Senior Manager - IT Security Specialist Senior Manager - IT Security Specialist Senior Manager - IT Security Specialist - Quest Diagnostics Rutherford, NJ Certified Information Security professional by ISC2. Experienced Information Technologist with demonstrated knowledge as an Information Security / Risk Manager protecting information systems and information data resources; specialize in the Security Assessment & Authorization (SA&A) process. Committed to providing adequate security in line with National Institute of Standards & Technology (NIST) Standards and organizations policies and procedures and other industry framework. TECHNOLOGY SUMMARY Project Management and Critical Writing   Security Assessment and Risk Management   MS Office Suite SOX, PCI DSS Audits, HIPAA   FISMA   Systems Development Life Cycle (SDLC), NIST, OMB Circulars Work Experience Senior Manager - IT Security Specialist Quest Diagnostics - Secaucus, NJ January 2017 to Present Manage third party IT security assessments of in scope third parties in accordance with policies and standards. ? Manage, design, plan, review, implement and track audit procedures, risk assessments, and performances of internal audits, SOX reviews. ? Responsible for assessing, documenting, and communicating third party risk exposure to ensure General Data Protection Regulation (GDPR) adherence. ? Provide high-level security guidance and leadership to executive team as well as across Quest. ? Perform and lead various audits of financials, internal controls and operations. ? Validate evidence from vendors prior to closing out remediation plans. ? Lead and perform required legal and risk due diligence for large scale contract negotiations (SOW, SLA, MSA). ? Responsible for identifying, developing, and managing compliance with security controls. ? Interpret and provide guidance on key data risks and controls, majorly on vendors handling sensitive and confidential data. Identify control weaknesses and suggest appropriate remediation ? Organize training and scheduling meetings with staff and management on Risk Management. ? Head of Change Management team, updating Risk Register and Policy Exception approval. ? Build and mentor information security team in managing organizational key controls. ? Develop and implement executive level metrics and dashboards for communicating third party risk to leadership. ? Create, implement, and maintain information security policies to stakeholders. ? Manage the review of vendor due diligence materials (SSAE 16 reports,

Penetration Testing reports, ISO 27001, Information Security Policy). Third Party Risk Manager KPMG International, Wood Cliff - Lake, NJ, US January 2015 to December 2016 Managed risk assessments for vendors, identified and documented control gaps, and presented results to support management action, escalation and risk acceptance processes. ? Collaborate with engineering teams to provide security solutions and ensure new products meet high security standard. ? Managed SOC, SOX or ISO 27001 engagements and performed internal control reviews. ? Managed the annual audit plan, investigations, special reviews and other ad hoc projects. ? Develop company-wide training programs to communicate information security risks. ? Worked directly with key business leaders to facilitate information risk analysis and risk management processes, identified acceptable levels of risk, and established roles and responsibilities with regards to information risk management. ? Identified issues, assigned appropriate risk ratings, and documented them according to Risk / Compliance Department's Issue Management process. ? Regularly audit IT systems to ensure regulatory and industry compliance. ? Responsible for reviewing and assessing security controls of third parties to ensure the security and integrity of data while in possession of vendors. ? Partnered with business across the enterprise to evaluate the information risks associated with their vendor engagements. ? Developed senior management reports including defining and tracking program-based metrics (assessments completed within SLA, MSA, challenges). ? Head of the IT Security Audits Team and Compliance Team. Information Assurance Security Manager Office of Mental Health - Albany, NY August 2012 to December 2014 Developed and Reviewed SA&A packages for compliance with NIST Risk Management Framework (RMF), including System Security Plans, System Categorization Documents, Risk Assessments, Plan of Action and Milestones (POAM) & Contingency Plans. ? Led audit activities including risk assessments, audit planning, audit testing, control evaluation, report drafting, work paper documentation, follow up and track management's corrective actions in response to control findings and verification of issue closure. ? Managed client interviews to determine the security posture of the system and to assist in the completion of the Security Assessment Plan using NIST SP 800-53A. ? Developed assessment packages throughout the life cycle of existing major applications and

General Support Systems. ? Managed Information Assurance (IA) team performing technical security risk assessments of systems via interviews, documentation review and walk-through both new and legacy information systems. ? Participated on IA team conducting risk assessments, documentation for Security Control Assessment, systems analysis and hardening, vulnerability testing and scanning. Senior Information System Security Analyst Envios de Valores La Nacional - Irvington, NJ October 2009 to July 2012 Examined existing IT Systems and business models to understand areas of performance degradation. ? Analyzed system requirements for clients' future needs. Implemented, configured and tested feasible solutions. ? Interpreted, identified, and prioritized risk based on impact and likelihood. ? Performed data analysis and extraction of queries to determine third parties in scope. ? Maintained the system for risk entity in the data using Intrusion Detection System (IDS). ? Served as the main strategist for assigned categories and worked with supporting teammates to fully understand scope of suppliers, services and sub-categories. ? Managed compliance audits as well as plan and update audit methodology and quality assurance. Information Security Analyst Cotecna Destination Inspection Limited - Lagos, NG April 2005 to August 2009 Provided guidance and direction on conducting thorough Information Security due diligence to onboard and pre-screen prospective new suppliers. Advise direct reports, as needed to engage with prospective supplier's technology and security teams to assess their technology, operating methodology, and security policy. ? Provided guidance and direction on the assessment of external information security certifications and internal or self-assessed evidence (Info Security Policy, Audit Reports, Data Flow diagrams). ? Established requirements on recommendations of risk mitigation techniques or compensating controls to relationship owners and suppliers based on business requirements, nature of relationship, and criticality of supplier. ? Configuration of packages into information systems and gap / patch management. Customs Checker / Risk Analyst SGS Inspection Services SA - Lagos, NG November 2000 to March 2005 Analyzed and determined risks to help clients make sound financial decisions. ? Determined solutions to minimize or eliminate risks. ? Set plan and resolution for vendor management activities within designated categories. ? Managed large-scale supplier service implementations within given categories by creating and

executing a project plan. ? Collaborated with internal supplier relationship owners to understand business requirements, and provided them with support, education, and training to build their risk awareness. ? Monitored and assessed the post-period implementation of risk management strategies. Education MBA University of the People June 2019 Bachelor of Arts in Mass Communication in Mass Communication Auchi Polytechnic, Auchi, Edo State December 1998

Name: Marissa Gould

Email: shelleybaker@example.org

Phone: 8505986892