Director of Cyber Governance, Risk, & Compliance

Cybersecurity Department

Summary:
The Director, Cyber Governance, Risk, & Compliance is responsible for critical Cybersecurity risk processes for Covington & Burling LLP, including IT and Information Security Governance, Cyber Risk Management, Cyber Compliance, and Third-Party Risk Management (TPRM).

Email Resume Here to Apply

Qualifications:

- Bachelor's degree required; advanced degree and CISSP (or CRISC, CISA) certification preferred.
- Expert working knowledge of security principles, risk assessment, risk management, control frameworks, and third-party risk management.
- Minimum of 15+ years' experience in cybersecurity, with 10+ years' experience running governance, risk, and compliance (GRC) or equivalent functions.
- Demonstrated track record of planning and executing successful information security strategies, programs, and processes in a highly sophisticated, global environment.
- Exceptional interpersonal skills with the ability to lead and influence stakeholders to foster broad commitment.
- Demonstrates good written and oral communications skills and communicates effectively.

Duties and Responsibilities:

Information Security Governance:

- Strengthen and optimize the Cybersecurity governance framework and related documentation to ensure continuous alignment with industry-leading practices, regulatory requirements, and corporate insurability standards such as NIST CSF, ISO 27001, EU/UK GDPR, HIPAA/HITRUST, and SOC 2 Trust Services Criteria.
- Maintain the firm's Governance, Risk and Compliance (GRC) framework and "controls baseline" compliance defining adherence to industry frameworks and regulations.
- Coordinate with the Chief Compliance Officer and Data Protection Officer (DPO) to track client security obligations, including those specified in outside counsel guidelines.

Cyber Risk Management:

- Maintain the Security and Risk Reporting framework for the firm, providing critical information for decision-making by key stakeholders.
- Manage comprehensive Cybersecurity policies, procedures, and standards to establish clear and actionable guidelines for cyber security and data protection controls.
- Develop data-driven dashboards communicating the Firm's current cyber risk posture, utilizing Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and cyber trends to offer actionable insights.
- Define, develop, and maintain the firm's security-related policies, procedures, and standards, ensuring they conform to the firm's narrative style and are well-written.

COVINGTON

Qualifications (Continued):

- Experience working with and implementing NIST, ITIL, and ISO 27001 standards.

- Working knowledge of regulatory data governance obligations, such as EU/UK GDPR, HIPAA/HITECH, ITAR/EAR, and CUI a plus.

This position requires access to equipment, software, or technology that is subject to U.S. export controls. To be granted access in accordance with US Export Control laws, candidates must meet one of the following criteria: (a) be a United States citizen or national; (b) be a person lawfully admitted for permanent residence of the United States (i.e., "Green Card" holder); or (c) be an INS-approved refugee or asylum holder who has applied for naturalization within six months of becoming eligible. If not yet naturalized, the candidate must still be actively pursuing naturalization if two years have passed since the date of application. Candidates will be required to submit appropriate documentation to determine eligibility for access before proceeding further through the application process.

Duties and Responsibilities (Continued):

Cyber Compliance:

- Develop and monitor remediation strategies to ensure ongoing compliance with regulatory requirements and assessment mandates.

- Collaborate closely with IT and Compliance Teams to validate the effectiveness of security practices, ensuring alignment with relevant standards, and thorough documentation in policies and procedures.

- Ensure the effectiveness of Security Training and Awareness processes, educating employees regularly and effectively about their security responsibilities, and periodically testing employees' resilience and knowledge through anti-phishing tests and other exercises.

Third Party Risk Management (TPRM):

- Engage with the Procurement department and other internal stakeholders to evaluate and manage Cybersecurity risks related to third-party vendors and service providers, ensuring proper implementation of contractual obligations and security controls.

- Collaborate with the firm's DPO to facilitate Privacy Impact Assessments.

- Manage the Third-Party Risk Management (TPRM) function, involving vendor triaging, risk assessment, security clause implementation, monitoring, and additional diligence when necessary.

Status: Exempt
Reports To: Chief Information Security Officer
Workplace Type: Hybrid

Salary range of $226,000- $318,000.