GEORGIA DEPARTMENT
OF COMMUNITY HEALTH

Brian P. Kemp, Governor **Russel Carlson, Commissioner**

2 Martin Luther King Jr. Drive SE, East Tower | Atlanta, GA 30334 | 404-656-4507 | www.dch.georgia.gov

Cybersecurity Audit Manager
Job Code: FIP060

SALARY INFO:
Annual Salary: $69,134 - $113,485
Pay Grade: O

AGENCY SUMMARY:
The Georgia Department of Community Health (DCH) is one of Georgia's four health agencies serving the state's growing population of almost 10 million people. DCH serves as the lead agency for Medicaid, oversees the State Health Benefit Plan (SHBP), and includes Healthcare Facility Regulation, impacting one in four Georgians. Through effective planning, purchasing and oversight, DCH provides access to affordable, quality health care to millions of Georgians, including some of the state's most vulnerable and under-served populations. Six enterprise offices support the work of the agency's four program divisions. DCH employees are based in Atlanta, Cordele and across the state.

JOB SUMMARY:
DCH is in the process of transforming existing legacy Medicaid Enterprise Systems (MES) into modern, loosely coupled, seamlessly integrated, modular systems where the exchange of data and processes is seamless and automatic. This procurement and implementation represent one of the largest and most significant projects at DCH and will impact millions of Georgians with the goal of improving health outcomes and wellness and improving system performance and efficiency.

DCH is seeking a highly skilled and experienced **Cybersecurity Audit Manager** for the **Office of Information Technology**, to coordinate and lead the testing efforts for the Medicaid Enterprise System Transformation initiative. The successful candidate will be responsible for developing and executing comprehensive test plans, ensuring the quality and functionality of the application, and managing a team of testers.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

1. **Risk Management:** Identifies and assesses cybersecurity risks to DCH's information assets, IT infrastructure, and systems. Implements risk management processes and frameworks to prioritize and address vulnerabilities.
2. **Security Policies and Procedures:** Establishes and enforces information security policies, standards, and procedures to guide DCH's security practices.
3. **Security Auditing and Compliance:** Conducts regular security audits and risk assessments to ensure compliance with relevant industry standards, regulations, and legal requirements.
4. **Vendor and Third-Party Risk Management:** Assesses and manages cybersecurity risks associated with third-party vendors and partners accessing DCH's data and systems.
5. **Regulatory and Legal Compliance:** Ensures DCH's compliance with relevant data protection laws, regulations, and contractual obligations related to information security.
6. **Continuous Improvement:** Continuously assesses and enhance DCH's cybersecurity program based on emerging threats and industry best practices.

.

MINIMUM QUALIFICATIONS:

- High school diploma/GED and three (3) years in the specific field of IT Security, which includes one (1) year in a managerial role.
- A minimum of one (1) year of management experience.

PREFERRED QUALIFICATIONS:

Preference will be given to candidates who, in addition to meeting the qualifications listed above, demonstrate some or all of the following skills/experience:

- Thorough understanding of federal and state computer security and privacy laws, regulations, standards, and controls, including the HIPAA Final Security Rule, the National Institute of Standards and Technology (NIST), Risk Management Framework, and Special Publications (including 800-53 Moderate-Impact-Baseline).
- A minimum of five (5) years of cybersecurity auditing experience, focusing on healthcare or government environments.