**Senior I/S Risk and Compliance Analyst**

This is a great 12 month contract opportunity based in Columbia SC.   
  
Columbia, SC, ranked as one of CNN's Money magazine's "Best Places to Live " and Forbes Best place for Business and Careers!  
  
We'd love to hear from you to tell you more about our industry leading benefits, as well as the team that will be dedicated to helping you achieve your career goals from start to finish!  
  
**\*Please Note: Only U.S. Citizens will be considered. Corp to Corp will not be considered.**

**How will you contribute?**   
  
Under the guidance of the System Security Manager, Information Security Analyst is responsible for supporting the information security risk reduction goals within the Information Technology organization and across the business units of the company.

* Assist in the development, implementation and ongoing management of the Information Security Program
* Consult with Systems &Technology staff members, business unit staff and provide guidance in the definition of the appropriate security architecture and technical requirements necessary to address information security needs
* Use the risk assessment process to continually identify new internal and external threats, vulnerabilities, and use those results to generate recommendations for mitigating control
* Provide corporate and local project team leadership for information security initiatives
* Work with the organizations training department to provide supplemental Information Security Awareness Training for all TRICARE I/S employees
* Work with Systems &Technology staff, local and corporate project teams to identify, develop, pilot, implement and manage integrated and usable security technology solutions that appropriately mitigate business risk
* Conduct annual Information Security Vendor Reviews in conjunction with Legal, the Vendor Manager and the System Security Manager
* Provide technical ownership and continuous improvement direction for assigned technologies or areas of responsibility
* Ensure that the controls environment and any related processes, procedures and standards adhere to the National Institute of Standards and Technology (NIST) framework
* Develop and maintain documentation related to departmental processes, procedures and standards
* Collaborate with internal Audit Department in the planning, execution, response and remediation of audit examinations and findings
* Work closely with internal Audit Department to gather information and respond to requests from other third-party vendors or business partners
* Assist System Security Manager with responses to audit findings
* Support in conducting Security Controls Assessment (SCA) activities
* Responsible for testing security controls
* Reviewing and analyzing systems, along with conducting network security and vulnerability assessments
* Staying up to date with current vulnerabilities, attacks, and countermeasures
* Perform independent hands-on risk assessments to identify information security risks and recommend risk treatment strategies
* Serve as a subject matter expert for team members who may perform information security risk assessments
* Work with business units to help them understand identified risks as well as proposed risk treatment strategies
* Prepare formal documentation detailing the outputs of risk assessments
* Update and report on metrics to show where the organization stands with relation to information security risks
* Keep abreast of current and evolving information security threats and regulations; create new policies, review existing corporate policies and make modifications and recommendations to policies when required.
* Assist the manager in reviewing third-party supplier contracts to reduce risks to manageable levels

**How will you spend your time during the day?**

* Conduct procedural and operational review of I/S processes and systems against corporate, government, and internal I/S compliance standards.
* Act as the I/S representative for computer forensic examinations, incident investigations, and risk assessment activities conducted by internal and external areas.
* Evaluate technology and business-related controls for integrating business and information system security and risk mitigation efforts.

**What do you need to know to perform this role?**

* Knowledge of regulatory and compliance requirements including: HIPAA and HITECH, Sarbanes Oxley, GLBA, and PCI
* Knowledge and prior experience in IT security compliance
* Strong knowledge of DoD and NIST IA policies and risk assessment methodology
* Familiar with technical knowledge of network devices and interconnection (i.e. routers, switches, IDS/IPS, firewalls and DNS) and configuring or testing computer systems according to DISA Security Technical Implementation Guides (STIGs) or similar configuration guidance
* Knowledge and understanding of audit principles for the coordination and advisement of appropriate management action plans that will address the cause of control deficiencies
* This position requires an in depth understanding of the National Institute of Standards (NIST) Special Publications (800 Series) with particular emphasis on the SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. Must be able to demonstrate extensive knowledge of the control structures and application of controls.
* Knowledge in analyzing, recommending, and reviewing enterprise wide security policies, standards, and guidelines within appropriate organizational risk tolerances Skill in implementing enforcement of security policy within technology solutions
* Knowledge of enterprise security assessments using Enterprise Governance Risk and Compliance solutions

**Behavioral Skills:**

* Self-motivated and directed; able to manage multiple competing priorities based on risk level and ease of implementing controls
* Must possess excellent written communication skills and the proven ability to understand and present complex, technical information to both technical and non-technical audiences
* Must be an independent self-starter
* Demonstrates exceptionally strong written and verbal communication
* Excellent presentation and public speaking skills required. Must be comfortable presenting technical information to a group
* The ideal candidate should be able to multitask and give equal attention to a variety of functions while under pressure

**\*Please Note: Only U.S. Citizens will be considered. Corp to Corp will not be considered.**  
  
Modulant provides a competitive benefits package including health, dental, vision, 401k plan and paid time off.  
  
Modulant is an EEO/AA employer. All qualified applicants, who are eligible for employment, will be considered for advertised job opportunities without discrimination based on race, color, religion, sex, national origin or disabilities.