Job ID: S-GRC-001
Job Title: Senior Cybersecurity Analyst – Governance, Risk and Compliance (GRC) Lead
Date: 06/21/2020
Location: Manassas, Virginia (Primary), Wash DC (Secondary)

At Cybereye, we are a small business with a laser sharp focus on bringing high quality cybersecurity assessment and assistance services to organizations that are embarking on a risk and compliance journey. We are building a team of driven, talented, and thought leading consultants that share our desire to become a trusted partner to our clients and fully vested in their business outcomes. Cyber security is as much a business challenge as it is a technical challenge, and we bring our clients solutions for both. Cybereye was founded by an expert in Governance, Policy and Compliance, built on a foundation of 18 years cyber strategy consulting for large corporations, military clients, and state and local governments. If you are looking for an entrepreneurial environment, crave a fast-paced setting, thought provoking work, and are looking for an opportunity to expand your cyber skills in new specialty areas, you may be the right candidate to help Cybereye bring our client's business to the next level.

Job Summary

Provide Cybersecurity Governance, Risk, and Compliance (GRC) services to assist our clients with planning, implementing and maturing their cybersecurity program activities in alignment with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). A qualified candidate will be responsible for the following primary duties and responsibilities, but are not limited to:

- Design and develop GRC processes, procedures, and metrics
- Work with test team to document risk based on system architecture diagrams and vulnerability reports
- Build a Cybersecurity Awareness & Outreach Program
- Lead a team of junior and mid-level cybersecurity analysist by providing templates, quality standards, coaching and mentoring

Job Description

Key Role:
Provide Cybersecurity Governance, Risk, and Compliance (GRC) services to assist our clients with planning, implementing and maturing their cybersecurity program activities in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. A qualified candidate will be responsible for the following primary duties and responsibilities, but are not limited to:

- Develop of a policy framework, and independently author policies that encompasses all NIST Cybersecurity Framework (CSF) categories and topics
- Design, develop and implement governance processes, procedures, and metrics to ensure adequate enforcement and oversight of the organization's cyber activities in conformance with written policies
- Perform and document organizational risk assessments using system architecture diagrams, vulnerability reports, and an understanding of the threat vectors and the operating environment
- Design a Cybersecurity Awareness & Outreach Program, complete with branding materials, a communication strategy and creative development of awareness products to create a "cyber aware" culture.

Basic Qualifications:

- 10+ years of experience developing or assisting clients with the implementation of cybersecurity policy and regulatory compliance
- 8+ years of experience leading a team in the Assessment and Authorization (A&A) process, in accordance with NIST Risk Management Framework
- 2+ years assessing cloud-hosted systems for the purposes defining security control responsibility between providers and consumers,
- 2+ years of experience generating, analyzing, and reporting GRC program metrics using Microsoft Excel

Submit Resume to kim.maurer@cybereyesolutions.com

- Experience independently authoring complex business process documentation
- Experience reviewing system architectures, decomposing systems into testable components, and selecting applicable configuration standards to achieve NIST 800-53, NIST 800-171, NIST CSF, Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) or International Organization for Standardization (ISO) standards and security requirements.
- Experience with risk assessment and mitigation, Information Assurance principles, NIST special publications
- Possession of excellent oral and written communication skills
- B.A. or B.S. degree in Information Technology (IT) related field (may be waived for equivalent experience)
- Professional security certification such as CISSP, Security+, CEH, ISSEP (alternative certifications will be considered)

Preferred Qualifications:

- Experience with Tableau, Splunk, or Power BI for security data analytics
- Experience with ServiceNow for GRC workflow management and tracking
- Experience with RedSeal for networking mapping and vulnerability impact assessments
- Experience generating RMF A&A Packages or overseeing a team and resolving challenges
- Experience with both commercial and government organizations (e.g., Legislative Branch, DoD, or State and Local

Clearance:
Applicant selected may be subject to a security investigation and may need to meet eligibility requirements for access to classified information.

Submit Resume to kim.maurer@cybereyesolutions.com