Senior Risk Analyst

Cybersecurity Department

Summary:

The Senior Risk Analyst is responsible for ensuring that the firm assesses risk in a consistent manner, and for sustaining a culture of risk awareness. Reporting to the Director of Cyber GRC, the Senior Risk Analyst operates a focused, thematic risk and control program for assessing cyber, technology and operational risks rigorously, registering and tracking issues to completion, and reporting these issues to the Cybersecurity leadership and other stakeholders.

The Senior Risk Analyst will provide strategic insights and guidance to enhance the firm's risk framework, third-party risk management program, and training and awareness program to support its global operations. 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 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; and using security learning and training software such as Proofpoint, Skillsoft or KnowBe4.

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.
- Prepare detailed risk reports for Cybersecurity and Technology leadership. Highlight key risk exposures, trends, and the effectiveness of mitigation strategies.
- 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.
- Defines, documents, and manages the firm's Security Awareness and Training program, ensuring that training content is up-to-date, fit-for-purpose, and consistently delivered.
- Regularly reports on program progress to the CISO and other senior stakeholders as appropriate, using defined 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.

Qualifications (continued):

- 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.

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.

Duties and Responsibilities (continued):

- Mentor and train junior risk analysts, fostering a culture of continuous improvement and knowledge sharing within the team.
- Perform other duties as assigned.
- 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
Reports To: Director of Cyber Governance, Risk & Compliance
Workplace Type: Remote (local NYC)

Salary Range of $117,000- $165,500 based on geography and experience level.