SENIOR INFORMATION SECURITY COMPLIANCE ANALYST

The Senior Information Security Compliance Analyst will support the client in the development, oversight, and maintenance of FISMA compliant security programs. This includes the monitoring and maintenance of security controls, draft processes & procedures, creation of Security Authorization (formerly C&A) packages, oversight of monthly Continuous Monitoring reports which include vulnerability scanning, interviews and system testing. The candidate would be expected to work with a variety of stakeholders, including system owners, implementation engineers, 3rd-party auditors, and the organizational security team to develop deliverables, to recommend security solutions, and to maintain the existing Authority to Operate (ATO) for the client's systems and implement new ATOs for other emerging systems and platforms (e.g., SalesForce.com).

Roles and Responsibilities

- Support the analysis and review of information security programs and systems to ensure compliance to federal security policies.
- Provide Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) guidance and support. Specific standards include NIST 800-53 rev. 4, NIST 800-53A rev 4, FIPS 199, NIST 800-37, NIST 800-137.
- Independently develop a variety of Security Authorization deliverables including: System Security Plans (SSP), Security Assessment Reports (SAR), Risk Assessment Reports, Privacy Impact Assessments (PAI), Annual Assessments, Contingency Plans, FIPS 199 Security Categorizations, Plan of Action and Milestones (POA&M), etc.
- Experience migrating FISMA Authorizing Official (AO) package from revision 3 to revision 4.
- Analyze and review existing processes and procedures to determine areas of possible improvement that will lead to gains in efficiency and security.
- Develop, review and monitor compliance with organizational security policies.
- Draft and finalize processes & procedures for compliance with FISMA and NIST 800-53 rev4.
- Monitor, track and report on the status of POA&M items. Prepare monthly ISCM (NIST 800-137) packages for submission to AO.
- Proactively manage risks, and systematically resolve or escalate issues in a timely manner.
- Monitor industry trends for changes in physical and cyber security challenges and implement planning, policy and procedure changes in response.
- Contribute to industry and government forums that develop industry guidance and regulations regarding security practices.

Requirements

- Experience with FedRAMP security controls for an Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud paradigms.
- FISMA experience with Salesforce and other SaaS providers.

- Experience with PCI DSS SAQs and SASE16 SOC1 reports.
- Thorough understanding of the NIST risk management framework and related industry best practices.
- Experience with PCI (Payment Card Industry) Security Standards.
- Must have past experience and be capable of independently developing Security Authorization deliverables. Migrating from NIST 800-53 rev3 to rev4 is essential.
- Broad background in information assurance (IA) activities required to facilitate and coordinate IA activities for a project to obtain an Authorization to Operate (ATO).
- Working knowledge of system and network security engineering best practices, operating systems and application auditing.
- Strong written and verbal communication skills as well as a dynamic, creative personality.
- Ability to work calmly during stressful circumstances.
- Strong planning and task management skills.
- Ability to work in collaboration with a variety of stakeholders to identify and discuss issues.
- Ability to work in fast paced environment managing multiple projects driven by multiple
- deadlines.
- Proven capability to achieve results in a fast paced environment managing multiple projects driven by multiple deadlines.

Education and Experience

Applicant must have

- Bachelor's degree or equivalent experience in an information technology or information security discipline.
- CAP Certification essential. Security Certifications preferred (e.g. CISSP, GIAC, CISA, CISM).
- 5+ years of experience in Information Assurance (IA), Information Security (InfoSec)
- 3+ years of experience auditing under FISMA requirements

Please Contact: Recruiter@coremax.com