GRAHAM HOLDINGS

Director, Information Security and Privacy

Reports to VP - Chief Information Security Officer · Rosslyn, VA (Hybrid)

Overview

Graham Holdings Company (NYSE: GHC) is a diversified holding company with operations across education, media, healthcare, manufacturing, automotive retail, and other industries. Refer to the Company website for additional information.

Graham Holdings is seeking a Director, Information Security and Privacy to serve as the principal operational leader of the company's enterprise cybersecurity and compliance program.

Reporting directly to the Chief Information Security Officer (CISO), the Director will be responsible for the day-to-day execution of the enterprise security strategy, management of the corporate security team, and direct engagement with portfolio company security and technology leaders across our portfolio of businesses.

This is not a traditional corporate security role defined by centralized authority or command-and-control program management. The successful candidate will operate within a highly decentralized holding company model where influence, trust, and operational rigor are the primary drivers of security maturity across an autonomous and diverse portfolio of businesses. Operating-company security execution lives within the businesses; the Director maintains enterprise-level governance standards, drives program consistency, and provides hands-on leadership for shared compliance and risk management programs.

The Director will inherit a well-established, respected security program with a strong compliance foundation, a functioning enterprise metrics platform, and an active portfolio-wide engagement model — and will be positioned to mature that program in meaningful ways as the organization's threat landscape and strategic priorities evolve.

The role offers meaningful visibility across the enterprise, direct team leadership, and the opportunity to contribute to a next-generation security operating model within one of America's most distinctive public companies.

Key Responsibilities

Primary Functions

- Execute the enterprise cybersecurity strategy in partnership with the CISO, translating strategic direction into operational programs, team accountabilities, and measurable outcomes across the portfolio.
- Lead the annual SOX ITGC and application controls testing program, directing annual testing, coordinating with the Corporate Audit SOX team and external auditors, and maintaining exceptional external audit reliance built on the quality and consistency of the program.
- Manage and operate the enterprise-wide cybersecurity metrics program, overseeing data collection, quality assurance, reporting cycles, and dashboard maintenance across all portfolio companies - and surfacing risk trends and escalation items to the CISO for executive and board-level reporting.
- Lead the enterprise incident response program, including maintenance of policies, playbooks, and vendor agreements; coordination of legal and insurance protocols; and facilitation of annual tabletop exercises across portfolio companies.

- Manage the enterprise vulnerability management program, and coordination of risk-prioritized remediation with portfolio company technology teams.
- Lead annual cybersecurity risk assessments across portfolio companies, evaluating control environments, identifying gaps relative to enterprise standards, and producing prioritized remediation roadmaps that inform enterprise risk reporting and investment prioritization.
- Operationalize the third-party risk management program, implementing active vendor assessment cycles, creating / maintaining the vendor risk inventory, and escalating material findings to the CISO.
- Work with portfolio companies to implement and administer the enterprise AI governance framework - including the Acceptable Use Policy, the generative AI guidance framework, AI vendor and deployment evaluation processes, and ongoing monitoring of agentic and multi-agent AI system behavior.
- Maintain and administer the Archer GRC repository and support preparation of the annual cyber insurance submission, coordinating program data across the portfolio and preparing for underwriter meetings as required.
- Directly manage the corporate information security team - providing coaching, performance management, professional development, and clear program accountability - while building and sustaining trusted working relationships with portfolio company technology and security leaders.
- Monitor security operations, including vulnerability management, privileged access management, data classification, compliance posture, resilience and user awareness programs across the portfolio - providing ongoing risk visibility to the CISO and escalating risk concerns or operational issues requiring attention as they arise.

Qualifications

Required

- Bachelor's degree in information security, computer science, information systems, or a related field.
- Minimum of 10+ years of progressive cybersecurity, IT risk, or security governance experience in a large, complex enterprise environment.
- Demonstrated experience managing SOX ITGC or similar compliance testing programs at enterprise scale, including direct coordination with external auditors.
- CISSP certification, or equivalent credential with a clear plan to obtain CISSP.
- Proven ability to lead cross-functional programs across decentralized or matrixed organizations, where influence and credibility drive outcomes more than formal authority.
- Strong analytical, risk assessment, and problem-solving skills, with rigorous attention to documentation quality and evidence standards.
- Excellent written, verbal, and interpersonal communication skills, including the ability to translate technical security risk into business and financial terms for operational and executive audiences.
- Ability to manage a team, maintain multiple concurrent programs, and meet recurring deadlines in a high-scope, high-accountability environment.

Preferred

- Big Four accounting firm and / or top-tier professional services firm background in IT audit, cybersecurity advisory, or technology risk assurance.

- CISM and/or CISA certification.
- Experience in a diversified holding company, multi-business enterprise, or similarly decentralized operating environment.
- Experience designing or operationalizing AI governance frameworks, including generative AI acceptable use, vendor evaluation, and agentic system risk management.
- Experience applying AI tools to improve security program workflows, risk assessment processes, or compliance operations.
- Working familiarity with applicable regulatory frameworks across a diversified portfolio, including HIPAA, FERPA, GLBA, PCI-DSS, and state cybersecurity and privacy requirements.

Logistics & Expectations

- Location: This hybrid role is based in our Arlington, VA corporate headquarters, with in-office presence required on an ad-hoc or as-requested basis for key team meetings, collaborative sessions, or company events.
- Travel: Expect periodic travel to business unit locations, including periodic international travel.

People and Culture

Graham Holdings is committed to being an exceptional place to work - one built on inclusion, fairness, and mutual respect. We hold ourselves to the highest ethical and professional standards and are dedicated to hiring and developing talented people from all backgrounds.

Benefits

We offer a comprehensive benefits package designed to support you at every stage of your career and life. Graham Holdings offers standout retirement benefits - a 401(k) plan plus a pension with company pension contributions starting at 8% and growing to 10% with tenure. Beyond that: 4 weeks of vacation to start, paid transportation, family leave, short- and long-term disability, and $5,000 in adoption assistance.

We also offer $5,250/year in tuition assistance plus tuition discounts, a choice of 3 medical plans, 2 dental plans, vision coverage, life and accident insurance, FSA/HSA accounts, a legal plan, and employee discounts.

For consideration, please send resume and salary requirements to careers@ghco.com.

Graham Holdings Company is an Equal Opportunity Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, age, sex, sexual orientation, gender identity/assignment, disability, genetic information, marital status, national origin, pregnancy, or maternity status, protected veteran status, or any other legally protected basis, in accordance with federal, state, and local applicable law. We will ensure that individuals with disabilities are provided reasonable accommodation to participate in the process. Please contact us to request accommodation.

The wage range for this role considers various factors used in making compensation decisions, including but not limited to skill sets, experience, training, licensure, certifications, and other business and organizational needs. It is not typical for an individual to be hired at or near the top of the range for their role, and compensation decisions are dependent on the specifics of each individual situation. A good-faith reasonable estimate of the current range is $175,000 to $250,000.