Manager, Information Security Risk and Compliance

The Manager of Information Security Risk and Compliance is primarily responsible for execution, monitoring and enforcement of the information security governance, risk management, compliance and policies, procedures, and standards. The successful candidate will oversee day to day execution of operational information security risk and compliance initiatives at Ipsidy. This position will report to Vice President/Chief Information Security Officer (CISO) and collaborate closely with other Ipsidy teams within the organization to ensure successful implementation of security initiatives.

Responsibilities:

- Manage and execute the day-to-day information security risk and compliance operational activities
- Develop and recommend appropriate information security policies, standards, procedures, checklists, and guidelines using generally-recognized security concepts tailored to meet the requirements of the organization
- Develop risk/vulnerability assessment programs and questionnaires to aid in the identification and mitigation of security risks
- Perform risk assessments per the InfoSec program on different technology components and processes at Ipsidy.
- Identify and document specific security issues, propose resolution options, and interpret matters from the perspective of involved stakeholders
- Communicate regularly with other Ipsidy teams and staff as part of risk assessments, follow-up on open issues, status tracking, and other miscellaneous items.
- Identify and document specific security issues, propose resolution options, and interpret matters from the perspective of involved stakeholders
- Independently design, recommend, plan, develop and support implementation of project-specific security solutions to meet requirements
- Manages remediation of identified risks and vulnerabilities; identify those within the organization responsible for remediation tasks; track progress on remediation of identified risks and vulnerabilities and provide appropriate reporting to all constituents
- Provides regular reporting metrics on the current state of the program.
- Other duties as assigned

Basic Qualifications:

- Bachelor's degree in Computer Science, Information Technology, Business Administration or related field
- 5+ years of experience in information security risk assessment, compliance and/or security operations
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and nontechnical audiences.
- Strong analytical skills to analyze security requirements and relate them to appropriate security controls.
- Working knowledge of relevant security regulations, standards and frameworks, including SOC2, ISO27000, PCI, and NIST.

Preferred Qualifications:
Professional certifications such as CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor) or other similar credentials.

Job Location: Atlanta, GA

What We Offer:

- Competitive Salary
- Healthcare: Medical/Dental Benefits
- Fast-paced, rapid career growth opportunity

Contact: Nihat Guven, nihatguven@ipsidy.com