Information Security Risk Analyst Information Security Risk Analyst Information Security Risk Analyst - Apple Inc Austin, TX I have over ten (10) years of working experience with more than 5 years in Information Security system assessment, C&A and Risk Assessment of General Support Systems (GSS), I'm seeking IT Security Analyst opportunity in an organization with focus on Information Assurance, Risk Assessments, Certification and Accreditation (C&A), HIPPA Compliance Assessments and in Internal Control Audit engagements. I am task oriented and have a proactive attitude and personality towards work. Work Experience Information Security Risk Analyst Apple Inc August 2016 to Present I perform Third Party/Vendor Risk Assessment to assess the effectiveness of vendor's controls against ISO 27001. Performs security assessment to achieve PCI, HIPAA and FISMA compliance through the use of GRC tool. I document assessment work paper, audit findings, develop corrective plan of action and prepare assessment report. I review organizational policies, standard, procedures and guidelines in conducting IT control risk assessment. Assessing control gaps and auditing applications within the health system. Develop report after my audit findings, remediation, gap analysis and a corrective action plan in accordance to the organization's policy. Conduct risk assessment on new systems for business units within the company Monitor all in-place security solutions for efficient and appropriate operations. IT Security Analyst HID Global February 2015 to July 2016 Conducted kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60. Conducted security control assessments to assess the adequacy of management, operational privacy, and technical security controls implemented. Security Assessment Reports (SAR) were developed detailing the results of the assessment along with Plan of Action and Milestones (POA&M). Developed system security plans to provide an overview of federal information system security requirements and described the controls in place or to meet those requirements. 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). Prepared Security Assessment and Authorization (SA&A) packages to

ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. Performed vulnerability assessment, making sure risks are assessed and proper, actions taken to mitigate them. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Developed risk assessment reports. These reports identified threats and vulnerabilities. In addition, it also evaluates the likelihood that vulnerabilities can be exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level. IT Security Analyst Foreground Security June 2012 to November 2014 I met with the IT team to gather evidence, develop Test Plans, Testing Procedures and document test results. I worked with the Information System Security Officer and other Security analysts ensuring compliance with all security requirements and updates. I was partly responsible for implementing and following the Federal Information policies and guidelines throughout the whole Certification and Accreditation process for securing clients information system.(NIST SP 800 series). I created SSPs, ST&Es and POA&Ms. I developed Risk Assessment Reports that identify threats and vulnerabilities; and they also evaluate the likelihood that the vulnerabilities can be exploited. I assessed the impact associated with these threats and vulnerabilities and identified the overall risk.

I worked on Test plans, ST&E, SAR and develop remediation plans (POAMs). I assisted the System Owners in preparing Certification and Accreditation package for the Company's IT systems, making sure that Management, Operational and Technical security controls adhere to a formal and well established security requirement authorized by NIST SP 800-53. IT Coordinator NIIT - GH February 2009 to April 2011 I track priority problems faced by customers browsing the internet. I help students with computer desktop application issues. Organize regular trainings on the use Microsoft Office application for students. I organize IT tutorials or students. Education Bachelor's Skills SECURITY (5 years), NIST (3 years), TESTING (2 years), AUDITING (1 year), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (1 year) Additional Information Skill Profile IT risk assessments, Certification and Accreditation (C&A), 3rd party/Vendor security control assessment and IT Auditing. PCI, HIPAA, ISO and FISMA. Physical Security, General Computer

Controls, Application control Testing, Compliance Testing; Policies and Procedures, NIST 800-53rev 4, NIST 800-53A, NIST 800-30, NIST 800-37, NIST 800-34, NIST 800-18.

Name: Jennifer Ramos

Email: smarsh@example.com

Phone: 757.856.4178x850