Product Brief

AT&T Security Consulting

Information Assurance – Federal Information Security Management Act (FISMA)

Introduction

Ensuring the confidentiality, integrity and availability of information resources is a complex undertaking for any organization. Add in a multitude of regulations that govern this process for government agencies, and you may need the support of AT&T Security Consulting. Our Consulting experts assist agencies in addressing industry best practices and provide Security Authorization Process, formerly Certification and Accreditation (C&A) solutions delivered by experienced specialists in federal IT security.

The AT&T Consulting Process

AT&T Consulting will serve as a resource to you as you work to meet your regulatory and compliance requirements under the Federal Information Security Management Act of 2002, of general support systems and major applications. We provide an independent assessment of the SSP and its implementation to evaluate the security controls for the information system.

The AT&T Consulting methodology is based on National Institute of Standards and Technology (NIST) Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," and is easily adapted to meet agencies' own internal C&A process. The assessment methodology is sufficiently flexible to evaluate systems in all lifecycle stages, systems under evolutionary development, and single-purpose or legacy systems. Our assessment methods and procedures include:

- Interviews with agency personnel associated with the security aspects of the system
- Review and examination of security-related policies, procedures and documentation
- Observation, analysis, testing and evaluation of security-relevant and security-critical aspects of system hardware, software, firmware and operations
- Conducting demonstrations and exercises

If needed, we will create tailored assessment methods and procedures for specific information-system implementations. In the majority of cases, assessment procedures follow the NIST 800-37 phases of the following:

Initiation

The Initiation phase helps ensure that the authorizing official and senior agency security officials are in agreement with the contents of the SSP, before AT&T Consulting begins the assessment of the security controls in the information system. There are three tasks in this phase:

- Preparation, notification and resource identification
- Categorize Information System
- System security plan (SSP) analysis and acceptance

Security Assessment

The Security Assessment phase helps determine the extent to which the security controls in your agency's information systems are implemented correctly, operating as intended and producing the desired outcome. This phase addresses specific actions taken or those planned to correct deficiencies in your agency's security controls. AT&T Consulting

Benefits

- Reduce time and resources spent demonstrating effectiveness of IT controls
- Maintain continuous compliance
- Identifies gaps in your agency's security program and FISMA reporting
- Provides detailed recommendations for remediating or maintaining compliance. Dedicated resources help allow your agency team members to focus on business issues rather than security matters

Features

- Validates policies, procedures
- Provides configuration management
- Provides certification and accreditation
- Recommends and delivers remediation plans
- Conducts security awareness training

at&t

provides your agency's authorizing official with information to help you determine the risk to operations, assets, or individuals. There are two tasks in this phase:

- Security control selection and assessment (risk assessment-RA, and security test and evaluation-STE)
- Security control assessment documentation

Security Authorization

The Security Authorization phase helps determine if the remaining known vulnerabilities in your agency's information system pose a level of risk that is acceptable to your agency's operations, assets and individuals. Upon completion, your agency's authorizing official may make one of the following three decisions:

- Authorization to operate the information system
- Interim authorization
- Denial of authorization

There are two tasks in this phase:

- Security authorization decision
- Security authorization documentation

Continuous Monitoring

Finally, the continuous monitoring phase provides oversight of the security controls in your agency's information systems, informing the agency's authorizing official when changes occur that may impact system security. AT&T Security Consulting works with your agency officials to perform the activities in this phase throughout the life cycle of the agency's information systems.

There are three tasks in this phase:

- Configuration management and control
- Security control monitoring
- Status reporting and documentation

Summary

Completing a security accreditation helps ensure that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that re-accreditation occurs periodically in accordance with federal or agency policy or if a significant change to the system or its operational environment occurs.

Solution: What You Get

AT&T Consulting produces the following documents during the Security Authorization process:

- Information System Security Policy (ISSP)
- Security Requirements Document/ Traceability Matrix
- Certification Test and Evaluation (CT&E) Plan
- Security Test and Evaluation (ST&E) Plan
- Residual Risk Assessment Results
- Security Education, Training, and Awareness Plan
- Incident Response Plan
- Contingency Plan
- Certification and Authorization Statement

AT&T Differentiators

AT&T Security Consulting engagements use industry standards best practices:

- Value-oriented, professional project management
- Efficient, repeatable processes
- Staff expertise in C&A
- Cleared personnel
- Operator of Critical Infrastructure, as designated by U.S. Department of Homeland Security

Certification & Authorization Statements

AT&T Consulting prepares a Security Authorization Statement, which documents the results of the security controls assessment and provides the Designated Approving Authority (DAA) with information to help make a credible, risk-based decision on whether to authorize operation of the information system. AT&T does not provide legal advice or recommendations.

Key Benefits

AT&T Consulting takes a holistic approach in assisting in your security reviews, addressing elements of people, technology, and processes. We combine in-depth knowledge and use of Information Security Standards of Good Practice (SOGP), applicable regulatory requirements and our experience in information security management practices within the industry.

Security Solutions: Expertise from a Trusted Provider

AT&T provides a unique and world-class portfolio of assessment, compliance and related security services. Our extensive capabilities, expertise, and commitment to open standards have established us as a strategic and Trusted Advisor with our customers. With AT&T you can expect a global network of proven technology, and a cost-effective program-based approach to meet all of your security and compliance needs.

For more information contact your AT&T Representative, visit us at www.att.com/consulting/security, email us at mss@att.com, or call 1 877 954-7771.

06/29/11 AB-2162