Manager IT Manager IT Manager IT - Coal fire Labs Atlanta, GA Enterprise Information Security Technologies experience with focus on Cyber security, Information Security, Application Security, IT Governance, Risk Management, Compliance and IT Audits with specialization in Security analysis, design, development and testing of applications in n-tier architecture and Systems Security Certified ISO 31000 Lead Risk Manager Certified ISO 27001 Lead Auditor SANS GIAC certified in Information Security Policy (GFSP) Experience with Cloud technologies and implementation of SaaS based security controls Experience with IT Compliance and Audit Standards of ISO 27000 series, SOC and SSAE Experience with Data Protection and Data Privacy- GDPR Manage technology teams and develop and implement project schedules to meet deadlines, ensuring projects maintains profitability and engage in ongoing client meetings to ensure client satisfaction. Managed Regulatory Compliance implementation with OWASP, FISMA, HIPAA, PCI- DSS, GLBA, SOX, COBIT, COSO, FFIEC, NIST, ISO 27001, ISO 27002, DFARS NIST SP 800-171 and GDPR Knowledge of 21 CFR Part 11, Annex 11 Regulations and Good Manufacturing Practice (GMP) Governance and Compliance experience with ISO 31000, COBIT, ISO 27001, PA DSS, PII and PHI Strong understanding of information technology controls and security experience in a widely used financial application environments like (SAP, Oracle, JD Edwards, PeopleSoft, etc.) Provided Project Management and Continuous improvements, defined ITIL Project goals, managing resources, project time lines and lead multi-discipline teams while fostering input from various levels Experience in Enterprise Risk Management frameworks - COSO ERM, ISO 31000, ISO 27005, NIST 800-30, FAIR, OCTAVE Experience in Compliance and Audit in ISO 27001-2 standards in domains of Security Policy, Incident Management, Cloud, Business Continuity/Disaster Recovery, Access Control, Asset Management Managed and lead Business Continuity (BCP) and Disaster Recovery process (DRP) Experience with Cloud technologies and implementation of SAAS based security controls. Experience managing Projects based on Agile Methodologies including ITIL, COBIT and CMMI Experience leading and managing IT Risk, Governance, Security and Audit frameworks (COBIT, COSO, ISO 27001/2/5, NIST 800-53, SSAE 18, SSAE 16) Experience in developing a compliance schedule tailored for SSAE 16/SOC and ISO 2700x Audits Experience and strong knowledge of Internal Controls over Financial reporting including SOX 404, SOC 1 Audit reports, COSO, US GAAP, ITGC, PCOAB and IIA Standards   Managed and lead Regulatory & legal security standards such as PCI DSS, Sarbanes-Oxley, HIPAA   Managed and provided regulatory expertise and solutions on complex risk and compliance issues.   Managed and lead projects involving Security best practice frameworks - COBIT, NIST 800.x, ITIL, ISO 27001, ISO 27002, ISO 27005, HITRUST, PCI, SOX, FED RAMP and FFIEC   Several years of technical experience in Information Security, in an environment certified and compliant with globally recognized Security Frameworks and maintained Compliance with GDPR, PCI, COBIT, SOX, NIST, ISO 27001 and ISO 27018 Controls   Experience with Web App Security tools with an understanding of Application security   Experience with Cyber Security compliance and regulations and knowledge of NY DFS Cyber Security rules and regulations.   Knowledge and experience with NERC CIP and SSAE-18 Compliance, ERP Systems   Experience with computer security procedures and protocols and experience with Security Information Event Management tools (SIEM), Intrusion Detection & Prevention Systems (IDS/IPS), Firewalls & Log Analysis, Network Behavior Analysis tools, Antivirus, and Network Packet Analyzers and malware analysis. Monitored Security State and managed continuous monitoring   Experience with Web application development using Java, .NET (C#)   Implemented Security Controls, Common Security standards, Practices and Risk frameworks - FAIR, ISF, NIST, OCTAVE, STRIDE, ISO 27005 and ISACA   Experience with Payment Card Industry (PCI DSS, PA-DSS, P2PE)   Knowledge and understanding of Cryptography -PKI, PGP, SSL, SSH   Involved in Risk Assessment and GAP Analysis performing GAP analysis w.r.t. Security, Privacy and Compliance of regulatory standards and reported Risk factors. .Experience with Threat Modeling using STRIDE, Penetration testing and Code Security reviews   Application Security Planning and Security Architecture Work Experience Manager IT Coal fire Labs - New York, NY August 2017 to Present Coal fire Labs   Responsibilities   Responsible for performing Security Risk Assessments, managing Vulnerability Management Program and implementing Controls with Regulatory requirements of HIPAA, PCI DSS, GDPR   Manage Technology teams and provide Project Management and strategy in all aspects of IT, Business risks and Audit engagements   Experience in IT Governance Frameworks of ISO 31000, COBIT, FFIEC and COSO   Managed IT Compliance and Security of Audits, Compliance checks and assisted external assessment processes for Auditors, Payment Compliance Industry (PCI), Personally Identifiable Information (PII), General Data Protection Regulation (GDPR), HIPAA and SOX Compliance   Responsible for ensuring Privacy and Data Protection and implementing Security and Compliance programs; working towards implementing Privacy by design in creating solutions and meeting   PCI DSS, ISO 27001, HIPAA, HITRUST, SOC II security and privacy requirements   Worked with Top Payment Application Clients in the industry for PCI and HIPAA, HITRUST CSF, and Compliance to meet Information Security requirements and Security Maintenance   Experience with Cloud architecture, Cloud Security, Risk and Governance Process design and and implementation of security controls   Managed, developed and executed Annual IT Audit Plans as well as Testing IT Processes   Created and managed Cyber Security Policies along with 23 NYCRR 500 cybersecurity requirements   Managed and conducted IT Audit on overall Information Security aspects for each client covering User & Access Management, Database Access & Network, Data Storage, Internet, Intranet, Audit trails & Data Privacy Protection management   Experience with Internal Controls, Risk Assessments, Business Process and Internal IT Control testing and Operational Auditing   Involved in performing Audits and Internal testing of Controls annually around ISO 27001, FISMA audits and other IT Risk areas as needed   Participate in Internal and External Audits and coordinate into Security Services activities   Experience in performing Auditing and other testing of Security Controls, developing Audit Plans and Procedures and reporting the results of such audits   Manage GDPR Compliance overview, Road mapping, Program development and Implementation   Manage and lead GDPR Program Management, Regulatory Compliance mapping and monitoring   Managed and delivered IT Risk Assessments and Audits on various projects involving IT Governance and Strategy, DRP, BCP Change Management and Cyber Security areas   Experience in Payment Card industry, Credit card transactions and Audit of Payment Application logs and ensure PAN is rendered unreadable   Managed Projects with Data Governance, Data Privacy, Created Plan of Action and Milestones (POA&M)   Managed and Lead Business Continuity and Disaster Recovery Program including Business redemption, System Recovery and restoration and provided overall IT Support for Internal Clients   Managed and lead development, implementation of relevant Metrics to measure the efficiency and effectiveness of ISMS, Governance, Risk Management and Compliance programs across Coal fire   Experience working with Risk, Security and Audit frameworks (COBIT, COSO, ISO 27001/2, ISO 27005, NIST 800-53, SSAE 16) and ISO 27018 controls   Experience in Governance and Compliance for PCI PA-DSS, FISMA, PII and GDPR   Assisted in the analysis of PCI Assessment findings, owner identification, remediation planning   Experience in Information Security Policy creation and acceptance   Experience in meeting PCI, PII and PHI requirements   Involved in maintaining Data Privacy for GDPR, HIPAA, FDR and lead SOC 2 and HITRUST Audits   Implemented Data Protection Governance Practices, Privacy Impact and Gap Assessments   Involved in Cybersecurity Controls Assessment delivered using best practice frameworks including NIST CSF, COBIT 5, CIS and other frameworks   Implemented SaaS based Cloud security Controls   Involved in working with Information Security Analysts and application & service owners with PCI-DSS compliance tasks such evidence preparation, gathering and submission to the PCI-DSS assessor for annual compliance   Collect and evaluate evidence and prepare reports and documentation in an appropriate format.   Involved in working with Payment Card Industry (PCI DSS, PA-DSS) and P2PE relevant projects.   Assisted in filling out ROVs and ROCs for numerous Clients including POS applications   Validated technical controls of PSS Data Standard   Created White Papers through Client Documentation and review   Involved in implementation of System Security Software and other Forensic tools   Evaluated Payment Applications using Wire Shark Forensic Tools.   Exposure to PKI and Asymmetric and Symmetric encryption   Utilized Control Routines and Risk Management Policies to identify and analyze risks   Environment: ITIL, PCI DSS, P2PE, HIPAA, GDPR, FTK, GRC Archer, NIST RMF, OCTAVE, STRIDE, FED RAMP, Wire Shark, PKI, NIST CSF, ISO 27005, Cyber security, NERC CIP, SSAE-18 SOC 1, ISO 27018, COSO ERM VP Senior IS Tech Analyst Citibank - Fort Lauderdale, FL July 2015 to August 2017 Technology, Security and Operations   Responsibilities   Managed Audit in meeting GLBA Compliance requirements and

FFIEC Compliance   Managed and supported Combined US Operations Enterprise Wide Risk in assessing areas for improvement and Gaps related to internal standards, new and existing rules and regulations   Managed and supported all aspects of Governance, Risk and Compliance within the CUSO   Managed Bank IT Audit implementing best practices and meeting Regulatory Compliance needs and provided Audit reports to improve Bank IT Security Program   Managed Bank IT Compliance and Risk assessments, IT Audits, and Internet Banking Audit,   Managed Bank Disaster Recovery Plan and Bank's Business Continuity Program   Manage Risk Assessments internally and externally and support a large-scale global enterprise and set direction as a leader working through three lines of defense   Involved in ensuring Risk Management in coordination with different Stake holders of Risk, IT Risk Management Group, OPC, Compliance, Regulatory affairs and Supervisory relations   Involved in implementing Safeguarding Standards and provided implementation in relevance with NIST Cyber Security Framework (CSF) incorporating it into Risk Management.   Evaluated Applications using Static Coding analysis tools - Vera code, IBM AppScan Tools and provide Application Vulnerability Assessment services (Dynamic and Static) to all Citi businesses and technology teams globally   Implemented Cloud Security Controls across technology stack to meet Security and Compliance requirements for IaaS, PaaS, SaaS   Involved in evaluating current risks and provide recommendations for Risk Tolerance and Mitigation.   Collaborate with Stakeholders to document and implement necessary Policies and Procedures to comply with ISO 27001 Standards and to obtain Certification.   Participate with leaders in definition and implementation of Information Security Policies, Strategies   Involved in creation and maintenance of new Policies and Procedures enhancing the existing Policies, Procedures and IT Risk requirements as needed.   Source Code Reviews and OWASP Secure Coding Practices   Experience in Security Policy development, writing, security education, Application Vulnerability assessments, Risk Analysis and network penetration testing   Assisted in driving day to day activities and execution of PCI Program across Citibank   Worked with Policy and Standards team to integrate PCI Compliance aspect into Citi's current Policy and Risk Management Process.   Managed BC/DR program including BIA Analysis, DR Plan documentation, BC and DR exercises, emergency management communications across Banking divisions during Cyber events/outages Managed and involved in all aspects of Risk Management including implementation and monitoring Risk Management process in the organization. Managed Audit activities for a functional entity at Regional level including a portion of Annual Audit Plan along with managing Annual Audit Work Plan Managed IT Audits, Information Technology Risks and Controls, Information Security & Governance Overseeing and implementing the Global SOX, ISO 27001 Control Frameworks across Citi Global IT Managed and developed Information Security Standards, Procedures, Policies and guidelines along with Application architecture and threat modeling Involved in defining Bank's Information Security Program, Policy and Standards and Provide reasonable assurance that Security Program and IT Governance processes and Controls are properly implemented and Corrective actions are taken where needed. Environment: ITIL, ISO 31000, ITIL, SOX, COBIT, IBM AppScan, Vera code, PCI Compliance, ISO 27001, GRC Archer, FAIR, STRIDE, OCTAVE, NIST RMF, ISF, NIST CSF, ISO 27005, COSO Applications Security Analyst General Electric (GE) Capital - New Orleans, LA October 2013 to July 2015 IT Security and Operations Responsibilities Responsible for Internal Controls and Risks of GE Capital Bank Technology network Involved in identifying Application Vulnerabilities and implementing Security Practices for Cloud Involved in Planning and execution of Internal Audit procedures and creation of Internal Audit reports. Experience in Audit Log reviews and SOC Operations support Managed Security Policies, Procedures and responded to security reviews Reviewed system Audit logs in accordance with the SSP Managed and involved in performing manual Security architecture risk analysis, thread model reviews of applications and assess their design against known or emerging threats Managed, driven remediation efforts related to Information Security, Remediation for Incidents, Vulnerability Scans, Pen tests, Internal and external Audits and Critical Practice assessments. Lead Vulnerability and remediation efforts for identified issues on Systems, devices and Network devices with System owners Assisted in managing an outsource relationship for 3rd party application development Lead trouble shooting technical issues and identified modifications needed in existing applications to meet the changing user requirements and managed risk with reference to NIST Cyber Security Framework (CSF) and mitigate Cyber Security events Enterprise level Information Security Architecture design and, coordinate Information Security procedures and controls, application testing and security incident response Analyzed and tested new and existing procedures, information systems and utility programs for security vulnerabilities and recommended remediation procedures. Coordinated application development with Code Scanning with HP Fortify for multiple projects. Assisted in Source Code Analysis, Remediation and troubleshooting of application security issues. Analyzed data contained in the corporate database and identified data integrity issues with existing systems and proposed system solutions. Assisted System analysis and design of security requirements for GE Security & Operations division Managed and lead Security Development Lifecycle (SDL), system development life cycle and Programming with Internet facing applications using Java and C# Analyzed Action plans for application vulnerabilities and provided remediation plans Involved in Firewall Policy evaluation, review and design Recommended alternatives for application security and issue resolutions Deliver reporting to Security Leadership on Remediation efforts Assisted various divisions of GE in the implementation of Software Security and Systems software Involved in educating Security awareness with end users Retrieved data to prepare documents, and produced a variety of reports from databases Creates and generated documentation concerning security procedures and maintenance of Reports Assisted in maintaining a System Security Plan (SSP) and Security Testing Assisted in updating OS software and antivirus definitions in accordance with the SSP requirements Participated in weekly meetings with the IT Security and Network team to discuss progress and issues to be resolved, and report progress on a weekly basis to the Team Manager. Deliver reporting to Security Team leadership on remediation efforts Experience in running Vulnerability Management tools and utilize manual techniques to identify and validate closure of security issues. Environment: ITIL, NIST RMF, STRIDE, UNIX, HP Fortify, Vera code, Qualys, Java, .Net, C#, Oracle, Java script, SQL, HTML, Information Security, COSO, COBIT Education Master of Computer Applications in Computer Applications Nagarjuna University Bachelor of Computer Science in Computer Science Nagarjuna University Post Graduate Diploma in Systems Management in Systems Management NIIT Additional Information TECHNICAL SKILLS

Project/Program/Portfolio Management: ITIL, COBIT, ISO, Agile, PMI IT Risk management: COSO ERM, ISO 31000, ISO 27005, NIST 800-30 Compliance & Audit: ISO 27001/2, COBIT 5, GDPR, Fed Ramp, DFARS, FFIEC, SOX, NIST 800-53, NIST SP 800-171, PCI DSS, HIPAA, FISMA PCI: PA DSS, PCI DSS, P2PE, SSAE 18 SOC 1, SSAE 16 IT Security Tools: FTK, Wire Shark, Nessus, Encase Vulnerability scans tools: Qualys, HP Fortify, IBM AppScan, Vera Code Business Intelligence: SSAS, SSIS, SSRS, BOE Crystal Reports XI /2008 / 2011 Data Bases & Data Analytics: SQL Server 2008/2012, Oracle, PL/SQL Languages & Web: JAVA, C#, Ruby, PHP, C, Pascal, COBOL, HTML, XML, TCP/IP Reporting Tools: Oracle Reports, Crystal Reports, SSRS Operating Systems: UNIX, Linux, Sun Solaris, Windows XP/98/NT/2000

Name: Lauren Moore

Email: shelby43@example.com

Phone: 260-685-6644x76245