Senior Cyber Security Policy & Compliance Analyst / Information System Security Engineer Senior Cyber Security Policy & Compliance Analyst / Information System Security Engineer Senior Cyber Security Policy & Compliance Analyst / Information System Security Engineer - Booz Allen Hamilton Woodbridge, VA An Information System Security Officer (ISSO) and Cyber Security Analyst with about 5 years' experience in Cybersecurity, Compliance Management, Information Assurance (IA) and security assessment documentation to support various systems to achieve their Authorization to Operate (ATO). Liza is proficient and has sound understanding of all phases of the Risk Management Framework (RMF) process including IT security controls assessment for test of design and operating effectiveness, documentation and compliance with FISMA and NIST 800 series. Work Experience Senior Cyber Security Policy & Compliance Analyst / Information System Security Engineer Booz Allen Hamilton November 2018 to Present Support meetings with client working groups to identify initiatives and needs in regard to the ATO Support client's ATO process and authorization artifacts using the Governance Risk & Compliance (GRC) implementation tool Review results of vulnerability scans to ensure client system is devoid of critical and high vulnerabilities Review systems to identify potential security weaknesses and recommend improvements to amend vulnerabilities, implement changes, and document upgrade Assist with creating strategies to achieve cyber-related objectives including due dates, critical paths, and milestones in alignment with goals Develop and maintain client's security policies and procedures that include evaluations and compliance with security measures such as Access Control, Configuration Management, Incidence Response, Privacy Threshold Analysis / Privacy Impact Analysis etc. Cyber Security Senior Analyst Deloitte & Touche LLP June 2016 to November 2018 Assisted with creating strategies to achieve cyber-related objectives including due dates, critical paths, and milestones to exceed project goals Continued to measure remediation over time and help prioritize client's cybersecurity projects Monitored, evaluated, and assisted with the maintenance of assigned security systems and assist with the review and definition of security requirements Assisted in ensuring that vulnerabilities identified in client's IT security POA&M database are addressed promptly by working with system owners and managers Assessed the

information technology systems, security regulatory risk management and security vulnerabilities; using the NIST SP 800-series and FIPS Conducted security control assessments and control test of design and operating effectiveness to ensure adherence to customer specific security policy, procedures and industry standards Scheduled, tracked and managed quarterly Plan of Action & Milestones (POA&M) review process Built and nurtured positive working relationships with clients with the intention to exceed client expectations Complied with security systems and respond to internal and external customer request for computer security information and reports Provided support for system reviews to determine if they are designed to comply with established standards Facilitated use of technology-based tools or methodologies to review, design and/or implement products and services Information System Security Officer / IT Controls Assessor Deloitte & Touche LLP November 2015 to June 2016 Conducted several Security Controls Assessments (SCAs) from the planning phase through to client follow-up for several systems Assessed design and operating effectiveness of IT Controls for several information system boundaries using corresponding System Security Plans (SSP), according to the National Institute of Standards and Technology (NIST) 800-53 publications Performed Federal Information System Management Act (FISMA) compliance audits Identified control gaps and created Plan Of Action & Milestones (POA&Ms) reports for vulnerable systems Assisted in the development of appropriate information security policies, standards, procedures, checklists, and guidelines using generally-recognized security concepts tailored to meet the requirements of the organization Evaluated identified vulnerabilities and risks, working with business owners, risk management, and IT leaders Identified tasks and controls necessary to remediate identified risks and vulnerabilities; negotiated dates for remediation to be complete Prepared and updated comprehensive Certification & Accreditation (C&A) packages Tracked progress on remediation of identified risks and vulnerabilities and provide appropriate reporting to constituents Conducted Security Impact Analyses (SIAs) on changes that required them Risk & Compliance / Senior IT Auditor Morgan Franklin Consulting March 2015 to November 2015 Communicated results of audits and reviews to management and work with management to develop remediation plans Reviewed deficiencies and formulated solutions for implementation

Planned, performed and documented results of internal audits and reviews Recommended improvements to internal controls to ensure/enhance compliance with company policies. Provided front-line support for all information security related issues, advising on security policy compliance, handling data confidentiality issues, monitoring and responding to emerging threats, and security compliance projects (e.g. FISMA). Worked with appropriate system managers and operations personnel to remediate identified vulnerabilities. Followed up with management to confirm remediation plans are completed as scheduled Assisted Managing Directors, Senior Managers and Managers with various initiatives related to business development and practice development Reviewed junior staff's progress to ensure compliance with audit program and professional standards. Reviewed timelines and budget to ensure compliance with customer needs Mitigation of network and operating systems vulnerabilities and recommending compensating controls Senior IT Auditor PerfectNet Inc June 2014 to March 2015 Performed audit planning, conducted walkthroughs, and assessed the internal control environment through control testing Ensured that policies and procedures were implemented and well documented Performed internal reviews and identified compliance problems that called for formal attention. Provided day-to-day execution of audit engagements and projects such as SOX, compliance audit, and operational audit Performed Information Technology audits (e.g. information security, change management, computer operations) for clients from various industries (manufacturing, technology, education, healthcare, etc.) Documented clients' internal controls (both IT controls and some business cycle controls) Prepared work papers supporting audit results Prepared audit reports detailing results of audits and provided written recommendations to clients based on results Liaised with external auditors for remediation of findings Performed Tests of Design (TODs), Tests of Effectiveness (TOEs) of Key defined control activities and tested for Audit Readiness Education BS in Computer Information Studies and French University of Ghana May 2011 Certifications/Licenses Security+ Additional Information AREAS OF EXPERTISE ? C&A Process ? NIST 800-53 ? NIST 800-37 ? FISMA Compliance ? IT Security Controls Assessment ? Standards Policies and Procedures ? Risk Management Framework (RMF) ? DoD Directive 8570 Standard ? MCCAST ? eMASS ?

RiskVision ? SharePoint ? System Security Plan Updates ? Gap and Risk Analysis ? Control Implementation Guidance ? CNSSI-1253 Standards ? Authorization-To-Operate (ATO) ? COBIT

Name: Courtney Walker

Email: cooperevan@example.net

Phone: +1-523-773-8067x5647