IT Security Analyst IT Security Analyst IT Security Analyst - Solvdata Systems Solution LLC Upper Marlboro, MD Security Assessment and Authorization professional, knowledgeable in risk management framework (RMF), systems development life cycle (SDLC), security life cycle, and vulnerabilities management using FISMA, and applicable NIST standards. Organized, Solutions-focused, deadline-focused, team oriented, work well independently, or in team providing all facets of computer supports with in-depth knowledge and understanding of numerous software packages and operating systems. A proven project and team lead with aptitude for good customer service, leadership, excellent communication (both oral and written), and presentation skills. Specialized in providing IT security expertise and guidance in support of security assessments and continues monitoring for government (FISMA & NIST) and commercial clients. Functional areas of expertise include: ? Assessment and Authorization (A&A) ? Certification and Accreditation (C&A) ? IT Security Compliance ? Vulnerability Assessment ? Network Vulnerability Scanning ? Information Assurance ? Systems Risk Assessment ? Systems Development Life Cycle ? Technical Writing ? Project Management and Support Work Experience IT Security Analyst Solvdata Systems Solution LLC July 2016 to Present - Provide security expertise and guidance in support of security assessments - Review authorization documentation for completeness and accuracy for compliance - Facilitate Security Control Assessment (SCA) and Continuous Monitoring Activities - Execute examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4 - Ensure cyber security policies are adhered to and that required controls are implemented - Validate information system security plans to ensure NIST control requirements are met - Develop resultant SCA documentation, including but not limited to the Security Assessment Report (SAR) - Author recommendations associated with findings on how to improve the customer's security posture in accordance with NIST controls - Update and review A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, POA&M, CPTPR, BIA, PTA, PIA, and more - Collect Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless - Upload supporting docs in the System's Artifact Libraries, Google Docs, and CSAM - Update, review, and align SSP to the requirements in NIST 800-53, rev4; so that assessments can be done against the actual requirements and not ambiguous statements - Manage vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network - Review SAR post assessment; create and complete POAM's milestones to remediate findings and vulnerabilities - Independently review complex security analysis of existing systems for compliance with security requirements - Monitor security controls post authorization to ensure continuous compliance with the security requirements HIPAA Compliance Officer HCR ManorCare August 2014 to May 2016 * supports the Security Assessment and Authorization process of the clients' systems as a technical Security Analyst * Maintains the HIPAA-compliant privacy program * Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. * Conducts risk assessments and develop HIPAA-compliant procedures * Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple assets across the enterprise network. * Carried out monitoring duties for the HIPAA Compliance hotline and calls. * Helped with updating IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. * Ensured that independent contractors are aware of the privacy requirements as per HIPAA Compliance Plan. * Performed risk assessments to identify the risk level associated with the findings. * Worked closely with HIPAA auditors to create comprehensive monthly audits for management and clients. * (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). * Monitored controls post authorization to ensure constant compliance with the security requirements * Reviewed artifacts regarding Plans of Action and Milestones (POA&M) created by ISSO before closing * Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). * Review and analyze Nessus Vulnerability and Compliance scans for possible remediation. * Assess systems of varying scope and complexity and comprised of various technologies. Provide weekly status reports on ongoing tasks and deliverables Location Captain Technician / Junior Cyber Security Analyst TOP

Group Technology - Largo, MD April 2012 to July 2014 Selected Responsibilities: - Reassembled machines after making repairs or replacing parts - Conversed with customers to determine details of equipment problems - Disassembled machines to examine parts, such as software, wires, gears, or bearing for wears or defects, using hand or power tools and measuring devices - Advised customers concerning equipment operation, maintenance, or programming - Calibrated equipment according to specification - Maintained parts inventories and order any additional parts needed for repair - Reinstalled software programs or adjust settings on existing software to fix machine malfunction - Maintained records of equipment maintenance work or repairs - Tested new systems to ensure that they are in working order - Installed and configured new equipment, including operating software or peripheral equipment. - Analyzed equipment performance records to assess equipment functioning - Provided continued maintenance and development of bug fixes and patch sets for existing web applications - Diagnosed and troubleshot Windows processing problems and applied solutions to increase company efficiency - Enforced and Review Data Flow interface program (HL7) - Monitored healthiness of client's host system and file servers - Reviewed SQL database - Supported and troubleshot over twelve system applications - Point of escalation for cases that cannot be resolved by the Level I Deskside technician. - Provided direct support to client's executive management personnel - Effectively communicated with Deskside Support Supervisor in regards to asset management and break/fix processes - Monitored and analyzed network/system performance, ensuring operational efficiency and maintenance of capacity Education Associate of Science in Information Systems Management Westwood College - Annandale, VA June 2010 Bachelor of Science in Accounting / Auditing Ondo State University March 2000 Skills Active Directory, HTML, Security, access, testing

Name: Laura Patel

Email: edwardsjerry@example.com

Phone: 393-286-4081x028