Manager, Cybersecurity

New York, NY

About Advance:

Advance (www.Advance.com) is a private, family-owned business that owns, operates and invests in assets spanning media, communications, technology and other promising growth sectors. Our mission is to build the value of our companies over the long-term by fostering growth and innovation.

Advance's portfolio includes Condé Nast, Advance Local, Stage Entertainment, American City Business Journals, The IRONMAN Group, Leaders Group, Turnitin, 1010data and Pop. Advance is also among the largest shareholders in Charter Communications, Discovery and Reddit.

About the role:
The Manager, Cybersecurity will be involved in all aspects of the cybersecurity program with direct responsibility of cybersecurity risk assessments, control reviews and cybersecurity/compliance audits. The incumbent will participate in the development of the cybersecurity strategy and help us mature existing cybersecurity programs (e.g., third-party risk management program). The successful candidate must demonstrate a strong technical background and a proven track record of successfully managing and leading security assessments. Interested candidates should submit their resume and cover letter to **Recruiting@advance.com**

Primary Responsibilities

- Manage and perform cybersecurity risk assessments, security control reviews, and compliance audits; develop recommendations, and track remediations of identified issues and risks.
- Manage and provide technical guidance and consultation related to various security and technology initiatives, cybersecurity investigations, and issues.
- Perform third-party risk assessments to evaluate security controls, identify vendor strengths and weaknesses, and provide recommendations to stakeholders.
- Contribute to the development of the cybersecurity program strategy and program assessment at Advance and its operating companies.
- Foster a collaborative dialogue across a highly matrix environment to gain consensus on cyber risk, impact, prioritization, resource sharing, and issues resolution.

- Support Internal Audit activities to guide auditors and control owners on technical security controls that are effective in mitigating risks.
- Assist the cybersecurity incident response team.

Qualifications

- Minimum of 4-6 years of experience managing, consulting, auditing, or working in the fields of cybersecurity, technology, or risk management.
- Bachelor's degree in computer science, cybersecurity, or related field of study.
- Strong communication, analytical and problem-solving skills.
- A team player who can successfully build relationships across the portfolio companies.
- Ability to work independently with minimal direction and collaborate effectively with local and remote teams.
- Knowledge of Cybersecurity and risk standards and frameworks such as NIST 800-53, CIS benchmarks, OWASP, ISO-27001 and PCI DSS.
- Familiarity with enterprise cloud solutions (e.g., AWS, Azure, o365, G-Suite, Workday).
- Working knowledge of multiple areas of technology (e.g., infrastructure, applications, SDLC, end-user platforms, SOC).
- Comfortable with articulating security related concepts to a broad range of technical and non-technical staff, including executive management.
- CISSP, CISM, PCI-QSA, PCI-ISA or other cybersecurity certifications a plus.
- Insurance, Financial Services, or Technology industry experience a plus.