Information Security

FISMA Audit & Enterprise Risk Management

Safe.
Compliant.
Business.

The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have changed the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, systems are unprotected from individuals and groups with malicious intent to intrude and use the access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

This concern is well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies where maintaining the public's trust is essential.

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each Federal Agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Partner in Success

Information Technology Company, LLC (ITC) offers a best in class partnership in helping Federal Agencies with FISMA compliance. Built on ITC's long relationship providing audit support with the Government Accountability Office (GAO) the company combines technology, proven methodologies, and experience to help its customers reduce risk and achieve maximum security. ITC recently performed successful FISMA audits of the General Support System of the National Transportation and Safety Board (NTSB).

Founded in 1993, ITC is an experienced service solutions provider that has the knowledge, tools, and proven methodology to help Federal Agencies achieve total security with their information technology environment.

ITC provides high-technology solutions and services to Federal Agencies and commercial customers that require high quality in every aspect of a project, from planning to delivery and documentation. ITC provides services for project architecture design, application design, development of specialized hardware and software, hardware installation and support, systems programming, staff training, and data center auditing.

Information Technology Company

7389 Lee Highway
Suite 210
Falls Church, VA 22042

PO Box 688
Falls Church, VA 22040-0688

Phone: 800-994-9441
Fax: 703-237-0223
Web: www.p390.com

Business Partner IBM™

Active in the Federal sector since 1993, ITC is an IBM Business Partner specializing in IBM S/390, zSeries, and pSeries (RS/6000) computing platforms. Within those IBM hardware environments ITC provides superior expertise in z/OS, z/VM, z/VSE, Linux, and AIX operating systems. ITC also supports a variety of application environments including DB2, IMS, CICS, Oracle, MQSeries, MXG, SAS, CA-ACF2, CA-Top Secret, and CA-DYL. ITC is currently in the 8th year of an ongoing contract to provide FISMA auditing support to the Government Accountability Office (GAO).

ITC excels in providing information security testing and Enterprise Risk Management (ERM) services. The company brings experience and expertise in enabling Federal Agencies with relevant FISMA and Certification and Accreditation (C&A) services.

ITC aids Federal Agencies in their efforts to achieve total security with their systems by creating comprehensive periodic evaluation plans including network vulnerability and infrastructure penetration assessments. Our greatest strength lies with our team of industry certified personnel. Each one carries extensive C&A and Independent Verification and Validation (IV&V) experience and will work to assist each agency to achieve total security risk mitigation.

Featured Solutions

Gold. The Gold product aims to provide FISMA compliant Security Test and Evaluation and Risk Assessment to a Federal Information Systems enterprise by implementing the minimum security guidelines set forth by the National Institute of Standards and Technology (NIST).

These include:

- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information System FIPS Publication 200, Minimum Security Requirements for Federal Information and Federal Information Systems
- NIST Special Publication 800-30, Revision 1, Risk Assessment Guideline
- NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST Special Publication 800-39, NIST Risk Management Framework
- NIST Special Publication 800-53 Revision 2, Recommended Security Controls for Federal Information Systems
- NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
- NIST Special Publication 800-59, Guide for Identifying an Information System as a National Security System
- NIST Special Publication 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories

The plan specifies security test requirements and vulnerability tools for any and all devices, applications, and components within the agency infrastructure accreditation boundary to ascertain the level of compliance.

Our effective and proven standards and procedures include:

- Periodic review of information security policies and procedures.
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls.
- Periodic risk assessments, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.
- Effective review of continuity of operations procedures for information systems that support the operations and assets of the organization.

Platinum. The Platinum product offers the highest level of Security Test and Evaluation and Risk Assessment by various Federal Agencies' Office of the Inspector General (OIG) in performing information security audits. The process is an aggressive evaluation of the agency's information systems enterprise to ensure not only FISMA compliance but total risk mitigation.

This plan follows the procedures laid out in the Federal Information System Controls Manual (FISCAM) that evaluates the reliability of computer generated data supporting financial statements or to evaluate the adequacy of controls in systems to help reduce the risk of loss due to errors, fraud, and other illegal acts and disasters or other incidents that cause the systems to be unavailable. This product aims to pinpoint security deficiencies specifically related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, and physical security.

The Platinum service helps prepare Federal Agencies for GAO or OIG information security audits in advance. It includes all of the services available in the Gold product plus an in depth review to assure GAO or OIG audit conformity.

Procedures involve examination of the agency's environment and correcting weaknesses in risk assessments, security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions.

Some of the key factors to be reviewed and assessed include but are not limited to:

- Security Policies and Procedures
- Security Configuration Settings
- Contingency Planning
- Incident Response Planning
- Security Awareness and Training
- Physical Security
- Personnel Security
- Access Control Mechanisms
- Identification and Authentication Mechanisms
- Audit Mechanisms
- Encryption Mechanisms
- Firewall and Network Security Mechanisms
- Intrusion Detection Systems
- Anti-Viral Software
- Smart Cards