Information Security Analyst Information Security Analyst Information Security Analyst - Okinyx IT Consulting Hyattsville, MD Insightful, results-driven Information System Security Professional with experience in Risk Management Framework (RMF), Vulnerability Management, Risk Assessment, and System Development Life Cycle (SDLC). A proven project and team lead with aptitude for good customer service, leadership, excellent communication (both oral and written), and presentation skills. Authorized to work in the US for any employer Work Experience Information Security Analyst Okinyx IT Consulting January 2014 to Present Conducted security assessment interviews to determine the Security posture of the System and to develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Performed information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. Developed and conducted ST&E ( Security Test and Evaluation) according to NIST Special Publications. Provided recommendations in finding meeting with selection and implementation of controls that apply security protections to systems, processes, and information resources using the NIST family of security controls. Worked with support and security coordination team to ensure compliance with security processes and controls. Responsible for developing Security Authorization documents and also ensures System Security Plan, Security Assessment Plan, Plan of Action and Milestones (POA&M), Contingency Planning and artifacts are maintained and updated in accordance with NIST guidelines. Assist System Owners and ISSO in preparing Assessment and Authorization Package for IT systems, ensured management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53. Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60. Conduct Self-Annual Assessment (NIST SP 800-53A). Perform Vulnerability Assessment. Ensured that risks are assessed, evaluated and proper actions have been taken to limit their impact on the Information and Information Systems Performed library functions such as archiving and

filing of final SA and RA documents, Process/Procedure documents, inventory and maintenance. Validated remediated vulnerabilities. Information Security Analyst Midland Consulting Services July 2010 to December 2013 Ensured all systems are operated, maintained, and information is disposed in accordance with internal Midland security policies Developed System Security Plan (SSP), Security Assessment Report (SAR) and POA&Ms that were presented to the Designated Approving Authorizing Official (AO) in order to obtain the authority to operate (ATO) or (DATO). Conducted periodic IT risk assessment and reviewed IA controls for any deficiencies. Deficient controls are then reported to the Information System owner for appropriate mitigation actions Conducted security controls assessment to ensure controls are implemented to comply with standards Initiated and led information security awareness and training program in order to inform the employees of their roles in maintaining a matured security posture Contributed in weekly change management meetings in order to evaluate change requests (systems or application) that could lead to approval or denial of the requests, validated testing results from testing environments and promoted changes to production environment. Conducted weekly review of security logs and vulnerability scans on Operating Systems, Databases, and Applications. Identified, respond to, and report security violations and incidents as encountered to ensure that senior management is kept apprised of all pertinent security systems issues. Assisted with the development and updating of Midland security policies Conducted Risk Assessment on all Midland system changes Assisted in daily administration of security controls, compliance, monitoring and enforcement program. Ensured security logs and audit trails are reviewed in accordance with established schedules and procedure. IT Support Staff Enterprise Consulting, DC October 2009 to July 2010 Provided base level IT supports to both internal customers. Logged all complaints and inform customers about issue resolution progress. Assigned issues to appropriate support group for thorough support and prompt resolution. Supported users having data and network connectivity issue. Monitored network performance and troubleshoot problem areas as needed. Provided first level support to customers before escalation. Installed, configured and troubleshoot software. Cross-trained and provided back-up for other IT support representatives when needed. Displayed exceptional

telephone etiquette and professionalism in answering and resolving technical calls. Education Associate The Polytechnic 2010 Bachelor of Science University of Maryland Additional Information Skills Broad knowledge of Microsoft Windows (Windows server 2003-2008, XP, Vista and Windows 8) and UNIX platforms. Vast knowledge in all aspects of Security Authorization and Continuous Monitoring process using National Institute of Standard Publications 800-30, 800-37 Rev 1, 800-60, 800-53A, 800-53 Rev- 3 & 4, FIPS 199 FIPS 200, OMB A-130 App. III. Good knowledge of Federal Information Processing Standards (FIPS) 199 System Categorization, System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), Risk Assessment (Impact Analysis), Continuous Monitoring and the Plan of Action & Milestone (POAM). Broad knowledge of Information Security Risk Assessments, Implementation of Controls, Security Infrastructures and the entire Risk Management Framework. Knowledge of IT security architecture and design (Firewalls, Intrusion Detection Systems (IDS), Intrusion prevention system (IPS), Anti-virus, Virtual Private Networking, and Security Monitoring Tools). Proficient in the use of Vulnerability Scanning tools such as Retina Web Security Scanner, Retina Network Security Scanner, DBProtect, Tenable Nessus) and analyzes security reports for security vulnerabilities. Proficient in the use of Document Management Systems such as Enterprise Content Management Software (ECMS, SharePoint and Trusted Agent FISMA (TAF)). Knowledge of compliance standards such as PCI DSS, FISMA. Outstanding knowledge of hardware like Switches, Servers and Routers. Microsoft Office expert (MS Word, MS Excel, Outlook and PowerPoint) with excellent communication and writing skills. Excellent team player with Project Management skills.

Name: John Jones

Email: deborah90@example.com

Phone: +1-352-228-4010x44177