Streamlined FISMA Compliance For Hosted Information Systems

Faster Certification and Accreditation at a Reduced Cost

IT CNP Inc.

:: Executive Summary

Federal, State and Local Government agencies alike are increasingly turning to web-based outsourced hosted solutions.

Achieving an operational level of FISMA security compliance is time and resource intensive, even for hosted solutions.

IT-CNP has a mature methodology to minimize the time and risk associated with information system Certification and Accreditation process.

:: Hosted Solutions Overview

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

GovDataHosting.Com is a division of IT-CNP, Inc., a national provider of FISMA compliant secure hosting, information management and cyber security services as a standard set of its service offerings.

IT-CNP provides industry leading certified professionals with solid technical background experience, able to support a full range of cyber security, hosted hardware and software support issues.

For hosted Federal information system under our care, we specialize in providing a package of secure FISMA compliant hosting solutions, required level of security controls and a set of all-inclusive C&A documentation support services to accommodate all aspects of government security requirements.

Hosted systems within our secure NIST and DIACAP compliant telecommunications infrastructure are supported by technology specialists experienced in all aspects of FISMA compliance.

:: What Is FISMA Compliance?

FISMA is the Federal Information Security Management Act of 2002. It was passed as Title III of the E-Government Act (Public Law 107-347) in December 2002.

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, the Department of Defense, the Intelligence Community and many quasi-government organizations. Specifically, FISMA requires federal departments and agencies to:

- Maintain an inventory of information systems
- Categorize information systems by risk
- Implement policies and procedures to reduce risk
- Certify and accredit information systems
- Implement the appropriate security controls
- Periodically test information assurance controls
- Implement continuity of operations
- Implement security incident response

The benefits of FISMA compliance lead to:

- The implementation of cost-effective, risk-based information security programs
- The establishment of a level of security due diligence for federal agencies and contractors
- Consistent and cost-effective application of security controls across the federal government information technology infrastructure
- Enterprise-wide mission risks visibility for all information systems
- Improved information systems security for the critical infrastructure of the United States

:: Certification and Accreditation

The Certification and Accreditation (C&A) process is the process whereby the government audits the policies, procedures, controls and contingency planning of each Federal government information system.

The C&A process is much more comprehensive than just a security audit of the application or the server infrastructure. The C&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), encompassing four phases.

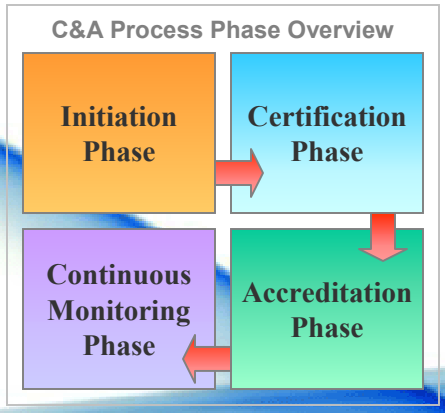
- Initiation Phase
- Security Certification Phase
- Security Accreditation Phase
- Continuous Monitoring Phase

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, before the assessment of the security controls in the information system.

The Certification Phase consists of two tasks: (i) security control assessment; and (ii) security certification 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 meet the security requirements for the system in accordance to its risk classification.



The Accreditation Phase consists of two tasks: (i) security accreditation decision; and (ii) security accreditation documentation.

This phase is completed when a high-ranking government official approves the operation of the information system by issuing an Authorization To Operate (ATO) based on the results of the certification 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 oversee and monitor 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.

The C&A process is much more comprehensive than just a security audit of the application or the server infrastructure.

The C&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).

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 re-accreditation occurs periodically in accordance with federal or agency policy and whenever there is a significant change to the system or its operational environment.

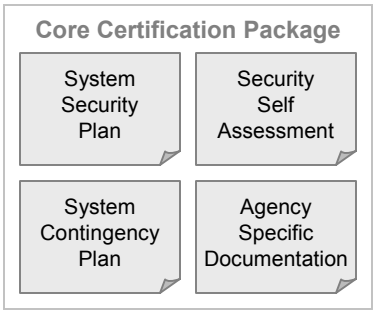
Each system must receive an ATO before a system can be legitimately used for production purposes.

:: C&A Certification Package

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

A typical Certification Package usually contains at least a half a dozen components, though significantly more documentation is required if the system contains classified information or high risk data.

Once a Certification Package is prepared, the government agency IA auditors review the package and make decisions on whether or not the systems should be accredited.



In preparing a C & A Certification 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.

:: C&A Methodologies

To comply with FISMA requirements, the following two C&A methodologies are mainly used.

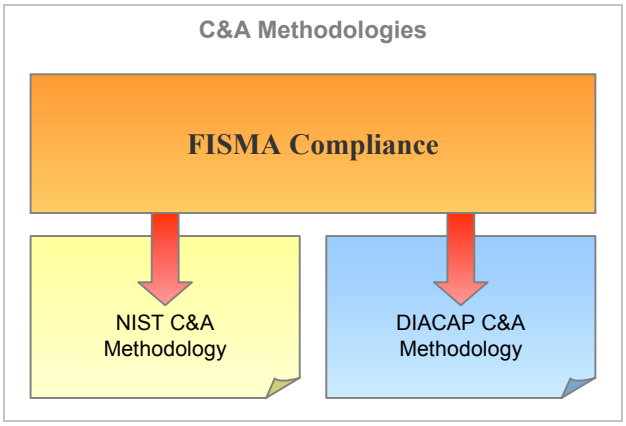
- **NIST C&A Methodology** is used for most civilian (e.g. Transportation, HUD, USDA, Commerce, Treasury) and quasi-government agencies. NIST stands for the National Institute Of Standards and Technology.
- **DIACAP C&A Methodology** is used for the Department of Defense agencies. DIACAP stands for the Defense Information Assurance Certification and Accreditation Process.

:: NIST C&A Methodology

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

NIST C&A process is defined in Special Publication 800-37 while Special Publication 800-53 contains a standardized set of applicable security control requirements for information systems, grouped by functional areas as listed below.

NIST Control Subject Area	# of Controls
Risk Assessment	5
Planning	5
System and Services Acquisition	11
Certification, Accreditation and Security Assessments	7
Personnel Security	8
Physical and Environmental Protection	17
Contingency Planning	10
Configuration Management	7
Maintenance	6
System and Information Integrity	12
Media Protection	7
Incident Response	7
Awareness and Training	4
Identification and Authentication	7
Access Control	20
Audit and Accountability	11
System and Communications Protection	19



:: DIACAP C&A Methodology

DIACAP C&A Methodology is driven by the U.S. Department of Defense (DoD) regulatory policy listed in DoD Directive 8500 (Information Assurance).

All applicable DIACAP Information Assurance (IA) controls are referenced in DoD Instruction 8500.2 (Information Assurance Implementation) and grouped by functional areas as listed in below.

DIACAP Control Subject Area	# of Controls
Security Design and Configuration	31
Identification and Authentication	9
Enclave and Computing Environment	48
Enclave Boundary Defense	8
Physical and Environmental	27
Personal	7
Continuity	24
Vulnerability and Incident Management	3

Under the DIACAP methodology, each information system is classified as one of the following Mission Assurance Categories (MAC):

- MAC I (equivalent of high risk and availability)
- MACII (equivalent of moderate risk and availability)
- MAC III (equivalent of low risk and availability)

Additionally, the Confidentiality Level (CL) measures each information system's confidentiality requirements based on the type of information processed. The CL categories used are Classified, Sensitive and Public.

To determine the applicable level of DIACAP IA controls applicable to a specific system, the government uses a combination of both the MAC and CL levels (e.g. MACII, Public). Each of the 9 unique MAC/CL combinations are cross-referenced to a set of applicable IA controls for each information system.

:: Streamlined NIST and DIACAP C&A Processes

IT-CNP significantly streamlines the C&A process by accelerating the Initiation Phase of the process. To streamline the Initiation Phase IT-CNP utilizes:

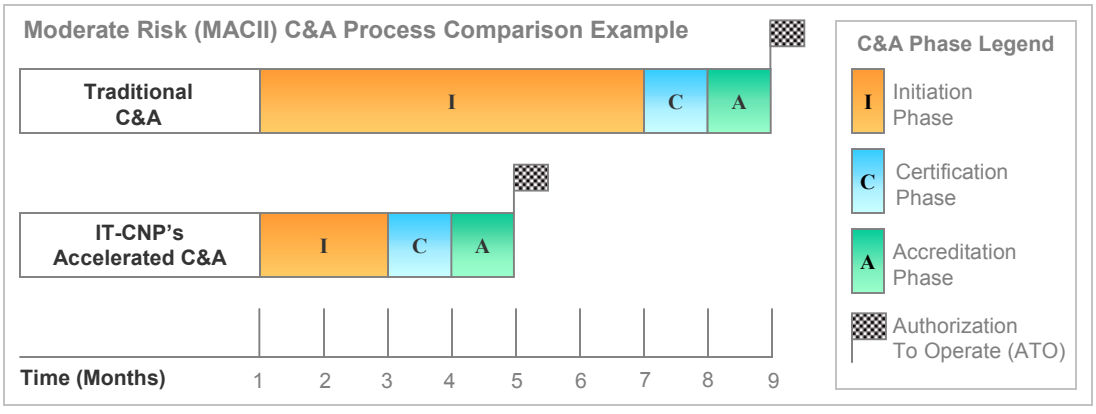
- Technical personnel experienced in NIST and DIACAP
- Documentation personnel experienced in the preparation of the Certification Package
- Proven NIST and DIACAP artifact document templates
- Operational, Management and Technical controls that have been audited by the government
- Datacenter facilities audited by the government

Benefits of IT-CNP's Streamlined C&A Process

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

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

IT-CNP significantly streamlines the C&A process by accelerating the Initiation Phase of the process, which has a dramatic effect on the overall process.



A traditional approach of accomplishing a C&A process on a hosted moderate risk system can last from 7 - 9 months to accomplish all the necessary compliance tasking while IT-CNP's streamlined process typically takes 3 - 4 months. Please contact us for further information how we can streamline your C&A process with our FISMA compliant hosting infrastructure.

About IT-CNP

IT-CNP, Inc., is a leading national provider of the premier government-oriented high availability hosting, information management, cyber security and custom helpdesk solutions. Created exclusively to serve the demanding hosting needs of Federal, State and Local government agencies, IT-CNP serves as a unique government oriented hosting solutions provider that delivers proven government past performance, solid value and secure hosting industry's best practices.

Corporate Headquarters
9160 Red Branch Road
Columbia, MD 21045
Tel 410.884.1004
Fax 410.884.0412
U.S. Toll Free 800.967.1004

www.it-cnp.com
www.govdatahosting.com