First Information Technology Services

Security Control Assessor

Job Description

First Information Technology Services (FITS) seeks a Security Control Assessor (SCA) to support a federal government client by conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls.

Security Control Assessors:

- Provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operational and recommend corrective actions to address identified vulnerabilities; and
- Prepare the final security assessment report (SAR) containing the results and findings from the assessment.

Required Qualifications

- Active Secret clearance
- 5-7 years of experience as a cyber security control assessor or similar role
- Expert knowledge of U.S. Federal Information Assurance (IA) and the Risk Management Framework (RMF), including knowledge of related best practices from FedRAMP, NIST, and other sources.
- Exposure to IT Security Engineering Life Cycle and Release Management
- Extensive experience with Assessment and Authorization (A&A), Certification and Accreditation (C&A), FISMA, FedRAMP, NIST SP 800-53, RMF
- Exposure to Risk and Issue Management and Mitigation
- Strong written, verbal communication and presentation skills
- Ability to interface with customers and articulate technical content to a non-technical audience.

Essential Duties and Responsibilities

- Support NIST RMF-based Assessment and Authorization (A&A) activities.
- Monitor and prepare required actions and documents pertaining to the A&A of the system throughout its lifecycle, to include security evaluation findings and residual risks.
- Conduct comprehensive reviews of security authorization documents to ensure the appropriate NIST security guidelines were used during the assessments and the selections of security controls are relevant to the confidentiality, integrity, and availability of the systems.
- Ensure required security authorization activities are completed and the results are documented in the DHS Information Assurance Compliance System IACS / XACTA tool.
- Review and process Interconnection Security Agreements (ISAs), Policy Waivers, Approval to Test (ATT), and Interim Approval to Operate (IATO) documents.
- Review IS security plans and other A&A documents for all applications to determine if DHS mandated procedures and tasks are followed, such as using IACS.
- Assist the Government in preparing a written justification, when appropriate, to obtain a written waiver of policy for mandated security features.

Security Control Assessor

- Ensure that assigned systems/applications meet the minimum DHS A&A standards before a recommendation is made to the CISO for Authorization.
- Attend Compliance Team meetings and provide reports in the approved format on the status of requested activities.
- Update and upload all pertinent information for all systems within the DHS Headquarters FISMA portfolio repository.
- Update relevant FISMA Compliance SOPs on a quarterly basis.
- Provide guidance and support for all assigned Security Authorization activities.
- Conduct Security Authorization entrance conferences.
- Develop a preliminary Security Assessment Report (SAR).
- Create the CSS Plan, including rules of engagement (ROE) for each major application, information system, or GSS undergoing authorization.
- Document the results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, analyze findings, and develop risk mitigation techniques to address weaknesses.