

MedAssets

*Position Title:	IT Security Analyst
*Location:	Alpharetta, GA
	Full Time/Permanent
*Compensation:	Salaried/\$90K (negotiable)
*Start Date:	ASAP

ISACA Atlanta is not responsible for the content or accuracy of this job posting.

***JOB DESCRIPTION**

Company Overview:

MedAssets (NASDAQ: MDAS) partners with healthcare providers to improve financial strength by implementing spend management and revenue cycle management solutions that help control cost, improve margins and cash flow, increase regulatory compliance and optimize operational efficiency. MedAssets serves more than 180 health systems, 4,000 hospitals and 90,000 non-acute healthcare providers. For more information, visit www.medassets.com.

Job Purpose:

The IT Security Analyst is responsible to the VP Information Technology. Primary responsibilities include ongoing management of enterprise information security to ensure maintenance of data confidentiality, integrity and availability of all organizational systems.

Position Objectives:

- Directing the development, implementation, maintenance and compliance with security policies and procedures
- Prepares and reviews status reports on security matters to develop security risk analysis scenarios and response procedures.
- Managing the response, tracking and monitoring of all information and technology security incidents;
- Enforcing security policies and procedures through internal control self-assessments.
- Coordination with key functional areas on information security matters

Essential Duties & Responsibilities:

- Performs highly complex analysis and technical tasks involving assignment and coordination of measures to provide information assurance, event detection and rapid response across various environments of the enterprise.
- Designs, implements and supports integration of information security solutions including security architectures, firewall administration/monitoring, integrating security products, and developing and coordinating security implementation plans.
- Guides users and technical team members in formulating security requirements, integrating security requirements into existing system architectures, developing security test plans, overseeing the execution of security testing, and advising on alternative approaches.
- Provides technical lead on security projects which involve a wide range of issues including secure architectures, secure electronic data traffic, network security, platform and data security and privacy.
- Provides organizational support of enterprise security architecture and design, benchmarking, technical framework and gap analysis.
- Reviews and contributes to the improvement and standardization of the security administration process across all business units.
- Prepares training plans for staff, allocates ongoing training for personnel on new computer systems or technologies being implemented which require security administration.
- Leads or assists in forensic analysis, cyber-crime investigation, incident emergency response and investigations related to information security.

Internal Responsibilities:

- Adheres to all company policies and procedures including, but not limited to those identified within the Standards of Business Conduct and the Employee Handbook, as may be amended from time to time. Adheres to all applicable laws and regulations and the company's governance/compliance program.
- Responsible for reporting violations of the company's policies and procedures, Standards of Business Conduct, governance program, laws and regulations through the company's Help Line or other mechanism that may be available at the time of the violation. Assists with internal control failure remediation efforts.
- Becomes knowledgeable of internal control responsibilities through training and instruction. Responsible and accountable for internal control performance within their area of responsibility. Participates in the internal controls self-assessment process.
- Ensures concerns with internal control design or performance and process changes that impact internal control execution are communicated to management.

Minimum Qualifications & Competencies:

- A four-year degree in Information Technology with an information security emphasis - preferred, Associates Degree with experience in Computer Information Systems and/or Engineering with emphasis in information security or equivalent relevant experience – required
- CISSP, CISM or CISA or equivalent certification required.
- 6-10 years of combined IT and security work with a broad range of exposure to systems analysis, applications development, database design and administration; at least 6 years of experience in information security.
- Proven experience, clarity and courage to drive an agenda with the ability to influence without direct authority.
- Demonstrated experience in developing and implementing an information security strategy in a large, complex environment with successful outcomes.
- Knowledge of HIPAA, PCI, and other regulations
- Knowledge of application systems, network architecture, multiple platforms and new technologies from a security perspective to include firewalls, intrusion detection, Windows server, network architecture, DNS, VPN, application, database and O/S security, web-based systems and single sign on technologies.
- Extensive knowledge of data security and access control systems, encryption and related matters.
- Extensive knowledge of information protection methodologies and concepts, such as identification and authentication, access control, inception and audit trails.
- Strong incident handling and forensics experience including knowledge of common probing and attack methods, network/service discovery, system auditing, viruses and worms.
- Strong analytical, writing and exceptional communication skills.
- Demonstrated problem solving and critical thinking skills.
- Ability to routinely multi-task between the tactical and the strategic; ability to work with flexibility, efficiency, enthusiasm, and diplomacy both individually and as part of a complex team effort.
- Knowledge of system and network exploitation, attack pathologies and intrusion techniques, such as denial of services, Sync attack, malicious code, password cracking, etc.
- Able to take complicated or complex information and present it in a clear, concise, and logical manner
- Builds appropriate rapport and develops constructive and effective relationships; Uses diplomacy and tact in dealing with others

Travel: 20%

Physical Demands:

The physical demands and work environment characteristics described here are representative of those that an employee must meet to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- Physical Demands: While performing the duties of this job, the employee is occasionally required to move around the work area; sit; perform manual tasks; operate tools and other office equipment such as computer, computer peripherals and telephones; extend arms; kneel; talk and hear. The employee must occasionally lift and/or move up to 15 pounds.
- Mental Demands: the employee must be able to follow directions, to get along with others, and handle stress;
- Work environment: The noise level in the work environment is usually minimal.

MedAssets is an Equal Opportunity Employer and ensures its employment decisions comply with principles embodied in Title VII, the Age Discrimination in Employment Act, the Rehabilitation Act of 1973, the Vietnam Veterans Readjustment Assistance Act of 1974, Executive Order 11246, Revised Order Number 4, and applicable state regulations.

***JOB REQUIREMENTS**

Please provide a description of skill sets and other qualification necessary for applicants.	
Travel:	20%
Education:	Bachelor's
Experience:	8-10
Certification:	Required: CISSP, CISM, or CISA Desired:

COMPANY INFORMATION

www.medassets.com

CONTACT INFORMATION

Job Reference:	IT-03-11-NH
*Contact Name:	Mary Beth Powell
*Method:	mpowell@medassets.com
Website:	www.medassets.com

SPECIAL INTRUCTIONS:

Please provide additional/special instructions for the potential applicant to follow-up (e.g., provide a cover letter, résumé, and salary history...).