IT Risk & Compliance Analyst IT Risk & Compliance Analyst IT Risk & Compliance Analyst - Bureau of Labor Statistics Frederick, MD Work Experience IT Risk & Compliance Analyst Bureau of Labor Statistics - Washington, DC September 2017 to Present Develop and maintain A&A documentations, including System Security Plans, Contingency Plans, Risk Assessment Reports and evaluated existing documents and their accuracy ? Experience in using security policies, standards, procedures, guidelines, and best practices from areas such as FISMA and NIST ? Updates IT security policies, procedures, standards, and guidelines according to private and federal requirements. ? Develops and/or maintains POA&Ms for all accepted risks upon completion of system SCA, including the utilization of waivers/exceptions where appropriate ? Creates remediation strategies for weaknesses based on priorities ? Reviews and updates FIPS 199 (SP 800-60), Initial Risk Assessment (SP 800-37), E-Authentication, PTA, PIA, ST&E, POA&M as part of the Security Assessment and Authorization (SA&A). ? Prepares Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. ? Provides review and progress reports of all Plan of Action and Milestones (POA&Ms) ? Coordinates with System administrators to provide fixes for vulnerabilities identified in systems. ? Analyzes organizational information security policy needs based on stakeholder interactions, develop and publish policy, standards, security handbook, and procedures for implementation ensuring alignment with NIST 800-53 Rev 4. ? Prepares security authorization (A&A) documentation including System Security Plan (SSP), Security Control Test and Evaluation (SCT&E), Security Assessment Report (SAR), Contingency Plan (CP) and other artifacts required for the ATO package. ? Conducts formal Security Test and Evaluation (ST&E) in conjunction with the ISSO, report findings to management, then devise strategies to mitigate risk ? Participate in security team meetings and render other support to IT Security office, which includes ensuring appropriate steps are taken to implement information security requirements for all IT systems ? Assist with conducting Security Assessment using NIST 800-53A ? Worked with System and Data Owners to develop security artifacts (e.g., SSPs, PIA, SRA, etc.). ? Performed Security Test and Evaluation (ST&E) - technical controls, document review, and management interviews. ?

Facilitated and participated in assessments and authorizations (certification & accreditation), compliance reviews, architecture reviews, trainings, plans of action & milestone resolutions, and reports on program status ? Assisted in risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs ? Monitored emerging IT security threats and developed appropriate response measures ? Assisted with the development of security related training and awareness programs. Information Technology Security Specialist Teleworld Solutions - Chantilly, VA June 2015 to August 2017 Identified vulnerabilities, recommend corrective measures and ensure the adequacy of existing information security controls (POAM) ? Reviewed and conducted audits to ensure information systems maintained the compliance baseline. ? Coordinated with appropriate personnel to run vulnerability scans on a regular basis and ensure timely remediation actions ? Liaised with audit team to investigate and respond to Financial Audits ? Coordinated with System administrators to provide fixes for vulnerabilities identified in systems. ? Reviewed and analyzed log files to report any unusual or suspect activities ? Collaborated with IT Operations team to ensure cybersecurity threats are properly identified, analyzed, communicated, addressed and/or defended, investigated, and reported to management. ? Assessed vendors' security controls to ensure new and existing vendors adequately protect customer information ? Prepared reports that document security breaches and the extent of the damage caused by the breaches ? Assisted with installation and software usage, such as firewalls and data encryption programs, to protect sensitive information ? Assisted business units with understanding the risks associated with a particular vendor and recommended solutions to reduce or eliminate risk. ? Reviewed and conducted audits to ensure information systems maintained the compliance baseline ? Delivered evidence and feedback to assist the client with review of the audit ? Handled all preparations & planning for upcoming Audits ? Scheduled/ run a vulnerability/penetration test and oversee remediation of any vulnerabilities before engaging external auditors ? Managed all requests from the QSA during the audit ensuring that timely responses are obtained ? Assisted with ongoing compliance activities such as antivirus, patching, and half a year firewall rules review ? Performed quarterly Access Control reviews such as removing any terminated employees IT

Security Analyst INOVA Fairfax Hospital - Fairfax, VA March 2014 to May 2015 Performed risk assessments of various technologies within the client's environment ? Worked with internal auditors on various compliance audits and assessments, such as PCI-DSS and HIPAA ? Coordinated internal and external regulatory IT and Security audits; met with subject matter experts to facilitate reviews ? Updated IT security policies, procedures, standards, and guidelines according to private and federal requirements. ? Created remediation strategies for weaknesses based on priorities as contained in vulnerability reports ? Coordinated with System administrators to provide fixes for vulnerabilities identified in systems. ? Responsible for managing security vulnerabilities patching, application, and OS version control compliance ? Ensured audit logs were captured and maintained to meet compliance requirements ? Monitored the regulatory requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law ? Coordinates initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the client ? Worked cooperatively with departments and health information staff and other applicable organization units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate. ? Planned and executed the tasks necessary to ensure the services, provided by key third party vendors, suppliers and business partners do not pose a risk ? Performed site HIPAA audits to ensure compliance with HIPAA regulations ? Assisted in performing periodic internal audits to ensure compliance as well as preparing material for any external IT audit from delegated Health Plans or State and Federal agencies as needed ? Tested information security controls, across multiple business processes and/or locations, ensuring implementation techniques meet the intent of organizational compliance frameworks and security requirements ? Updated policies and procedures describing security requirements, guidance, and standards for organizational information systems and architecture Education BA in Information Technology Southern New Hampshire University - Manchester, NH December 2017 MS in Cybersecurity Technology University of Maryland University College Skills Compliance, Assessment Certifications/Licenses AWS Developer Associate October 2018 to October 2020 Scrum Master December 2017 to Present

Name: Carol Baker

Email: hallnathan@example.org

Phone: 839-744-9863x2765