GOVDATAHOSTING

Streamlined FISMA Compliance for Federal Information Systems in the Cloud

GovDataHosting Cloud Solutions Overview

Created exclusively to serve the demanding hosting needs of Federal, State and Local government agencies, GovDataHosting serves as a unique cloud solutions provider that delivers governmental proven past performance, exceptional value and hosting industry's best practices at a cost-effective price.

FedRAMP

GovDataHosting is a specialized government cloud provider of service bundles that include FedRAMP certified Infrastructure as a Service platform, security compliance, application support and disaster recovery services to help government agencies reduce the cost and complexity of leveraging modern cloud technology in support of its mission.

Hosted within our own FedRAMP certified cloud storage, computing and telecommunications infrastructure, your system will be supported by technology specialists experienced in all aspects of FISMA compliance.

What is FISMA Compliance?

FISMA, originally the Federal Information Security Management Act of 2002, was updated as Federal Information Security Modernization Act of 2014. By setting a uniform policy for information security across the Executive Branch of the government, 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.

FISMA requirements are applicable to all civilian agencies (Department of Housing, U.S. Department of Homeland Security, Department of Commerce), as well as the Department of Defense, the Intelligence Community and many pseudo-government organizations.

Specifically, FISMA requires federal departments and agencies to:

- Maintain an inventory of information systems
- Categorize information systems by mission impact
- Implement policies and procedures to reduce risk to an acceptable level
- Certify and accredit the information systems according to the level of risk
- Implement the appropriate technical, management and operational security controls
- Periodically test the applicable information assurance controls
- Provide appropriate security training to employees and contractors
- Implement procedures for security incident response and continuity of operations
- Report periodically on information security posture status

The benefits of FISMA compliance leads to:

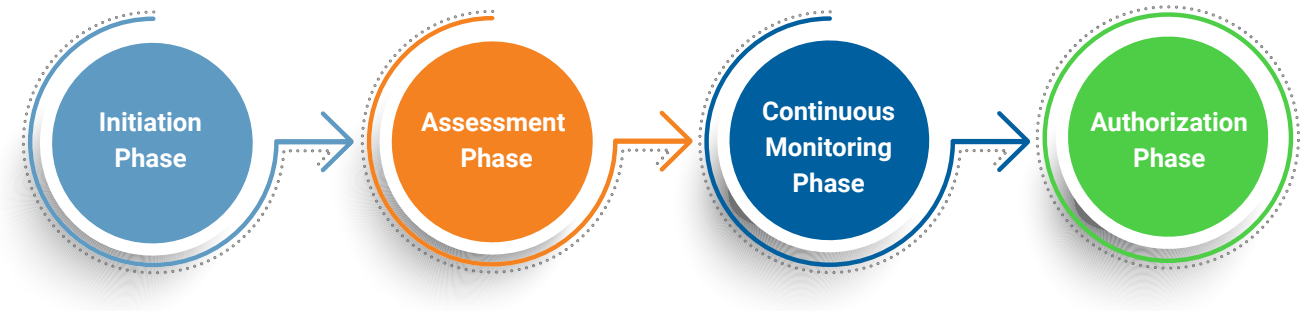
- The implementation of cost-effective, risk-based information security programs
- Consistent and cost-effective application of security controls across the federal government information technology infrastructure
- Improved, comparable, and repeatable information security control assessments
- Enterprise-wide mission risks visibility for all information systems
- Improved information systems security for the critical infrastructure of the United States

Federal Assessment and Authorization Process

The Assessment and Authorization (A&A) process is the process where the government assesses (audits) the policies, procedures, controls and contingency planning of each Federal government information system.

The A&A process is much more comprehensive than just a security audit of the application or the server infrastructure. The A&A process incorporates a thorough review of the organization's security policies and procedures (management controls), physical facility infrastructure (operational controls) as well as network, server and application security testing, penetration testing and scanning (technical controls).

A&A process lifecycle is comprised of the following 4 phases:



The Initiation Phase consists of three tasks: (i) preparation; (ii) notification and resource identification; and (iii) system security plan analysis, update, and acceptance. The purpose of this phase is to ensure that the authorizing official and senior agency information security officer are in agreement with the contents of the system security plan, including the system's documented security requirements, prior to initiation of the security control assessment.

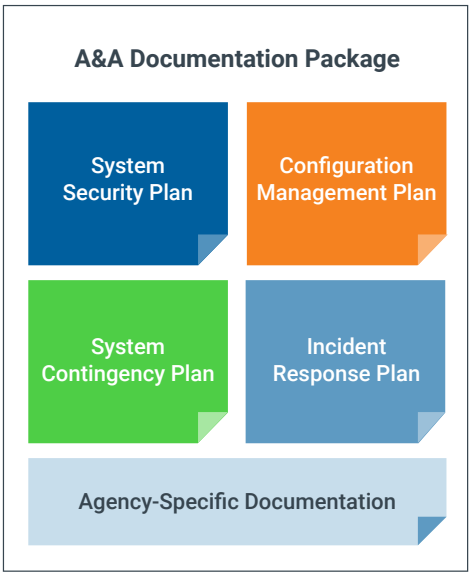
The Assessment Phase consists of two tasks: (i) security control assessment; and (ii) security assessment reporting documentation. The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system in accordance to its risk classification. Risk classification is established by the government in accordance with Federal Information Processing Standards as part of the A&A process initiation.

The Authorization Phase consists of two tasks: (i) security authorization decision; and (ii) formal security authorization documentation. This phase is completed when a high-ranking government official responsible for the information system security approves the operation of the information system by issuing an Authorization To Operate (ATO) based on the results of the assessment documentation and audit of all applicable technical, operational and management security controls.

The Continuous Monitoring Phase consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system.

A&A Documentation Package

The goal of the preparation for the A&A process is to compile a collection of information system-specific documents that describe the security posture of the system, evaluate risks, and makes recommendations for correcting any known deficiencies. These documents are commonly known as the A&A Documentation Package.



A typical A&A Documentation Package usually contains at least a half a dozen components, though significantly more documentation is required if the system contains PII, PHI or high risk data.

Once an A&A Documentation Package is prepared, the government agency information assurance managers review the package and make decisions on whether or not the systems should be accredited. Each system must receive an Authority to Operate (ATO) before a system can be used for production purposes.

In preparing an A&A package, the following components are prepared as required:

- System Overview
- Stakeholder Identification
- System Security Boundary
- Network and System Diagrams
- Software, Firmware and Hardware Inventory
- System Risk Assessment
- System Contingency Plan
- Self-Assessment
- System Security Plan
- Other agency-specific documents

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

NIST Based A&A Methodology

NIST created a series of Special Publications that provide specific A&A security requirement (control) guidance on implementing the provisions of FISMA and related policies. These Special Publications collectively define a Risk Management Framework for Federal information systems.

NIST based A&A process is defined in *NIST Special Publication 800-37 Revision 2 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, while NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations* contains a standardized set of applicable security control requirements for information systems, grouped by functional areas as listed in Table 1 below.

Table 1. Applicable Security Controls Based On NIST SP 800-53 Revision 4

Class	Control Subject Area	Low Baseline	Moderate Baseline	High Baseline
Management	Risk Assessment	4	7	8
Management	Planning	3	6	6
Management	System and Services Acquisition	7	14	18
Management	Security Assessment and Authorization	7	10	12
Operational	Personnel Security	8	8	9
Operational	Physical and Environmental Protection	10	18	26
Operational	Contingency Planning	6	22	35
Operational	Configuration Management	8	21	31
Operational	Maintenance	4	9	13
Operational	System and Information Integrity	6	21	27
Operational	Media Protection	4	9	12
Operational	Incident Response	7	12	16
Operational	Awareness and Training	4	5	5
Technical	Identification and Authentication	15	22	24
Technical	Access Control	11	35	43
Technical	Audit and Accountability	10	18	28
Technical	System and Communications Protection	10	24	30
		124	**261**	**343**

The Federal Information Processing Standard - *FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, and NIST SP 800-60 Revision 1 - Guide for Mapping Types of Information and Information Systems to Security Categories*, provide guidance on categorizing information systems and their data. Confidentiality, integrity and availability requirements are assessed to uniquely arrive at risk classification for each information system. The following are risk levels applicable to information system risk categorization under NIST A&A methodology: Low Risk, Moderate Risk or High Risk.

Streamlined A&A Process

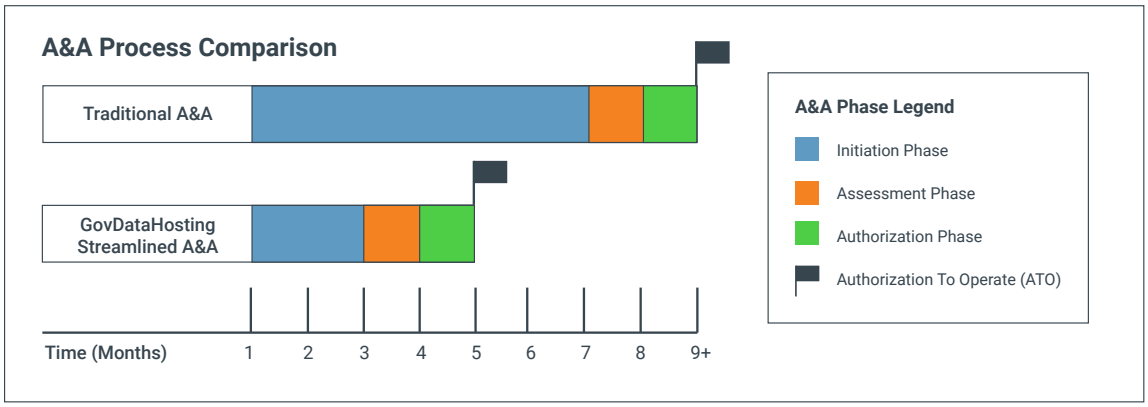
A traditional approach of accomplishing an ATO through the A&A process for a cloud hosted moderate risk system can last from 6 to 12 months and may involve a large number of technology, security and documentation specialists to accomplish all the necessary compliance tasking.

GovDataHosting's unique bundled approach significantly streamlines the A&A process by accelerating both Initiation and Assessment phases of the process, which has a dramatic schedule-reducing effect on the overall process.

To streamline each customer's system Initiation and Assessment phases GovDataHosting utilizes:

- Technical personnel experienced in NIST and FedRAMP security compliance
- Security management personnel experienced in the preparation of the A&A Documentation Package
- NIST, FedRAMP and agency-specific document templates
- Operational, Management and Technical controls that already have been audited by independent 3rd parties, FedRAMP and federal agencies
- FedRAMP-certified cloud infrastructure audited by the government

Illustration 1. Traditional A&A vs. GovDataHosting Streamlined A&A Process Comparison



Benefits of Streamlined A&A Process

A streamlined A&A process can be viewed by the stakeholders as beneficial from a number of different perspectives:

- Decrease in A&A process duration by over 50%
- Decrease the A&A process cost by over 50%
- Significant decrease of system deployment risk
- Predictable and successful system authorization (ATO)
- Increase in customer and stakeholder satisfaction

GOVDATAHOSTING

Please contact us for further information on how we can streamline your A&A process with our FISMA compliant cloud hosting bundles.

Corporate Headquarters
9160 Red Branch Road
Columbia, MD 21045

Tel 410.884.1004
Fax 410.884.0412
U.S. Toll Free 800.967.1004