IT Security/ IT Compliance IT Security/ IT Compliance IT Security and Compliance North Dallas, TX A highly motivated, result driven, team oriented and resourceful internal I.T/ I.S Audit subject matter expert. Equipped with strong industry methodological, analytical, problem solving and communication skills. Seeking to deploy my wealth of unique interpersonal and organizational skills, knowledge and industry standard expertise towards the attainment of an Organization and Client's IT success and business objectives. Work Experience IT Security/ IT Compliance Kubota Tractor Corporation November 2018 to Present the development and maintenance of privacy and security policies Design, facilitate and support adherence to administrative security processes Support internal privacy assessment, data mapping, and other privacy programmatic tasks Support privacy and security practices as they relate to 3rd party data sharing and contractual requirements Provide ongoing privacy and security awareness training, Add/ remove users Appropriately to wombat (Security Awareness application) Participate in projects as the privacy subject matter expert Performs ongoing monitoring of the information and usage landscape of the company Understands U.S. privacy and security regulations Lead projects using privacy and security frameworks such as GAPP, ISO 27001, NIST, COBIT as framework to implement IT controls. Support Security team making sure well implemented role-based access and segregation of duties is followed Support 3rd party risk assessments and privacy compliance Participate with incident response and business continuity planning / disaster recovery planning Coordinated in identifying great GRC / Data privacy tool for the company using cost effective approach Responsible for identifying technical security vulnerabilities by conducting application analysis, network analysis, and -scanning; reporting security vulnerabilities and the risks those vulnerabilities present to Vice Presidents, Managers, and other technical individuals Responsible for recommending mitigating solutions to remediate risk associated with vulnerabilities maintaining knowledge of cybersecurity trends and changing technologies, and providing recommendations for adaptation of new technologies for - vulnerability -monitoring; providing management with vulnerability assessments and security briefings to advise them of critical and high risk vulnerabilities that may affect customer, or corporate security objectives. IT Security Auditor III Securus Technologies, Inc August 2017 to

October 2018 Establish and manage compliance programs across the Company (PCI-DSS, FedRAMP, FISMA, SOC II Type II, HIPAA, etc.) Provide SME-level advisory services to IT and the business as it relates to regulatory and industry compliance issues Manages, coordinates and executes internal compliance testing, documentation and follow-up Negotiates with internal departments and external business partners/vendors/consultants regarding audit findings; authors all management responses for both internal and external assessments Manages relationships with key regulatory and industry assessment vendors Works alongside policy and standards team to incorporate changes into the enterprise policy document based on compliance assessment results Leads root cause and remediation activities for remediation activities and related information security issues Assist the IT Audit and Compliance Manager in the maintenance of a comprehensive risk assessment model Plan and perform and document audits in accordance with the Institute of Internal Auditing's Standards for the Professional Practice of Internal Auditing, generally accepted auditing standards, and with departmental policies and procedures. Recommend and explore alternative courses of action for correcting control weaknesses, resolving operating problems or improving performance. Maintain relationships with key personnel responsible for the designated audit units. Stay abreast of organizational structure, policies and procedures within the designated audit units Perform special assignments, studies and special projects assigned by the IT Audit and Compliance Manager IT Security & Controls Analyst XTO Energy Inc., a subsidiary of EXXON Mobil - Fort Worth, TX October 2016 to July 2017 Controls compliance monitoring /reporting out overdue tasks, monitoring risk assessment review due dates / scheduling follow-on review meetings, organizing various controls evidence as part of Audit readiness/UIA field work, etc., stewarding Security Controls metrics, Managed clear strategies to protect information, business and IT assets. Providing increased intelligence to executives, enabling them to understand, prioritize, mitigate, & manage risk. Managed Security Controls SharePoint sites / document repositories (audit, Unit Internal Assessment testing, controls remediation, etc.) Coordinated efforts & communications with the Business/ Application owners during Audits and Unit Internal Assessments, conducting access reviews and advising on remediation of Audit/Unit Internal

Assessment findings. Involved with revising risk assessments & controls catalogues, and monitoring for compliance, including oversight of various documentation associated with UIs, Audits and all-related IT memos. Worked with IT Application owners/ Business Custodians to complete full risk assessments on all in house IT developed applications, through deploying Risk Assessment questionnaires to identify areas of potential threat, mitigating with fully implemented controls. Involved in identifying appropriate owner/ custodian for IT Applications within organization, Initiates change of owner and custodian process as needed. Managed numerous IT Audit Engagements from risk assessment through audit plan development to execution and remediation coordination. Prepare specs for new infrastructure and VMware servers, disk storage, and network switches, routers, firewalls, and VPN's Evaluated existing system security and made recommendations for the mitigation of IT-related business risks. Assisting in defining the scope of the organization's cardholder environment. Assisting in defining the scope of the organization's cardholder environment. Performing network scans for merchants who process via the internet to check for vulnerabilities that could possible compromise their cardholder environment. Assessing an organization's compliance with the PCI DSS by evaluating how the merchant organization handles and protects the cardholders' information. Assisted in pre-implementation reviews of new application systems considered for purchase or in-house development IT Compliance and Security Professional ATOS/Xerox - Lewisville, TX November 2015 to October 2016 Interpreted systems specifications to develop, maintain and support automated business processes. Introduced Agile Scrum methodology to software system development life cycle, understanding of SDLC. In depth knowledge and expertise in SOC 1 type I, II, III, PCI, Sarbanes Oxley, ISO 20000, and/or ISO 270001 audit requirements Managed SSAE 16 SOC2 implementation Defined Controls and Report requirements Design roles and groups for users and resources using AWS Identity Access Management (IAM). Provided policies to groups using policy generator and set different permissions based on the requirements. Involved in development, user acceptance, and performance testing, production & disaster recovery server. Coordinated the Audit Requests gathering and Observed audit walk through; Worked with support teams for evidence gathering

Made recommendations to mitigate identified IT controls issues/risk Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk. Create and maintain a risk register to ensure that all identified risk factors are accounted for. Responsible for the Overall Coordination and Management of the Data Center and Client audits, Central point of contact and Liaison between the Audit Firm and Support Teams. Participated in meetings with external audit and Public Accounting firms Made recommendations to mitigate possible IT controls issues Updates policies and procedures as needed or required within Information Technology space. Provides IT audit and compliance expertise to the Company through facilitating roundtable discussions with IT department, Controller group (SOX), External Audit Partner, and Senior Management. Assisted external auditors to facilitate compliance with Sarbanes Oxley and other external control requirements Assist in the preparation and periodic review of a comprehensive Company risk assessment. Dallas, TX, IT Audit Consultant IP Connect Consulting - Mansfield, TX November 2014 to October 2015 Conducted full review of the organization's Disaster Recovery readiness - Business Impact Analysis (BIA), DR plan, Call Tree and annual test, Warm, Hot or Cold site adequacy, critical processes and application listing and ranking etc. Review SSAE 16 SOC I, II, and III standard allows for management's monitoring activities to provide evidence regarding the design and operating effectiveness of controls. Developed risk-based IT Audit program and conducted system and application audit evaluation based on COBIT or COSO standard; ISO 27001; NIST; GLBA standard; GRC; SOX For critical business applications and systems (ERP, Web applications, Firewall, Network, Operating Systems, Remote access connectivity devices etc.), reviewed the adequacy of critical controls such as Logical Access control, Audit log events, Data integrity/ security, Segregation of duties, Incident, Problem and Change control, Incident management, Release management, ITGC etc. to mitigate any potential risk; Communicated and interacted with all levels of management on audit issues and managed audit engagements from entrance through closing conferences. Responsible for identifying control weaknesses and assist in remediation Reviewed systems for adequate management controls, efficiency, and compliance with policies. Made recommendations when

necessary. Conduct internal audits and track findings through close Ensure audit tasks are completed accurately and within timeframes PCI Compliance Auditor Super Pro Processing Corp - Irving, TX January 2014 to November 2014 Knowledge of end to end processing, transmission and storage of credit card information in adherence to PCI DSS standards; Ensure the customer's privacy is always maintained by protecting the PAN information in the custody of the Organization, as well as conduct privacy compliance reviews; Conducts detailed review of all 12 PCI DSS control elements covering wired and wireless Networks, Security policies and procedures, Firewall, Access Controls, Security Awareness Programs, Vulnerability analysis, Penetration testing and SOD amongst others; Through data analysis and interview with information technology and business units, identified all PCI/PII related applications and systems that processes, transmits and stores credit/ debit card and PII information; Through data gathering and analysis, conduct a revalidation of the organization's compliance level as defined by the credit card issuing organization guidelines (VISA, Master card etc.). Conduct detail review of all the PCI controls elements covering wired and wireless networks, security policies and procedures, Firewall, Access control, vulnerability analysis, penetration testing, segregation of duties control amongst others Participate in information technology team project as needed to address information technology security requirements (PCI/SOX) for new or upgraded hardware and applications Partner with IT Security/ Database/ IT Network and so on, to define appropriate compensatory controls for PCI compliance IT Controls and Compliance Auditor Emzol Pharmaceutical Limited - Atlanta, GA January 2013 to December 2013 Identified and evaluated complex business and technology risks, internal controls which mitigate risks, and the identification of related opportunities for internal control improvement; Conducted Access Review - ensure that industry standard "strong password algorithm" is being deployed on network and business application. Ensure access privileges and permissions are on a need-to-know basis. Developed risk-based IT Audit program and conducted system and application audit evaluation based on COBIT standard; GLBA Standard; GAAP Standard; ISO 27001/2, GRC and NIST Reviewed the adequacy of projects, adopted project management methodology for compliance with industry standard SDLC; Created IT operations group in order to consolidate

production support, which was formerly spread across multiple departments and functions Education B.Sc. in Biochemistry Adekunle Ajasin University - Dallas, TX December 2006 Computer Science St. Anthony Information Technology College January 2001 to December 2002 Skills BUSINESS CONTINUITY, CISA, DISASTER RECOVERY, HIPAA, PCI, Information Security, Cyber Security, Nist, Network Security Additional Information SKILLS: Disaster Recovery & Business Continuity testing/compliance review; SOX Controls, HIPAA Privacy and Security Rules, Operational Audit, Financial Audit, SDLC, Firewall Security tools, Network monitoring and Protection Systems review, PCI-DSS Compliance, Governance Risk and Compliance, Archer GRC, Risk Management, Project Management, Change Management/ Tape Backup, Incident management and Problem management; Microsoft Office, PowerPoint, Access, Excel (VLOOKUPS, Pivot tables) etc. , Microsoft Visio , Lotus Notes, privileged ID management ,Windows Servers and SharePoint. CISA Certification in progress.

Name: Julie Riley

Email: jeffreywilliams@example.net

Phone: +1-536-963-0421x034