

Advisory Project Specialist/Sr. Consultant Advisory Project Specialist/Sr. Consultant Advisory Project Specialist/Sr. Consultant Woodbridge, VA Work Experience Advisory Project Specialist/Sr. Consultant Deloitte & Touch - Arlington, VA 2016 to 2019 Conduct IT controls risk assessments that include reviewing organizational policies, standards and procedures Provide a variety of IT advisory services related to Certification and Accreditation, internal control, risk management, IT controls and related standards (DISA, FISCAM, FISMA, NIST, COBIT) Utilize established test procedures to test IT controls to assess the design and operating effectiveness of general and application controls Develop and submit management reports, i.e. monthly executive report, Bi-weekly status reports and plans of action and milestones (POA&M) for DHS Assist with the development of an Authority to Operate (ATO) package that contains objective information for the client to make an informed Authorization decision Identify and evaluate complex business and technology risks, internal controls which mitigate risks, and related opportunities for internal control improvement Apply risk-based control framework to identify and to evaluate complex business and technology risks, internal controls which mitigate risks, and related opportunities for internal control improvement Support internal team as well as system and control owners in development and maintenance of a remediation plan with milestones, dependencies, timelines, budget, project management, and communications for known IT control weaknesses Responsible for reviewing and validating supporting evidence in regard to following up on significant findings for DHS IT Security Analyst Pentracop Technologies - Washington, DC August 2011 to October 2016 Schedule, plan, and participate in internal auditing in accordance with HIPAA, NIST, and PCI standards Perform security assessments; design reviews; and provide guidance on new technologies for the customers. Develop POA&M (Plan Of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Perform Certification and Accreditation (C&A) documentation in compliance with company standards Perform Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), e-Authentication with business owners and selected stakeholders Author or coordinate the development of other required system security plans: Configuration management (CM), Contingency Plan (CP), Continuity of Operations

(COOP), Disaster Recovery Plan (DR) and Incident Response Plan (IRP). Conduct Systems Risk Assessment through Risk Analysis, assessed the various Assets within the systems boundaries and rigorously identifying all the possible vulnerabilities that exist within the system. Developed the audit plan and performed the General Computer Controls testing of Information Security, Business Continuity Planning, and Relationship with Outsourced Vendors. Performing Vulnerability scanning using Nessus. Ensure all security-related incidents are documented and reported to the ISSM and Security Officer. Perform systems security audit on a weekly basis to detect unauthorized activities and ensure systems maintain security compliance. Perform Security Control Assessment (SCA) according to NIST SP 800-53A. Document and conform to processes related to security monitoring, patching and incident response. Manage the organization's RMF continuous monitoring tool and complete specific control activities. Maintain security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Security Analyst Mid Atlantic - Alexandria, VA August 2009 to July 2012. Guided System Owners and ISSOs through the Certification and Accreditation (C&A) process, ensuring that management; operational and technical controls for securing either sensitive Security Systems or IT Systems are in place and are followed according to federal guidelines (NIST 800-53). Applied security risk assessment methodology to system development, including threat model development, vulnerability assessments and resulting security risk analysis. Provided support and guidance through the phases of FISMA C&A, including monitoring of the C&A artifacts compliance, annual self-assessment (NIST SP 800-53A guidelines) and quarterly self-assessment completion using NIST SP 800-26 guidelines. Created or updated the System Security Plan and conducted an Annual Self-Assessment. Applied knowledge of C&A policies, guidelines, and regulations in the assessment of IT systems and the documentation and preparation of related documents. Executed vulnerability assessment and vulnerability scanning tools such as Acas, Metasploit, on a challenging and complex systems-wide information assurance/ system security environment requiring analysis of user, operational, policy, regulatory, and resource demands. Assesses and mitigates system security threats/risks throughout the program life cycle;

determines/analyzes and decomposes security requirements at the level of detail that can be implemented and tested; reviews and monitors security designs in hardware, software, data, and procedures,    Worked with C&A team members and senior representatives to establish and define programs, resources, schedules, and risks.    Conducted the IT Risk Assessment and documented the controls. IT Help Desk Specialist/ security Officer The Fairfax - Alexandria, EG January 2005 to July 2010 VA    Provided support for application software installation and use.    Act as an advocate for the office in the resolution of any and all computer-related problems or issues.    Assisted in the delivery, installation, and use of systems and services, (e.g., Washington to district office connectivity, Internet, remote access, etc.).    Provided front line phone, Live Chat, and Remote Desktop support, may be required to resolve requests via on-site visit(s). Provide Hardware/Software Installation and Setup support.    Troubleshoot and solve common network issues using physical and logical diagnostic tools.    Troubleshoot and solve common Microsoft based platforms (Windows XP, Windows 7, Microsoft Office Suite, Etc.) and common hardware used throughout FBCH (Dell, Lenovo, and HP)    Troubleshoot basic technical issues over the phone or by logging in remotely to their computers    Escalate serious technical issues to engineering staff by relaying information from customer to help diagnose the problem. Education Bachelor of Science SHENANDOAH UNIVERSITY 2008

Name: Catherine Mitchell

Email: eadkins@example.com

Phone: +1-833-810-4864