

Senior IT Risk Specialist Consultant Senior IT Risk Specialist Consultant Senior IT Risk Specialist Consultant - Comcast Silver Spring, MD Work Experience Senior IT Risk Specialist Consultant Comcast - Silver Spring, MD October 2015 to Present Conduct regular analysis of security controls against compliance standards ? Continually review and enhance security policies and procedures ? Recommend solutions to eliminate, reduce, or mitigate risk, and communicate said solutions to both external parties and internal business stakeholders ? 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 Audits. ? Participate in closing meetings to present and discuss audit findings and recommendations. ? 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 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 ? Handle all preparations & planning for upcoming Audits ? Schedule/ run a vulnerability/penetration test and oversee remediation of any vulnerabilities before engaging external auditors ? Manage all requests from the QSA during the audit 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 ? Perform quarterly Access Control reviews such as removing any terminated employees Information Security Assessor (Contractor) Millennium Challenge Corporation - Washington, DC February 2014 to October 2015 Assisted business units

with understanding the risks associated with using a particular vendor and recommending solutions to reduce or eliminate risk. ? Prepared written reports after the completion of the assessment ? Categorized systems based on SP -800-60 in order to select the appropriate NIST recommended control SP 800-53. ? Developed, reviewed and updated Information Security System Policies and System Security Plans (SSP) in accordance with NIST, FISMA and industry best security practices. ? Performed Assessment and Authorization in compliance with FISMA/NIST Standards. ? Identified vulnerabilities, recommend corrective measures and ensure the adequacy of existing information security controls ? Reviewed and conducted audits to ensure information systems maintained the compliance baseline. ? Reviewed system-level documentation to ensure system security requirements, including SA&A is incorporated. ? Participated in the development and/or review of System Security Plans (SSP). ? Liaised with ISSO to update POA&M and to ensure that all findings from the SAR are entered into the POA&M to be remediated. ? Coordinated with appropriate personnel to run vulnerability scans on a regular basis and ensure timely remediation actions. ? Reviewed, analyzed, and researched scan findings and coordinated remediation efforts in a timely fashion. ? Liaised with audit team to investigate and respond to Financial and/or IG Audits. ? Performed IT risk assessment and document the system security keys controls. ? Reviewed and revised System Security Plan (SSP), System Security test and Evaluation (ST&E) Risk Assessment (RA), Privacy Impact Assessment (PIA), and the Plan Of Actions and Milestones (POA&M) ? Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk assessments (RAs), Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs) ? Conducted IT controls risk assessments (NIST 800-53A) including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with NIST standards ? Managed and coordinated Plan of Action and Milestone (POA&Ms) for DSS accredited approved classified systems. ? Assisted with the preparation and reviewing of Authorization to Operate (ATO) packages (i.e. SSP, RA, CMP, ISCP, DRP, IRP and PIA) for various systems IT Security Analyst Washington Hospital Center - Washington, DC May

2012 to February 2014 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 ? Coordinate internal and external regulatory IT and Security audits; meet 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. ? 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 a policies and procedures describing security requirements, guidance, and standards for organizational information systems and architecture Technical Support (Contractor) Choice Hotels - Rockville, MD April 2009 to May 2012 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 ? 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 ? Talked clients through a series of actions, either via phone, email or chat, until they've solved a technical issue ? Maintained and created detailed documentation through logging of support cases, e-mail and knowledge base articles for client and internal use ? Create and manage Service Requests, Incidents, and Problems through a ticketing system Education Associates of Applied Science in Applied Science Prince George's Community College - Largo, MD May 2011

Name: Stephanie Jimenez

Email: jvillarreal@example.org

Phone: 307.622.8585x0925