Title: Risk Management Security Analyst
Department: Information Security
Reports to: Associate Director, IT Security & Compliance

FLSA Status: Exempt
Internal Job Grade: 15

Position Summary

The Risk Management Security Analyst is responsible for assisting Access Health CT (AHCT) with its Information Security Risk Management Program, satisfying both regulatory compliance requirements and managing security risk to an acceptable level. This role is a hands-on role that will be responsible for actively identifying, detecting, monitoring, maintaining, analyzing, advising, and responding to ongoing IT security and compliance needs under the guidance of the Associate Director, IT Security & Compliance.

The individual selected for this role will collaborate with various cross-functional teams inclusive of partners and vendors in identifying, evaluating, categorizing, tracking and monitoring enterprise IT security risk and will assist with development and maintenance of IT security controls in adherence with federal and other government required cyber security frameworks.

Furthermore, the individual in this role will be responsible for assisting with development, automation, and ongoing maintenance of end-to-end risk register and related risk management work streams and processes (i.e., risk assessments, risk mitigation strategies, etc.) by utilizing existing Archer Governance, Risk, and Compliance (GRC) platform and other state-of-the-art security tools. This role reports to the Associate Director of IT Security and Compliance and has no direct reports.

Responsibilities

- Conduct third-party security risk assessments and security reviews in accordance with regulatory requirements.
- Collaborate with IT, Legal, product owners, and business teams to ensure appropriate IT Security and Compliance requirements are incorporated into new and ongoing engagements and initiatives.
- Support development, maintenance, and operation of a centralized enterprise cyber risk register and associated activities in Archer GRC platform.
- Define and report on key risk metrics to Management on regular basis.
- Liaise with IT, Legal, product owners, and business teams to provide accurate and timely responses to internal and external IT Security and Compliance inquiries and related activities.
- Assist with technical vulnerability assessments and security reviews of infrastructure, network, applications, and databases, utilizing Nessus scanning software and other state- of- the- art security tools.
- Facilitate, track, and manage vulnerability remediation based on risk categorization, with timely assessing and communicating risk, documenting, and reporting on mitigation status.
- Actively monitor, analyze, and generate reports on company's security landscape utilizing SIEM and other state- of- the- art security tools.

- Provide guidance, technical expertise, and training to the enterprise to ensure optimal use of the Archer GRC platform.
- Develop and maintain technical documentation, such as security control implementations, System Security Plan (SSP), user guides, process documentation, and configuration details.
- Identify opportunities for process optimization, automation, and streamlining tasks.
- Participate actively in frequent regulatory submissions and inquiries.
- Manage and continuously monitor remediation plans for compliance and mitigation of risk.
- Assist with responding to information system security incidents, including investigation of, countermeasures to, and recovery from computer-based attacks, unauthorized access, and policy breaches.
- Bridge information security requirements with business processes and IT systems and projects.
- Analyze and recommend security controls and procedures in business processes related to use of information systems and assets, and monitor for compliance.
- Develop, administer, and provide advice, evaluation, and oversight for information security training and awareness programs.
- Maintain a current and comprehensive understanding of relevant industry standards to incorporate into the risk management strategy, framework, and program.
- Completes other tasks, as assigned.

Qualifications

- Bachelor's degree in Management Information Systems, Cybersecurity, Computer Science or related Information Technology field and/or equivalent industry experience.
- A minimum of 3-5 years of combined hands-on experience in Information Security, Information Technology, Audit, or Governance, Risk, and Compliance.
- One or more of the following security certifications is preferred or in process:
    - Certified Information Systems Auditor (CISA)
    - Certified Information Systems Security Professional (CISSP)
    - Certified in Risk and Information Systems Control (CRISC)
    - Global Information Assurance Certification (GIAC)
- Working knowledge of common Cybersecurity Frameworks including the National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF), NIST SP 800-53, FedRAMP, and Center for Internet Security (CIS) Critical Security Controls.
- Hands-on experience with GRC platforms and other state-of-the-art security tools.
- Experience with development and management of metrics and reporting.
- Applied knowledge with data mapping, risk assessments, third-party risk management, audits, compliance tracking, and security controls management.
- Solid understanding of cybersecurity best practices and how to implement and apply at a business setting.
- Demonstrated success in problem solving, project management, business analysis, and data analysis.
- Solid organizational and excellent verbal and written communication skills.
- Detail oriented and highly organized, with the ability to thrive in a fast-paced environment and prioritize accordingly.
- Ability to successfully multi-task while working independently or within a group environment.
- Ability to collaborate with internal and external stakeholders in an effective manner that produces desired results.

Physical Demands: the physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is frequently required to sit, stand, hear, use hands to type data, and utilize a phone or other electronic communication devices. This employee may occasionally have to operate business machines. Specific vision abilities required in this job include close vision and the ability to adjust focus.

Work Environment: this is an in-office role on Tuesdays and Wednesdays and a remote role 3 days per week. The noise level in the work environment is usually low to moderate. The role requires the ability to work offsite with stakeholders at their locations, e.g., BITS, DSS. Requires fast-paced deadlines and has a high stress at times. Occasional local travel and some travel within the U.S.

Affirmative Action and Equal Opportunity Employer