

Identify and Manage Risks.

Information systems that are owned by the U.S. Federal government or contain Federal government information are subject to security requirements described in the Federal Information Security Management Act (FISMA); Office of Management and Budget (OMB) guidance; Department of Defense and Civilian Agencies directives and policies; and standards by the National Institutes of Standards and Technology (NIST). In order to comply with these requirements, organizations must ensure independent security test and evaluation (ST&E) is performed in accordance with Certification & Accreditation (C&A) guidelines.

SecureIT is a qualified independent Security Control Assessor (SCA) as defined by NIST with certified control assessors, security vulnerability and penetration testing specialists to provide organizations the following services and solutions:

Security Test and Evaluation (ST&E) - Involves the development of a plan to evaluate the security controls of the system and examine vulnerabilities in system infrastructure and applications. We prepare plans that leverage organizational and other common control assessments eliminating redundancy and costs. The ST&E scope and deliverables include:

- Security Control Assessment - Based on NIST SP 800-53A, DIACAP, or other standards.
- Vulnerability Assessment - Scanning of infrastructure, applications, and external penetration testing tailored to your organization and system characteristics.
- Sensitive Data Scanning - Detection of unprotected sensitive data and Personally Identified Information (PII).
- Contingency Plan Testing - Design test scenarios and conduct testing to evaluate effectiveness.
- Incident Response Testing - Evaluate your organizations processes for detection, response and reporting of security incidents.
- Security Assessment Report - Prepare a report of findings with recommendations for remediation.
- Plan of Action and Milestones (POA&M) - Corrective actions required for unacceptable risks.

Continuous Monitoring - A continuous monitoring program allows an organization to track the security state of its information systems. Effective continuous monitoring enables an organization to keep pace with new security threats and vulnerabilities which may be introduced due to system/process changes and new technologies. SecureIT designs, implements and operates effective continuous monitoring programs through:

- Development of a continuous monitoring strategy that is appropriate for the system and your organization, leveraging existing efforts, tools and automation;
- Implementation of configuration management and control processes which integrate security and risk management;
- Performance of security impact analyses on actual or proposed changes to determine controls impacted and associated risk;
- Assessment of selected security controls based on the continuous monitoring strategy;
- Periodic vulnerability scanning, configuration baseline audits, and penetration testing;
- Updated Security Assessment Reports reflecting current weaknesses and accounting for remediation successfully performed; and
- Preparation of security status reports for appropriate organizational officials.

To learn more about the specific ways in which **SecureIT** can help your organization, please contact us at 703.464.7010 or visit us at www.secureit.com