IT CONSULTANT (SECURITY ASSESSOR) IT CONSULTANT (SECURITY ASSESSOR) IT Security Engineer Marietta, GA Insightful and result oriented information system security professional with remarkable accomplishment in managing a wide scope of corporate IT enterprises while participating in service management, planning analysis, implementation of IT solutions as well as examining and testing security controls, hereby seeking opportunity to work in a professional environment where my 8 years of analytical and strong problem solving skills will be fully utilized as I remain committed to continuing education. Authorized to work in the US for any employer Work Experience IT CONSULTANT (SECURITY ASSESSOR) SPRINGHILL CONSULTING September 2015 to Present Assess implemented security controls using NIST SP 800-53 Rev 4 and NIST SP 800-53A Rev 4.   Re-evaluate the operating effectiveness of remediated security controls. Compile results from SRTM and generate Security Assessment Report (SAR).   Document findings and remediated actions in the Plan of Actions & Milestones (POA&M).   Draft walkthrough templates and questions for interviews, work-paper templates for documenting assessments, review current client reports and results, and planning memo.   Examine policies and procedure as well as security documentation such as System Security Plan (SSP) and Configuration Management Plan (CMP) to understand the system and its configuration.   Interview key security personnel such as ISSO and System Owner to understand key business processes tied to the in-scope systems and the risk posture of the computing environment.   Observe security control implementation as part of independent verification/ validation.   Plan security assessment by drafting assessment plan based on NIST SP 800-53A Revision 4.   Re-assess security controls based on information security continuous monitoring (ISCM) strategy.   Report on security assessment results to indicate security controls that need remediation.   Update Plan of Actions & Milestones (POA&M) with findings from ongoing security assessments.   Review SSP, SAR, POA&M, RAP, RP, CMP etc.   Review scan for critical and high vulnerabilities that need immediate remediation. RISK/COMPLIANCE ANALYST MIDLAND FINANCIAL SERVICES October 2014 to September 2015 Coordinated with key personnel such as system owner to perform oversee assessment and ensure timely remediation of resulting findings.   Assist the ISSO to conduct Privacy Threshold Assessment (PTAs), Privacy

Impact Analysis (PIAs) as required for existing systems. Perform periodic review of internal and security controls such as privilege access. Conduct control self-assessment of the IT environment to understand the current operating state. Review policies and procedures; business-line key processes; and internal controls; to identify and examine gaps or risks, to help formulate the future state of operations 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. Worked with support and security coordination team to ensure compliance with security processes and controls. Overseeing risk assessment for information systems and ensuring compliance with security requirements. IT SUPPORT SOMTECH SOLUTIONS February 2008 to June 2012 Assigned issues to appropriate support group for thorough support and prompt resolution. Provided base level IT supports to both internal and external customers. Logged all complaints and inform customers about issue resolution progress. Assist in training materials compilation both hard copies and soft copies format as well as PowerPoint presentations. Supported users having data and network connectivity issues. Monitored network performance and troubleshoot problem areas as needed. Provided first level support to customers before escalation. Provided back-up for other IT support representatives when needed. Ensured quality and effective trainings as scheduled Developed and coordinated trainings, workshops and seminars. Assisted with writing and presentation of business proposals to clients and follow-up with them. Education Bachelor of Arts in Philosophy University of Ibadan 2007 Skills POWERPOINT (4 years), SECURITY (3 years), INFORMATION SECURITY (3 years), SAR (3 years), SYSTEM SECURITY (3 years) Additional Information SKILLS Good knowledge of all aspects of Security Authorization and Continuous Monitoring process using National Institute of Standard Special Publications 800-30, 800-37 Rev 1, 800-60, 800-53A, 800-53

Rev- 3 & 4, FIPS 199 FIPS 200.   Knowledgeable in 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), Incident Response Plan, etc.   Broad knowledge of Information Security Risk Assessments, Implementation of Controls, Security Infrastructures and the entire Risk Management Framework.   Compile and analyze scan reports for weaknesses and vulnerabilities.   Proficiency in Document Management Systems such as Enterprise Content Management Software (ECMS, SharePoint and Trusted Agent FISMA (TAF).   Knowledge of compliance standards such as FISMA.   Proficiency in IT Service Management.   Great knowledge of Microsoft Office such as: MS Word, MS Excel and PowerPoint   Excellent communication and writing skills with the ability to work within stipulated time frame.

Name: Megan Hicks

Email: jacksonkelly@example.com

Phone: (425)697-5644