INFORMATION TECHNOLOGY RISK & COMPLIANCE DIRECTOR

The Information Technology Risk and Compliance Director 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, recommend security solutions, and 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.
- Migrate 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.
- Provide thought leadership to industry and government forums related to compliance practices, issues and challenges in the financial services industry.
- Monitor industry trends for changes in compliance challenges and implement organization planning, policy and procedure changes in response.
- Contribute to industry and government forums that develop industry guidance and regulations regarding compliance practices.
- Contribute to industry and government forums that develop industry guidance and regulations regarding security practices.

Requirements

- Experience with FFIEC IT Examination Handbook and compliance with privacy regulations (e.g. GLBA, HIPAA, Fair Information Practice Principles [FIPP], FTC Red Flags, etc.).
- Knowledge of ISO 27000 family of standards to keep information assets secure; especially ISO 27001:2013 Information Security Management system (ISMS).
- 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.
- Experience with FISMA Information Security Continuous Monitoring (NIST SP 800-137).
- FISMA experience with Salesforce and other IaaS/ SaaS providers.
- Experience with PCI DSS SAQs and SASE16 SOC1 reports.
- Thorough understanding of the NIST Risk management framework (NIST SP 800-30 & NIST SP 800-37) and related industry best practices.
- Experience with PCI (Payment Card Industry) Data Security Standards (DSS).
- Must have past experience and be capable of independently developing Security Authorization deliverables suitable for an ATO and migrating from NIST 800-53 rev.3 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.
- Some travel required

Education and Experience

Applicant must have:

- B.S. degree in Computer Science or equivalent experience. Master's degree preferred.
- Security Certifications (e.g. CISSP, GIAC, CISA, CISM). CAP Certification or equivalent experience essential.
- Experience in the Financial Services, Regulatory, or consulting services industries is highly desired.
- 15+ years of relevant business and technology experience, to include at least 10+ years of experience in Information Assurance (IA), Information Security (InfoSec).
- 7+ years of experience auditing under FISMA requirements; 5+ years of experience auditing under PCI DSS requirements and knowledge of CJIS requirements. Experience with System Security Plans (SSP) using NIST 800-53 Rev 4 is a must.

Please Contact: Recruiter@coremax.com