Information Security Specialist Information Security Specialist Information Security Specialist - Loudoun County Government Leesburg, VA Work Experience Information Security Specialist Loudoun County Government - Leesburg, VA August 2017 to Present Assist business units with understanding the risks associated with using a particular vendor and recommending solutions to reduce or eliminate risk. Identify vulnerabilities, recommend corrective measures and ensure the adequacy of existing information security controls Review and conducted audits to ensure information systems maintained the compliance baseline Coordinate with appropriate personnel to run vulnerability scans on a regular basis and ensure timely remediation actions. Review, analyze, and research scan findings and coordinated remediation efforts in a timely fashion. Liaise with audit team to investigate and respond to Financial and/or IG Audits. Perform IT risk assessment and document the system security keys controls. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with NIST Cyber Security Framework standards Assist 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 Deliver evidence and feedback to assist the client with review of the audit Collaborate with Assessment team members and stakeholders on PCI mandated, line of business, and risk and control projects Handle all preparations & planning for upcoming PCI Audits Coordinated by scheduling the running of vulnerability/penetration test and oversee remediation of any vulnerabilities before engaging the external auditors Manage all requests from the external auditors during the audit engagements ensuring that timely responses are obtained Communicate status and escalate on a timely basis to maintain schedule Ongoing compliance activities such as antivirus, patching, and 6-month firewall rules review Update of all documentation, inventories, and diagrams, if a significant change has occurred Perform quarterly Access Control reviews (ex. removes any terminated employees) IT Security Analyst Fauquier Hospital - Warrenton, VA April 2016 to June 2017 Performed risk assessments of various technologies within client's environment Worked 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 Managed Service Organization Control (SOC) examinations, SOC1 and SOC2, in compliance with SSAE18 Coordinate internal and external regulatory IT and Security audits; meet with subject matter experts to facilitate reviews Assisted financial audits in reviews of IT general controls (ITGC) and computer systems security Worked with a Qualified Security Assessor (QSA) and SMEs on annual PCI assessments Contributed to PCI Services 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 Responsible for managing security vulnerabilities patching, application and (Operating System) 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 Junior IT Analyst Cigna - Bloomfield, CT February 2015 to January 2016 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. 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 Technical Support Wells Fargo - Durham, NC April 2013 to January 2015  Displayed courtesy and strong interpersonal skills with all customer interactions  Resolved customer complaints and concerns with strong verbal and negotiation skills  Resolved Remedy tickets on a daily basis  Coordinated with other IT groups for remediation of complex issues  Diagnosed and troubleshooted technical issues, including account setup and network configuration  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 Economics University of Bouake May 2001 Skills Hipaa, Information security, Iso, Iso 27001, Nessus, Nist, Pci, Sox, Firewalls, Network security, Networking, Tcp/ip, Security, Rsa, Ms project, Tcp, Unix, Ms office, Security plan, System security Additional Information Core Skills  Developed, reviewed and evaluated System Security Plan based NIST Special Publications  Experience with Governance, Risk Management, and Compliance (GRC) tools desired  Able to multitask, work independently and as part of a team  Strong analytical and quantitative skills  Aid in training and spreading PCI compliance awareness within the organization  Effective interpersonal and verbal/written communication skills  Able to review, understand, and rely on technical and software documentation and apply that knowledge into practice.  Reliable knowledge about popular information security compliance and privacy regulations such as PCI-DSS, SOX, HIPAA, ISO 27001, SOC 2 Type II, GDPR  Technical skills  Security Technologies: Retina Network

Security Scanner, Nessus, Anti-Virus Tools, Web Inspect, Nessus,  Systems: Unix-Based Systems, Windows 9X/NT/2000/XP,  Networking: LANs, WANs, VPNs, Routers/Switches, Firewalls, TCP/IP Software/Artifacts: MS Office (Word, Excel, PowerPoint, Access, Outlook), MS Project, RSA Archer

Name: Tyler Walker

Email: ucurtis@example.org

Phone: 335-277-8121x08185