Cybersecurity Practitioner

Compass IT Compliance, LLC is a leading Information Technology Audit and Compliance firm. Companies large and small must comply with a confusing mix of regulations and laws such as the PCI DSS (Payment Card Industry Data Security Standard), FFIEC, Sarbanes-Oxley, HIPAA / HITECH, Basel II, Gramm-Leach-Bliley Act, Patriot Act, Identity Theft Red Flags, SEC requirements and state privacy laws. Even in today's tough economy, and in the face of rising costs and shrinking staffs, companies must remain a step ahead of these complex compliance requirements.

The practice of IT Audit and Compliance identifies and remediates any violations of these regulations and requirements from both a technical and procedural perspective. It is also a very complex practice that can become costly and time- consuming. To meet strict IT and security guidelines, organizations require independent assistance with:

- Payment Card Industry (PCI) Services
- Security Assessment Services
- IT Auditing and Risk Assessment Services
- Privacy and IT Regulatory Compliance Services
- Business Resiliency (disaster recover, business continuity, incident response) Planning
- Outsourced Information Security Officer duties

Compass IT Compliance provides experienced, certified IT Auditors to perform IT audit and compliance work at a lower cost than maintaining internal auditing staff. By outsourcing their IT Audit and Compliance requirements to Compass, organizations save costs while ensuring complete IT compliance by employing objective, certified consultants from an independent and trusted IT leader.

Compass is looking for an experienced cybersecurity practitioner to join the Compass IT Compliance Audit team to assist in meeting the growing need for cybersecurity and audit services within the business world today. The ideal candidate would need to be able to work independently as well as part of a team. During audits, the position will interact with all levels of client personnel from IT line staff to C-level executives, and present findings and recommendations to audit committees and senior management. During cybersecurity consulting, the position will be learning the client organization enough to recommend cybersecurity solutions, draft security programs and business resiliency documents, and assist with ensuring organizational compliance with all applicable security standards, laws, and regulations. Although COVID-19 has suspended travel to clients currently, under normal business operations a person could expect to experience regional travel up to thirty percent (30%) of the job.

Essential Duties and Responsibilities

- Perform IT Risk Assessments and audits for customers against IT Regulations and Standards
- Provide recommendations and guidance on identified security and control risks.
- Responsible for documenting methodology, findings and recommendations to support IT Risk Assessments and Audits
- Perform Business Impact Analysis (BIA) for business resiliency
- Develop, review, test and update customer business resiliency (disaster recovery, business continuity, pandemic planning, incident response planning) Plans
- Participate in team projects and assignments
- Represent the client as an outsourced IT Security officer
- Creation, review, and upkeep of an information security program for the client including all relevant policies and standards.
- Participate on security steering committees and/or board level meetings about cybersecurity for the client
- Conduct security awareness training for the client
- Plan, implement, monitor and upgrade security measures for the protection of the organization's data, systems and networks.
- Assist sales in a sales engineering capacity to ensure clients get the proper services based on their needs
- Assist management in improving services and deliverables and suggesting new opportunities

Qualifications (Knowledge, Skills, and Abilities)

- Bachelor's degree in Computer Science / Computer Information Systems or related field or equivalent experience
- 5-10 years of information technology and/or security experience or IT security auditing
- CISA, CISM, CRISC or CGEIT certifications
- Excellent written and verbal communication skills

- Knowledge of IT Regulations and Standards e.g. PCI DSS, FFIEC, HIPAA, CoBiT, ISO, SSAE 16
- Experience with Policy and Procedure development
- Experience with Business Continuity Planning and Disaster Recovery

- Ability to manage multiple projects and schedules independently
- Knowledge of operating systems, network architecture, web development
- Ability to travel for a portion of clients
- Cloud security experience (AWS, Azure, Google) a plus

Interested in applying? Visit our website at www.compassitc.com