Risk Analyst

Cybersecurity Department

Summary: The 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 Information Security and Assurance, the 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 CISO and other stakeholders. The Risk Analyst also implements the Firm's security awareness and training program. This role requires hands-on, collaborative work with stakeholders and IT implementers.

Email Resume Here to Apply

Qualifications:

- Bachelor's degree in Computer Science or Engineering preferred; advanced degree and CISSP certification preferred.
- Requires 5+ years' experience in cybersecurity, conducting technology audits, and third party security risk assessments.
- Strong working proficiency using risk assessment software such as ServiceNow, Archer, IBM® OpenPages® or C2C MyRiskAssessor; and/or using security learning and training software such as Proofpoint, Skillsoft or KnowBe4.
- Superior time-management skills, relentless follow-through, and metronome-like, consistent delivery.
- Effective written and oral communications skills.
- Big 4 experience preferred.

Duties and Responsibilities:

- Define, document, and manage the Firm's Risk Management program, including processes for identifying, categorizing, assessing, and registering risks; assigning owners; determining dispositions; and tracking issues to completion.
- Tier, assess, and monitor risks associated with clients.
- Manage client risk program. Review assessment alongside SOC 2 reports and ISO certs. Confirm clients controls and advise on any gaps.
- Research security controls and translate to actionable insights and strategy.
- Define, document, and manage the Firm's Security Awareness and Training program, ensuring that training content is up-to-date, fit-for-purpose, and consistently delivered.
- Regularly report 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.
- Perform other duties as assigned.

Status: Exempt
Reports To: Director of Information Security & Assurance
Workplace Type: Remote
Salary: $98,000 – $138,500 (dependent on geography and experience)

- 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.

COVINGTON