Job ID: J-GRC-001
Job Title: Junior Cybersecurity Analyst – Governance, Risk and Compliance (GRC)
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 support services to assist our clients with their cyber security activities. Provide research and analysis on a broad range of cybersecurity topics, and prepare technical documentation to support team assessment of risk and prepare recommendations to our client on risk to the organization. A qualified candidate will be responsible for the following primary duties and responsibilities, but are not limited to:

- Participate in a team helping to document processes, and procedures to protect highly confidential data
- Research and analyze the specific requirements associated with National Institute of Standards and Technology (NIST) in order to assist the team with plans to satisfy each requirement
- Attend strategy meetings and capture key notes, action items, and next steps
- Assist Team Lead in the development of executive briefings and project milestone reports
- Participate Cybereye brainstorming sessions to stimulate new ideas, innovative solutions, and more efficient ways of delivering repeatable services

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 Cybersecurity Framework. A qualified candidate will be responsible for the following primary duties and responsibilities, but are not limited to:

- Assist with the development of policy documents using online research methods and an understanding of basic cybersecurity concepts.
- Assist with the generation of metrics to depict compliance data in charts and graphs using MS Excel
- Perform as part of a larger team in the documentation of organizational risk assessments through review of system architecture diagrams, vulnerability reports, and a basic understanding of common threat vectors (e.g. phishing, zero-day vulnerabilities)
- Participate in the design of 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:

- 2+ years of experience developing or assisting clients with the implementation of cybersecurity policy and regulatory compliance
- 1+ years of experience supporting the Assessment and Authorization (A&A) process, in accordance with NIST Risk Management Framework (RMF)
- 1+ years of experience generating, analyzing, and reporting data using Microsoft Excel
- Experience writing business process documentation, whitepapers, or technical reports

Submit Resume to kim.maurer@cybereyesolutions.com

- Experience reviewing or developing system architecture diagrams
- 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)

Preferred Qualifications:

- A professional security certification such as Security+ (alternative certifications will be considered)
- Experience with Tableau, Splunk, or Power BI for data analytics
- Experience generating RMF A&A Packages
- Experience with government organizations (e.g., Legislative Branch, DoD, or State and Local)
- Experience analyzing the security responsibilities of cloud service providers (CSP).

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