IT Security Analyst-Consultant IT Security Analyst-Consultant IT Security Analyst-Consultant - Environmental Protection Agency Mebane, NC Work Experience IT Security Analyst-Consultant Environmental Protection Agency - Durham, NC October 2018 to Present October 2018- Present ? Perform security categorization, using FIPS 199, and review Privacy Threshold Analysis (PTA), and E-Authentication with business owners and select stakeholders Documents and Review security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for multiple EPA systems. ? Coordinate with system owner, system administrator, and system engineer, in implementing security controls that was selected using NIST 800-53 v. 4. ? Observe security controls and major support systems on an ongoing basis to assess control effectiveness, document changes to information system and conduct impact analysis. ? Work with Point of Contacts and client to resolve POA&M items ? Conduct Kickoff meetings and status weekly meetings with all stakeholders ? Assist Independent Verification and Validation (IV&V) team re-tests to confirm the remediation and mitigation strategies to close out POA&M items ? Supplement the security controls and security documents based on the organization's risk assessment and local documents. ? Assess security controls on a day to day basis by testing, interviewing, and examining of systems for compliance with FISMA regulations. ? Assist with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans. ? Conducted meetings with the IT team to gather documentation and evidence about their control environment. ? Prepare security assessment reports, documenting issues, findings, and recommendations from, security controls assessments. ? Facilitate and participate in assessment and authorization (certification & accreditation), compliance reviews, architecture reviews, training, plan of action & milestone resolution, and reports on program status ? Assist in the conduct of risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs ? Participate in on-site evaluations/audits for compliance with policy ? Create and maintain security checklists, templates and other tools to aid in the A&A process ? Perform security control assessment using NIST 800-53A guidance and as per continuous monitoring requirements ?

Review and update core documents such as System Security Plan, Contingency Plan, Incident Response Plan, Standard Operating Procedures, Plan of Actions and Milestones, Remediation Plans, Configuration Management Plan ? Support all assessment interviews and collects artifacts (evidence of a control being in place or not) and associates all information to the proper control PCI-QSA Security Consultant Citizens Bank - Cranston, RI September 2016 to October 2018 Establish schedules and deadlines for assessment activities ? Assist business units with understanding the risks associated with using a vendor and recommending solutions to reduce or eliminate risk. ? Develop, update and test the Information Technology Incident Response Plan ? Assist with implementing operating procedures including communication, documentation, quality, and change control processes ? Participate in new technology deployment initiatives, contributing to the foundation's overall adoption of best security practices ? Ensure that compliance PCI standards are maintained across all departments for the U.S. payment program ? Coordinate with other members of the information technology and information security functions and end user departments to implement and sustain appropriate technical and procedural controls ? Assisted with annual PCI audits and third-party audit relationships across multiple jurisdictions ? Remain apprised of pending changes to standards and proactively design and apply appropriate measures ? Monitor PCI DSS compliance of relevant hosting partners and application vendors ? Perform ongoing security procedures, including review of firewall activity and other system logs, vulnerability (anti-virus, software/firmware patch) management, periodic system intrusion testing and investigation of exception conditions ? Monitor compliance with Information Security Policies related to payments program with emphasis on PCI ? Review and conducted audits to ensure information systems maintained the compliance baseline Information Security Compliance Analyst National Science Foundation - Alexandria, VA June 2014 to August 2016 Alexandria, VA Information Security Compliance Analyst June 2014 to August 2016 ? Performed security categorization, using FIPS 199, and review Privacy Threshold Analysis (PTA), and E-Authentication with business owners and selected stakeholders Documents and Reviewed security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA)

documents per NIST 800 guidelines for various government agencies. ? Observed security controls and major support systems on an ongoing basis to assess control effectiveness, document changes to information system and conduct impact analysis. ? Supplement the security controls and security documents based on the organization's risk assessment and local documents. ? Coordinated with system owner, system administrator, and system engineer, in implementing security controls that was selected using NIST 800-53 v. 4. ? Assessed security controls on a day to day basis by testing, interviewing, and examining of systems for compliance with FISMA regulations. ? Assisted with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans. ? Conducted meetings with the IT team to gather documentation and evidence about their control environment. ? Prepared security assessment reports, documenting issues, findings, and recommendations from, security controls assessments. ? Facilitated and participated in assessment and authorization (certification & accreditation), compliance reviews, architecture reviews, training, plan of action & milestone resolution, and reports on program status ? Assisted in the conduct of risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs ? Participated in on-site evaluations/audits for compliance with policy ? Created and maintained security checklists, templates and other tools to aid in the A&A process ? Performed security control assessment using NIST 800-53A guidance and as per continuous monitoring requirements ? Reviewed and updated core documents such as System Security Plan, Contingency Plan, Incident Response Plan, Standard Operating Procedures, Plan of Actions and Milestones, Remediation Plans, Configuration Management Plan ? Supported all assessment interviews and collects artifacts (evidence of a control being in place or not) and associates all information to the proper control ? Worked with Point of Contacts and client to resolve POA&M items ? Assisted Independent Verification and Validation (IV&V) team re-tests to confirm the remediation and mitigation strategies to close out POA&M items IT Security Analyst Connecticut Children's Medical Center - Hartford, CT January 2013 to June 2014 Assisted business units with understanding the risks associated with using a vendor and recommending solutions to mitigate risk. ? Contributed to HIPAA requirements,

framework including findings, checklists, templates, testing methods and techniques ? Worked in the capacity of PCI-ISA and partnered with QSAs for annual assessments ? Assisted in developing baselines, standards, compliance, policies and procedures ? Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies ? 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. ? Analyzed organizational information security policy needs based on stakeholder interactions, reviewed and updated policy, standards, security handbook, and procedures for implementation and ensuring alignment with industry leading frameworks (PCI DSS, NIST, COBIT, HIPAA) ? Supported the completion of the annual PCI DSS, SOX, HIPAA Report on Compliance, as relates to networking ? Accountable for managing security vulnerabilities patching, application and OS version control compliance ? Ensured audit logs were captured and maintained to meet compliance requirements ? Obtained and reviewed evidence of compliance to support technical or complex PCI DSS networking requirements ? Supported with internal auditors on various compliance audits and assessments, such as PCI-DSS and HIPAA ? Provided data and guidance regarding current laws, rules and regulations related to IT controls ? Coordinated internal and external regulatory IT and Security audits; met with subject matter experts to facilitate reviews ? 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 ? 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 ? Assisted with administration, management, and reporting for security assessments and on-going monitoring activities; e.g., SOC 2 Type II, SOX, ISO/IEC 27001, PCI DSS, HIPAA, GDPR, ? 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 ? Monitored the regulatory requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law ? Coordinated initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the client Junior IT Analyst Walgreens - Deerfield, IL February 2012 to December 2012 Assisted in identifying and communicating application control deficiencies and the associated risks ? Monitored controls post-authorization to ensure continuous compliance with security requirements ? Provided expertise and assistance in the development of continuous monitoring programs and plans ? Performed the adequacy assessment, independently testing the controls and escalating control issues to Management ? Conducted assessment of the security safeguards compliance with PCI-DSS standards. ? Managed the vendor risk management process, evaluating the information security risk attributable to vendors and the vendors' management of that risk ? Provided support and guidance for legal and regulatory compliance efforts, follow through on security response to audits, and audit support for all appropriate regulatory requirements including the Payment Card Industry Data Security Standard (PCI DSS) and Sarbanes Oxley. ? 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 ? 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 ? Assisted with administration, management, and reporting for security assessments and on-going monitoring activities; e.g., SOC 2 Type II, SOX, ISO/IEC 27001, PCI DSS, HIPAA, GDPR, ? 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 ? Monitored the regulatory requirements under the Health Insurance

Portability and Accountability Act of 1996 (HIPAA) law ? Coordinated initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the client Technical Support Deloitte - Accra, GH April 2009 to January 2011 Displayed courtesy and strong interpersonal skills with all customer interactions ? Resolved customer complaints and concerns with strong verbal and negotiation skills ? Resolved Remedy tickets daily ? Coordinated with other IT groups for remediation of complex issues ? Diagnosed and troubleshooted technical issues, including account setup and network configuration ? Talked clients through a series of actions, either via phone, email or chat, until they've solved a technical issue ? Properly escalated unresolved issues to appropriate internal teams (e.g. software developers) ? Provided prompt and accurate feedback to customers ? Ensured all issues are properly logged ? Researched and identified solutions to software and hardware issues ? Installed software and resolved technical issues Education Masters in Business Administration in Business Administration Northcentral University - Scottsdale, AZ May 2018 Bachelor of Science in Mathematics University of Cape Coast May 2006 Skills audit (4 years), documentation (4 years), information security (6 years), Payment Card Industry (4 years), Security (7 years) Certifications/Licenses CompTIA Security+ May 2018 to May 2021 CEH January 2019 to January 2021 MBA Present Additional Information Essential skills ? Performed Certification and Accreditation documentation in compliance with company standards ? Developed, reviewed and evaluated System Security Plan based NIST Special Publications ? Experience with Governance, Risk Management, and Compliance (GRC) tools desired ? Outstanding written and oral communication skills ? Experience in the health sector, with medical practices, institutions, health insurance, and/or other HIPAA-covered entities ? Strong analytical and quantitative skills ? Aid in training and spreading PCI compliance awareness within the organization ? Effective interpersonal and verbal/written communication skills ? Performed comprehensive assessments and wrote reviews of management, operational and technical security controls for audited applications and information systems ? Coordinated internal vulnerability assessments and scheduling of third party external scans. ? Able to multi-task, work independently and as part of a team ? Reliable knowledge about popular information security compliance and

privacy regulations such as PCI-DSS, SOX, HIPAA, ISO 27001, SOC 2, GDPR ? Knowledge of security principles and technologies Technical skills Security Audit/Assessment Tools: Nessus Vulnerability Scanners, Cylance Protect, Splunk and Anti-Virus Tools, FIPS 199, SORN, E-Authentication, PTA, PIA, RA, SSP, CP, CIPT, ST&E, SAR, POA&M, ATO, 800-53A, ISA, MOU, CSAM. Software: MS Office (Word, Excel, PowerPoint, Access, Outlook), MS Project, RSA Archer, and Remedy.

Name: Steven Franklin

Email: wyattchristopher@example.org

Phone: (843)425-5216