



Manager, Information Security and Privacy

Reports to Director, Information Security and Privacy · 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 Manager, Information Security and Privacy to join the corporate information security team. The role serves as a key subject matter expert on cyber security, compliance and risk management for the company and its business units – maintaining and assessing enterprise-level governance standards, driving program consistency, and providing hands-on technical expertise for shared compliance and risk management programs.

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.

The Manager will work regularly with portfolio company technology and security teams, the Director and CISO, internal and external auditors, and vendor partners — translating complex technical conclusions into clear, actionable guidance for executive leadership and non-security stakeholders.

The role suits an experienced IT risk, IT audit, and cybersecurity professional who takes genuine satisfaction in operational ownership and program quality — 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

- Lead the day-to-day execution of the annual SOX ITGC and application controls testing program — managing testing workflows, timelines, workpaper documentation, and quality standards — and coordinating directly with control owners at portfolio companies to gather evidence, assess control effectiveness, and document findings in accordance with established methodology.
- Maintain and operate the enterprise-wide cybersecurity metrics program, managing data collection, quality assurance, dashboard maintenance, and reporting cycles across all portfolio companies, and preparing metrics reporting packages that flag material risk trends and businesses requiring escalated attention.
- Manage the enterprise cloud and on-prem vulnerability management program, including day-to-day operation of the Orca and Qualys platforms, coordination of vulnerability findings with portfolio company technology teams, and tracking of risk-prioritized remediation activities to completion.
- Support and execute annual cybersecurity risk assessments across portfolio companies, coordinating with business unit technology and operational leadership to evaluate control environments, identify gaps relative to enterprise standards, and document prioritized remediation roadmaps.

- Assist with planning and coordinating annual tabletop incident response exercises across portfolio companies — including scenario development, participant coordination, exercise facilitation, and post-exercise findings documentation — and support enterprise incident response activities during actual security events.
- Execute the third-party and vendor risk assessment program, conducting security assessments of new and existing vendors across the portfolio, maintaining the vendor risk inventory, and escalating vendors with material security deficiencies to the Director.
- Support operationalization of the enterprise AI governance framework — including coordination of AI Acceptable Use Policy adoption, execution of the AI vendor and deployment evaluation process, and monitoring of agentic AI system behavior across deployed environments.
- Maintain the Archer GRC repository with current SOX and compliance documentation, administer the enterprise security awareness and training program including phishing simulation campaigns, and support preparation of the annual cyber insurance submission.
- Engage directly with portfolio company technology and security teams as an operational partner — providing program guidance, coordinating compliance activities, and escalating material findings and operational concerns to the Director in a timely and well-documented manner.

Qualifications

Required

- Bachelor's degree in accounting information systems, management information systems, or a related field.
- Minimum of 6+ years of progressive experience in information security, IT risk management, IT audit, and / or cybersecurity compliance in a complex enterprise environment.
- Demonstrated experience with SOX ITGC testing, evidence collection, workpaper documentation, and external audit coordination.
- Hands-on experience operating security governance tools — including vulnerability management platforms and GRC systems as well as security metrics programs.
- Self-starter with strong analytical and documentation skills, with rigorous attention to quality and detail across compliance and risk management work products.
- Effective communication skills, with the ability to engage confidently with technology leaders, control owners, and operational stakeholders across multiple business units.
- Ability to manage multiple concurrent program commitments, meet recurring deadlines, and maintain quality under competing priorities.

Preferred

- Strong preference for Big Four accounting or top-tier professional services firm with experience in IT audit, cybersecurity advisory, or technology risk assurance.
- CISSP, CISM, or CISA certification; candidates actively pursuing relevant certification who bring strong experience will also be considered.
- Experience in a diversified holding company, multi-business enterprise, or similarly decentralized operating environment.
- Familiarity with cloud security environments and cloud-based vulnerability management platforms.

- Experience supporting or executing AI governance activities, including AI tool assessments or generative AI acceptable use policy implementation.
- Working familiarity with applicable regulatory frameworks across a diversified portfolio, including HIPAA, PCI-DSS, and SOX.

Logistics & Expectations

- Location: This is a hybrid role based out of our corporate headquarters in Arlington, VA, requiring regular in-office presence. Candidates should live within a reasonable commuting distance to attend as needed. Additionally, in-office presence may be required on an ad-hoc or as-requested basis for key team meetings, collaborative sessions, or company events.
- Compensation: Competitive manager-level base salary and a comprehensive benefits package. Leveling will reflect depth of experience.

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 \$130,000 to \$175,000.