IT Security Analyst IT Security Analyst Gaithersburg, MD Insightful, result driven Cyber analyst with over 4 years of experience in implementing and reviewing ATO packages and remediating POAMs. Thrive under pressure in fast pace environments while directing multiple projects from concept to implementation and working to prevent cyber-attacks in business and corporate settings. Authorized to work in the US for any employer Work Experience IT Security Analyst CYLOC SOLUTIONS - Lanham, MD August 2015 to Present Develop and maintain Plan of Action and Milestones (POA&MS) of all accepted risks upon completion of system (C&A) Conduct FISMA-based security risk assessments for various government contracting organizations and application systems - including interviews, tests and inspections; produced assessment reports and recommendations; conducted out-briefings. Assessments conducted following NIST 800 processes and controls. Reviewed and updated some of the system categorization using FIPS 199, Initial Risk Assessment, E-authentication, PTA, PIA, SAR, SSP, SAP& POA&M. Conducted meetings with the IT team to gather documentations and evidences (Kick-off meeting) about their control environment. Developed and conducted SCA (Security Control), Security Assessment plan (SAP) according to NIST SP 800-53A. Develop NIST Compliant vulnerability assessments, technical documentation, and Plans of Action and Milestone (POA&M), and address system weaknesses. Generate, review and update System Security Plans (SSP) against NIST 800-18 and NIST 800 53 requirements. Contribute to initiating FISMA metrics such as Annual Testing, POA&M Management, and Program Management. Supporting clients in creating Standard Operating Procedures (SOP) as guidance through Risk Management Framework. Sound understanding and experience with NIST Risk Management Framework (RMF) process. Document and review System Security Plan (SSP), Security Assessment Report (SAR), Security Plan of Action and Milestones (POA&M), Authorization letter/memorandum (ATO). Assist with review of policy, security alerts, guidance, regulations and technical advances in IT Security Management. Generate, review and update System Security Plans (SSP) against NIST 800-18 and NIST 800 53 requirements. Performed Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), E-Authentication with business owners and selected stakeholders. IT Security Analyst SKILLZPORT CONSULTING LLC -

Columbus, GA October 2013 to June 2015 Provide continuous monitoring support for control systems in accordance to FISMA guidelines and conduct FISMA-based security risk assessments. Assisted System Owners and ISSO in preparing Authorization and Accreditation package for company's IT System, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST 800- 53R4. Managed client delivery teams providing HIPAA, PCI-DSS, assessments & incident response and provide technical expertise and support to clients' engagements and the implementation Ensure clients are in compliance with security policies and procedures following NIST 800-53 and NIST 800-53A. Perform Vulnerability scanning and prepare Assessment Reports (VAR). Perform Comprehensive Security Control Assessment (SCA) and prepare report on management, operational and technical security controls for audited applications Perform Security Categorization (FIPS 199), review and ensure Privacy Impact Assessment (PIA) document after a positive PTA is created Conduct risk assessments regularly; ensured measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37. Document and Review security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for various government agencies. Conduct risk assessments regularly; ensured measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37. Perform specific quality control for packages validation on the SP, RA, RTM, PIA, SORN, E-authentication and FIPS-199. Schedule and attend weekly meetings for audits, POA&M findings and after action review. Expertise in National Institute of Standards and Technology Special Publication (NIST SP) documentation: Performed assessments, POAM Remediation, and document creation using NIST SP 800-53a and NIST SP 800-53 Rev 4. Education Bachelors of Science in Health Administration in Health Administration University of Ghana Skills FEDERAL INFORMATION SECURITY MANAGEMENT ACT (3 years), FISMA (3 years), NIST (3 years), Risk Management (2 years), security (3 years) Additional Information SKILL

SUMMARY Experience working with NIST SP 800-53 REV 4 Experience with NIST Risk Management Framework (RMF) Hands on experience in Risk Management Framework (RMF) Processes and FISMA. Expertise in the assessment of security controls using NIST SP 800-53A Good communication and writing skills. Great experience with ISO 2700 Series Great experience with PCI DSS Compliance SKILLS FISMA, NIST SP SERIES, TCP/IP, SPLUNK, NESSUS

Name: Elizabeth Bowman

Email: katelyn58@example.org

Phone: 849-566-3668x961