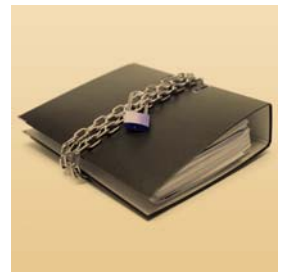


CERTIFICATION AND ACCREDITATION

Achieving Secure Information Systems



CSC
NORTH AMERICAN
PUBLIC SECTOR

CSC

Security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program. (NIST 800 SP-37).

Why Choose CSC?

CSC focuses on assisting clients develop, document, and institutionalize information security programs consistent with FISMA and other legislative and regulatory requirements, such as NIST, DITSCAP, DIACAP, HIPAA, DCID, NIACAP, E-Gov and Sarbanes-Oxley.

CSC has integrated tools that help ensure timely FISMA compliance, proven processes that have resulted in a steady climb in FISMA scorecard grades for their clients and a high level of customer satisfaction.

CSC employs more than 1,000 security and information assurance professionals worldwide. Our certified professionals include CISSPs, ISSMPs, ISSAPs, and CAPs.

IT Infrastructure Solutions

15000 Conference
Center Drive
Chantilly, Virginia 20151
1.703.818.4300
www.csc.com/itis

Overview

As a requirement of the Office of Management and Budget Circular A-130, Appendix III, Security Certification and Accreditation (C&A) of government systems and applications provides quality control, and challenges managers and technical staffs to implement effective security controls in their information systems, given mission requirements, technical constraints, operational constraints and cost/schedule constraints.

The C&A process is a standardized approach that provides guidance on the activities and the associated level of effort required based on assurance requirements. Assurance is defined as a measure of confidence that the security features, attributes and functions enforce the security policy.

Assurance refers to the evidence presented as to the correctness and effectiveness of the security controls applied to that system. Certification verifies and validates the security assurance for a system associated with an environment. Accreditation evaluates whether the risks associated with residual weaknesses are tolerable or unacceptable.

FISMA requires that all information systems be certified and accredited every three years and reviewed on an annual basis. The security controls that are applied to an information system are found in NIST 800-53, Recommended Security Controls for Federal Information Systems. These controls form the basis of an effective information security program, which include:

- Develop and review policy and procedures
- Create and track POA&Ms
- Perform security testing and assessments

- Support the accreditation process
- Define accreditation boundaries
- Provide C&A support
- Evaluate management
- Provide security awareness training and technical controls

Benefits

- Allows management to make credible, informed decisions whether or not to accept risks
- Allows for consistent, comparable and repeatable assessments of security controls
- Promotes a better understanding of the mission risks resulting from the operation of information systems
- Assures the system's security controls are implemented correctly, operating as intended and are producing the desired results
- Assesses the magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification or destruction of information
- Compliance with NIST SP 800-53 controls CA-1 through CA-7

Automated Tools

CSC's Enterprise Network Managed Services Center of Excellence (ENMS COE) serves as an optimal environment for research development, evaluation and testing. Automated C&A tools are fully available in the COE for demonstration. These tools have enabled CSC to create a standardized, repeatable C&A process, which provides a more cost-efficient bottom line.