, DLP, and internal ITGCs Worked closely with the IT organization as a SME for the protection of client health information and PII to ensure adherence to policies, procedures, and legal/regulatory requirements

Initiated, facilitated, and promoted activities to raise Information Security awareness within the organization   Collected and examined records as a part of IT compliance testing strategies to compile evidence of compliance with IT operations standards Education MSc in Information Technology University of Texas - Dallas, TX 2016 BSc in Statistics Obafemi Awolowo University 2010 Skills Network Security, COBIT, Web Applications ,IT Management, IT Audit, Information Security, Risk Management, Risk Assessment, Software Development Life Cycle (SDLC), Agile Project Management, Payment Card Industry Data Security Standard (PCI DSS), Cybersecurity, Enterprise Risk Management, Solution Architecture, Incident Management, Disaster Recovery, Identity & Access Management (IAM), ISO Standards, Cloud Computing, Penetration Testing. (7 years)

Name: Morgan Russell

Email: farmstrong@example.org

Phone: (758)691-0322x04359