IT Security Analyst IT Security Analyst IT Security Analyst - Montefiore Medical Center Bronx, NY Work Experience IT Security Analyst Montefiore Medical Center - Bronx, NY July 2015 to Present Schedule, plan, and participate in internal auditing in accordance with HIPAA, NIST, and PCI standards Perform security assessments; design reviews; and provide guidance on new technologies for the customers. Develop POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Perform Assessment and Authorization (A&A) documentation in compliance with company standards Perform Security Categorization (FIPS 199 and NIST SP 800-60 vol 2), Privacy Threshold Analysis (PTA), e-Authentication with business owners and selected stakeholders Author or coordinate the development of other required system security plans: Configuration management Plan (CMP), Contingency Plan (CP), Continuity of Operations (COOP), Disaster Recovery Plan (DR) and Incident Response Plan (IRP). Conduct Systems Risk Assessment through Risk Analysis, assessed the various Assets within the systems boundaries and rigorously identifying all the possible vulnerabilities that exist within the system. Developed the audit plan and performed the General Computer Controls testing of Information Security, Business Continuity Planning, and Relationship with Outsourced Vendors. Performing Vulnerability scanning using Nessus Ensure all security-related incidents are documented and reported to the ISSM and Security Officer Perform systems security audit on a weekly basis to detect unauthorized activities and ensure systems maintain security compliance. Perform Security Control Assessment (SCA) according to NIST SP 800-53A Document and conform to processes related to security monitoring, patching and incident response Manage the organization's RMF continuous monitoring tool and complete specific control activities, Maintain security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Upgrade security systems by monitoring security environment; identifying security gaps; evaluating and implementing enhancements. Perform security engineering analysis, risk and vulnerability assessment, etc. Monitor and analyze security functional tests. Prepare A&A documentation such as SSP, ST&E reports, etc. Information Security Analyst Beth Israel Medical

Center November 2012 to July 2015 NY Guided System Owners and ISSOs through the Certification and Accreditation (C&A) process, ensuring that management; operational and technical controls for securing either sensitive Security Systems or IT Systems are in place and are followed according to federal guidelines (NIST 800-53). Applied security risk assessment methodology to system development, including threat model development, vulnerability assessments and resulting security risk analysis Provided support and guidance through the phases of FISMA C&A, including monitoring of the C&A artifacts compliance, annual self-assessment (NIST SP 800-53A guidelines) and quarterly self-assessment completion using NIST SP 800-26 guidelines. Created or updated the System Security Plan and conducted an Annual Self-Assessment. Applied knowledge of C&A policies, guidelines, and regulations in the assessment of IT systems and the documentation and preparation of related documents Assesses and mitigates system security threats/ risks throughout the program lifecycle determines/ analyzes and decomposes security requirements at the level of detail that can be implemented and tested; reviews and monitors security designs in hardware, software, data, and procedures, Worked with C&A team members and senior representatives to establish and define programs, resources, schedules, and risks. Developed Test Plans, testing procedures and documented test results and exceptions. Conducted the IT Risk Assessment and documented the controls. System Administrator VALCO Ghana Limited March 2007 to September 2009 Contributed in system administration support for Windows systems including server, router, switches and workstation upgrades, backup and disaster recovery monitoring and security administration. Performed daily, weekly, monthly maintenance, backups/restorative exercises, reviewing server logs for prospective issues, as well as ensuring that anti-virus software and security patches are routinely updated and functioning Troubleshoot network device connectivity issues including IP addressing, DNS, gateway, and reverse proxy issues. Supervised the technical staff to troubleshoot complex issues faced by system users Ensured daily activities are aligned with Network operations priorities and objectives Prepared and delivered system performance statistics and reports weekly (disk usage, forefront reports) Supported and maintained network hardware, network operating systems and system applications

Reviewed multiple computer systems capabilities, workflow and scheduling limitations to increase productivity Conducted meetings with IT teams to gather documentation and evidence about their control environment Education Management Information System Kumasi Polytechnic Skills Change management (3 years), Nist (6 years), system security (6 years), testing (6 years), security Additional Information TECHNICAL COMPETENCY Working knowledge of Risk Management Framework (RMF) for Assessment & Authorization process to obtain an ATO using federal security policies, standards and guidelines including FIPS 199 & 200 and NIST 800 SPs such as 800-18, 800-30, SP 800-34, 800-37 rev 1, 800-60, 800-53 rev 4, SP 800-53A, SP 800-84). Experience in developing and reviewing security Authorization and Assessment (A&A) artifacts including, but not limited to Contingency Plans (CP), Incident Response Plans (IRP), Configuration Management Plans (CMP), Privacy Threshold Analysis, (PTA) and Privacy Impact Assessments (PIA). Knowledge of Federal and international regulatory bodies such as Office of Management Budget (OMB), FISMA, RMF, FedRAMP, HIPAA and ISO. Experience in performing on-site security testing using vulnerability scanning tools such as Nessus and Penetrating testing using tool such as Nessus and Wireshark Experience in the development of A&A Package Documents such as System Security Plans (SSP), Security Assessment Reports (SAR) and Plan of Action and Milestones (POA&M). Proficient in explaining technical information, resolutions, documentations, and presentations to clients and non-technical personnel at all levels of the organization or enterprise. Team oriented with the ability to work independently and proactively while prioritizing competing priorities, often under time constraints.

Name: Mr. Tommy Haley

Email: wilsonamanda@example.net

Phone: 819.297.3425x839