Senior Cyber GRC Specialist

Cybersecurity Department

Summary:

The Senior Cyber Governance, Risk, and Compliance (GRC) Specialist is responsible for leading the development, enhancement and implementation of a comprehensive cybersecurity risk management program for the firm. Reporting to the Director of Cyber GRC, the Senior Cyber GRC Specialist will engineer a data-driven risk and control program for assessing cyber, technology and operational risks rigorously and continuously, registering and tracking issues to completion, and reporting these issues to the Cybersecurity leadership and other stakeholders. The Senior Cyber GRC Specialist will provide strategic insights and guidance to enhance the firm's risk management and compliance activities to support its global operations and client requirements. This role requires hands-on, collaborative work with IT and Cybersecurity leadership teams and technical subject matter experts.

Email Resume Here to Apply

Qualifications:

- Bachelor's degree in Computer Science or Engineering preferred; advanced degree, CISSP, CISM, CRISC, CISA or other comparable certifications preferred.
- Requires 10+ years of experience in risk management, preferably within a law firm or professional services environment. Proven track record of successfully managing complex risk projects and initiatives.

Duties and Responsibilities:

- Defines, documents, and manages the firm's Risk Management program, including processes for identifying, categorizing, assessing, and registering risks; assigning owners; determining dispositions; and tracking issues to completion.
- Lead comprehensive risk assessments across all business units, identifying potential threats and vulnerabilities. Develop and implement risk mitigation strategies to safeguard the firm's assets and reputation.
- Provide expert advice to senior management on risk-related issues, ensuring that risk considerations are integrated into the firm's strategic planning and decision-making processes.
- Ensure the firm's risk and control program comprehensively accounts for emerging technologies and risk (e.g., AI).
- Manage security compliance efforts across the firm, ensuring adherence to industry standards (e.g., ISO 27001:2022) and client requirements (e.g., CMMC, NIST 800-171).
- Manage the firm's cyber governance forum, reporting on program progress to the CISO and other senior stakeholders.
- Build and curate Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to highlight control adoption gaps, identify areas of strong or weak performance, or quantify risks, respectively.
- Identity opportunities to automate control monitoring and work with technical subject matter experts to define and implement requirements.

- Strong analytical and problem-solving skills, with the ability to synthesize complex information and develop actionable insights.
- Ability to think strategically and align risk management practices with organizational goals.
- Superior time-management skills, relentless follow-through, and metronome-like, consistent delivery.
- Effective written and oral communications skills.
- CMMC and NIST 800-171 experience a plus.
- Position requires access to equipment, software, or technology that is subject to U.S. export controls. To be granted access pursuant to US Export Control laws, candidate must be either (a) a United States citizen or national; (b) a person lawfully admitted for permanent residence of the United States (i.e., "Green Card" holder); or (c) an INS-approved refugee or asylum holder who has applied for naturalization within six months of the date the individual first became eligible; and if not yet naturalized, is still actively pursuing naturalization if 2 years have passed since the date of application to be granted access pursuant to US Export Control laws. Candidates will be required to submit appropriate documentation to determine whether access can be granted before proceeding further through the application process.
- Contribute to the development and implementation of the Business Resilience plans; conduct Business Impact Analysis (BIA).
- Assess and provide guidance to improve the Business Continuity and Disaster Recovery plans and procedures across business units to ensure completeness.
- Uphold high standards of confidentiality, discretion, and integrity, particularly with respect to all sensitive and/or confidential firm and client information to which this position will have access.

Status: Exempt
Workplace Type: Remote
Salary Range: $134,000 – $188,000 (salary is calculated based on years of experience and location)