

IT Security Analyst IT Security Analyst IT Security Analyst - Akamai Manassas, VA Work Experience

IT Security Analyst Akamai - Reston, VA July 2017 to Present Develop and review security artifacts such as SSPs, POA&Ms, Security Control Assessments, Configuration Plans (CPM), Contingency Plans (CP) and Incident Response Plans. Review implementation statements and supporting evidence of security controls to determine if the systems are currently meeting the requirements. Review Nessus vulnerability scan results for mitigation actions and help the system stakeholders to create and maintain POA&Ms for the deficiencies identified in the scan results. Work with the Security Control Assessors (SCA) team to assess implemented security controls to determine effectiveness by interviewing, examining and testing. Develop Security Assessment Report (SAR) identifying the results of the assessment along with FISMA and NIST SP 800-53 rev 4 controls. Responsible for developing Rules of Behavior (RoB), Interconnection Security Agreement (ISA) and Memorandum of Understanding (MoU) for system assigned to me. Monitor controls post authorization to ensure continuous compliance with the security and regulatory requirements. Cyber Security Analyst EvoSwitch, VA September 2015 to May 2017 Created, monitored and updated the status of POA&Ms to ensure weaknesses are resolved in accordance to their scheduled completion dates. Assisted with Security Categorization of systems (using FIPS 199), Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA) guidelines with stakeholders. Ensured that security policies, procedures, and recommendations comply with FISMA, NIST, organizational guidelines. Developed and reviewed system security artifacts such as CP, IRP, PTA, PIA, MOU/ISA and SOPs for accuracy and compliance with NIST 800 guidelines and agency security requirements. Supported the review of all Cloud Service Provider (CSP) documentation for compliance and work with stakeholders until the cloud system documentation meets FedRAMP requirements. Managed findings in POA&Ms that are the result of non-compliant tests of security controls, vulnerability scan reports or continuous monitoring of information systems. Hosted meetings and presentations with stakeholders on the operational security posture for the systems in their purview and on security related policies. Information Analyst Ernst & Young - Washington, DC April 2013 to September 2015 Helped to prepare a comprehensive Authorization To Operate

(ATO) packages for submission to the Authorization Official (AO) Created and maintained security checklists, templates and other tools to aid in the A&A process. Performed security control assessments using NIST 800-53A guidance and as per continuous monitoring requirements. Developed System Security Plan (SSP) to provide an overview of system security requirements and described the controls in place by information system owners. Conducted follow up meetings to assist ISSOs, System Owners and Authorizing Officials to close remediated POA&M items. Participated in meetings to discuss vulnerabilities and potential remediation actions with system owners. Education Bachelor of Science in Information Technology Kwame Nkrumah University of Science and Technology

Name: Melissa Garrison

Email: latoyabaker@example.com

Phone: 443-487-4185x8638