Managing Consultant, IT Security & Compliance Managing Consultant, IT Security & Compliance Managing Consultant, IT Security & Compliance - NORTHHIGHLAND CONSULTING Atlanta, GA Work Experience Managing Consultant, IT Security & Compliance NORTHHIGHLAND CONSULTING - Atlanta, GA September 2015 to Present * Assess strategic and practical needs to ensure company maintains a world class information security and IT compliance program * Cultivate relationships to influence outcomes aligning company and client strategy and advancing company's position as a global leader in governance, compliance, data security, data privacy and innovation * Responsible for helping manage security projects for all of Blackboards products. Help create and implement a centralized security framework for the company to evaluate all its products and risk management. * Ensure the visibility, value, security, integrity and availability of electronic data and information throughout the enterprise and drive remediation and risk mitigation planning, risk assessments, security reviews, and internal assessments of key healthcare infrastructure to ensure compliance with policies, controls, and contractual obligations * Lead the development, implementation and management of key cross-organizational risk management and regulatory compliance initiatives and processes in this multi-state health care system. Key areas of ownership include: Conflict of Interest; Compliance Monitoring; Compliance, Privacy, and Security policies; Records Retention. * Develop and negotiate preferred information technology vendor contracts and manage key vendor relationships * Plan and Budget of the annual Security Assessment and staff recruitment. * Lead the implementation of security control defenses and services and vulnerability management * Assess, present and defend corporate security controls to regulators & clients Key Performance Indicator (KPI) and Key Risk Indicator (KRI) reporting. * Implementation and on-going management of Enterprise GRC System. * Oversee implementation and renewal of the NIST Cyber Security Framework (CSF), HITRUST, HIPAA, PCI-DSS engagement * Evaluate effectiveness of established controls to ensure gaps are identified and risk is within tolerance. * Interact with clients, vendors and suppliers, regulatory agencies, auditors and all areas of the company on risk and compliance issues and requirements * Communicate risk and compliance gaps or emerging threats to executive management by identifying potential compliance, operational, financial, or reputational

exposures and impacts with recommended remediation and communication plans for issue resolution Sr Analyst, Security & Compliance ACCENTURE - Atlanta, GA December 2009 to September 2015 * Lead and manage Vendor Security Risk Assessment. * Respond to RFP and RFI Requests. * HIPAA Privacy Rule Audit * Audit and Review Standard Operating Procedure for Routine Control activities like - Weekly Training Check for new hires, Badge Access Review, Weekly Job check review, Quarterly Logical Access Review, Weekly Backup Review, Financial and Engineering Reviews etc. * Lead Client policy and procedure documentation efforts for HITRUST and HIPAA. * Write and Review policy, procedure, evidence and artifacts with clients and offer remediations for all hitrust domains and requirements. * Represented and submitted clients evidence into HITRUST CSF Portal for hitrust certification. * Conduct ongoing internal HIPAA related audits to ensure regulatory compliance; obtain data from multiple sources and identify sample work lists (if applicable); provide results to areas audited and requested corrective actions plans; educate and act as a resource to departmental staff on regulatory guidelines and requirements. * Gap Analysis of security needs, processes and procedures and making recommendations. * Manage Vendor relations and responses for RFP within IT security, controls and compliance domains. * Responsible for auditing and advising on information security directives as mandated by HIPAA &HITRUST and NIST governing bodies. * Support requirements gathering and designed efforts of critical projects as needed. Perform yearly Risk Assessment. * Create an audit and testing program for HITRUST Common Security Framework (CSF) nineteen Domains for certification. * Negotiate a sample MyCSF Tool to obtain the 19 Domains to create the audit and testing program. * Use the HITRUST MyCSF tool to documents responses to control requirements. * Perform Domain pre-assessment reviews including interviews, walk-through and document reviews. * Help clients Write/update programs , policies and procedure documents in compliance and readiness for HITRUST and HIPAA certification. Senior Consultant AT&T - Atlanta, GA June 2006 to December 2009 * Built policy and procedure documents. * Provided security insight and expertise for customer-facing activities such as RFIs or periodic audits. * Managed third party security risk, providing oversight during vendor analysis/onboarding and periodic monitoring phases.

* Worked closely with technology and business groups to ensure security requirements are addressed. * Maintained information security awareness training and education programs. Test effectiveness of training thru periodic social engineering tests. * Managed Vulnerability Scanning tools Splunk. * Performed Vulnerability Assessment. Made sure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the Information and Information Systems. * Led formulation and assessment of vendor SIG Questionnaire using GRC tools like RSA Archer, Zen GRC etc. * Led and managed different stages in NIST Risk Management Framework Process * Led data migration, server decommission, disaster recovery and business continuity efforts * Provided internal security consulting for product development and IT operations projects across client organization. * Enterprise wide compliance management and HIPAA Privacy Rule Audit using ZenGRC. * Helped with PCI Audit. * Worked with clients on their projects to help them achieve HITRUST, HITECH, NIST, HIPAA and InfoSec compliance. * Investigated, documented, performed risk assessments and gathered information on data security requirements and recommendations. * Compliance within intrusion detection verticals and vulnerability management. * Analyzed vulnerability assessments to verify the strengths and weaknesses of a variety of operating systems, network devices, web applications, and security architectures utilizing commercial and open source security testing tools. * Evaluated technical and operational threats to the rights of customer users, review control implementation evidence, analyzing the effectiveness of safeguards, identified gaps and quantify risks. Senior Consultant COX COMMUNICATIONS - Atlanta, GA February 2003 to June 2006 * Maintained functional knowledge of all Information System standards, security, HIPAA, firewalls, and data encryption and updates technical skills through a variety of methods including individual research and group settings. * Worked with Conducted Assessment of various frameworks - PCI-DSS, HITECH, HITRUST, HIPAA. * Real-time server monitoring, real-time log forwarding, real-time syslog analysis, real-time alerts/notification of technology infrastructure. * Worked with Systems Administrators and Network Engineers to ensure detected vulnerabilities are resolved in a timely manner. * Work with cross functional teams to provide current Payment Card Industry Data Security Standard (PCI DSS) regulations to ensure

proper deployment of applications in the environment. * Participate in external security and penetration tests with vendors. Gap Analysis of security needs, processes and procedures and making recommendations. * Vulnerability scans: Monitoring Server Level Logs like source of IP traffic, security threat, network vulnerability, network traffic & spike; Monitor System logs for system performance, CPU usage &load, user access logs and App performance monitoring; & recommended solutions. * Conducted ongoing internal HIPAA related audits to ensure regulatory compliance; obtain data from multiple sources and identify sample work lists (if applicable); provided results to areas audited and requested corrective actions plans; educated and act as a resource to departmental staff on regulatory guidelines and requirements. * Conduct security assessment, following NIST Special Publication 800 guidance in support of obtaining an Authority to Operate for new systems or existing systems that undergo significant change. Coordinate security assessment activities with the appropriate system and security. Document comprehensive security assessment results that include a full description of the weakness and deficiencies discovered during assessment. Provide expertise and assistance in the development of continuous monitoring programs and plans. Configure vulnerability scanners, perform scans, analyze results and provide remediation assistance. Conduct technical vulnerability assessments and security impact analyses. Configure automated monitoring tools such as Splunk and Tripwire to perform centralized continuous monitoring activities. Collect, review and analyze audit logs for anomalies. * Managed Vendor relations, conducted vendor security risk assessment and responses for RFP within IT security, controls and compliance domains. * Responsible for auditing and advising on information security directives as mandated by PCI DSS, HIPAA and HITRUST governing bodies. * Patch management for virtual machines located in the AWS cloud - Linux & Window; Setup and Monitor SFTP/FTP, disc Space, operating system, network and security - TCP/IP, Firewalls. Daily monitoring & review of critical system logs using Splunk. * Actively work with numerous vendors and clients to conduct an organization wide Penetration/vulnerability testing. Conduct monthly vulnerability assessments using a Trustwave Vulnerability appliance to detect system vulnerabilities. * Consistently monitor systems for changes to critical file systems with Tripwire Enterprise. EMR

Integration Engineer JPS HEALTH NETWORK - Fort Worth, TX January 2001 to February 2003 * Maintained Epic Bridges Interface Monitor and Background Monitor and configured them to send emails and text alerts. * Performed go LIVE and support with various Epic project. * Error management, ticket resolution, troubleshooting or escalation and documentation of Epic Bridges Interface errors and training of staff using Epic and Help Desk support. * Configured bidirectional Ensemble interfaces between EPIC and downstream systems and external clients. * Led and oversaw the development, implementation and validation of bidirectional interfaces. * Analyzed HL7 data, including review of HL7 specifications and identifying required data translations * Monitored and reported progress to all stakeholders throughout lifecycle of project. * Developed and maintained strong strategic relationships with clients and vendors. * Performed message and system troubleshooting within InterSystems Ensemble and Epic Bridges as needed. * Designed/built/tested Ensemble routes, mappings across different HL7 messages types & versions, local & standard (SNOMED, LONIC, ICD-9/10) code set translations/lookup tables, Basic Security & privileges email and test alerts, Business Rules, transformation/mapping, Lookup Table/Translation Table custom & standard message formats based on business requirements & message specifications * Designed/built/tested all end to end interface ensuring business logic, HL7 requirements, connection connectivity and message handing/processing. * Worked with EMR Analysts to performed message validation/GAP analysis for inbound and outbound HL7 messages with respect to HIE requirements, establish VPN connectivity into the HIE & create/configure frontend Ensemble routes for the receiving & parsing of HL7 data into the HIE's downstream. * Extracted, transformed and Loaded different kinds of data set (HL7, X12, XML & Flat files) from clinical applications PM/EMR and ancillary applications to proprietary and downstream systems. * Created SSIS package to load data from HL7, 12XML Files, Excel, CSV file, Flat Files and SQL Server to SQL Server 2008/2012 by using Derived Columns, Condition Split, Data Conversion, Ole DB Command, Term Extraction, Aggregate, Pivot Transformation, Execute SQL Task and Script Component Task. * Scheduled Jobs for executing stored SSIS packages developed to update the database on Daily basis using SQL Server Agent. * Troubleshot Report and ETL processes failures

or warnings and provide technical support for all Reports and ETL- Data stage related issues. * Used SQL server reporting services (SSRS) to deliver enterprise and Web-enabled report to create reports that draw content from a variety of data sources. * Used SSIS to create ETL packages to Validate, Extract, Transform and Load data to Transaction and Data Warehouse. * Deployed created reports in various sources like Web browser, XML, PDF and Data Dumps. * Generated Tabular reports, Matrix reports, Conditional, List reports, Parameterized reports, Sub reports, Drill-Down reports, Drill-Through reports and Ad-hoc reports using SSRS. * Met business requirements by generating daily, weekly and monthly reports, and tested and validated for new reports. * Configured and deployed SSRS reports to Share point. * Implemented T-SQL queries such as Table, Views, Function, Stored Procedures and Triggers for load data and validation purpose. * Effectively used Normalization and De-Normalization techniques for both OLTP and OLAP systems in creating Database Objects like Table, Views, Function, Stored Procedures and Triggers, Joint, Constraints and Indexes. Education MBA Georgia Institute of Technology - Atlanta, GA MSc. in Computer Information Systems American University - Washington, DC Skills AWS (3 years), business continuity (3 years), database (2 years), EMR (2 years), Epic (2 years), HIPAA (10+ years), HL7 (2 years), Linux (3 years), Payment Card Industry (10+ years), PCI (10+ years), remediation (7 years), Risk Assessment. (9 years), RSA (3 years), Scanning (3 years), Security (10+ years), Splunk. (6 years), TCP (3 years), TCP/IP (3 years), testing (10+ years), Tripwire (3 years) Additional Information Areas of Expertise HITRUST * HIPAA * Business Continuity * Sarbanes-Oxley Act (SOX) * HITECH * PCI-DSS * ISO 27001/ISO27002 * Penetration Testing * Security Assessment & Authorization (SA&A) * FISMA * Network Security Controls Remediation * Internal Controls Design * COSO/COBIT * Risk Assessment * Risk & Access Management * Asset Security * Security Testing * Identity Management * Vendor Risk Mgmt. Software & Platform Programming Language: JAVA * SQL * Shell Scripting * XML Scanning Tools: IBM AppScan * Nessus * AppDetective * McAfee * Veracode * Cenzic * Qualys Operating System: Linux * Windows * Unix Database Security: Dbprotect * Imperva IDS Platforms: Sourcefire Snort Cisco * Juniper * Checkpoint * Palo Alto * Fortinet SOC technologies: RSA *Big Data * Qradar * Bluecoat * NetCache

* Solarwinds * ArcSight * Envision * LogRhythm Infrastructure Management: McAfee * Sophos Antivirus * ITSM Others: Tripwire * ServiceNow * Splunk * FileZilla * Tenable Security Center * SharePoint * Network Mapper * ServiceNow * HL7 * SharePoint * InterSystems Ensemble * EMR/EHR * EPIC * Salesforce * IDS/IPS * TCP/IP * SSIS/SSRS/SSAS * AWS * RDP * Microsoft SQL Server Management Studio

Name: James Villa

Email: pwolfe@example.net

Phone: +1-221-287-2714