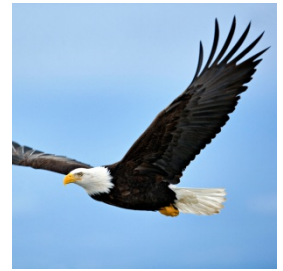


FISMA

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

CSC FISMA Service Offering: Managing the Complexities of IT Compliance



CSC
NORTH AMERICAN
PUBLIC SECTOR

CSC

CSC will leverage our expertise and experience to work with federal agencies to exceed information security management, as well as technical and operational controls. We have the track record to support our success in making other agency IT systems secure, and we can do the same for you.

CSC employs more than 1,000 security and information assurance (IA) professionals worldwide whose certifications include CISA, CISSP, SSAP, ISSEP, NAS IAM/IEM, SANS, and CCNP. These IA professionals are the backbone of the organization that will get your agency into federal compliance.

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

Background

The Federal Information Security Management Act (FISMA) of 2002 (enacted as Title III of the E-Government Act of 2002) is the primary legislation governing federal information security. FISMA requires reporting on security compliance through a set of standard internal controls driven by the National Institute for Standards and Technology (NIST) — Special Publication 800-53.

Even with a strong working Security Operations Center, integrated workflow processes and a trained, certified staff, security architectures can still be exposed to risk. A comprehensive security management program is absolutely essential to a complete solution. Security management starts with a sound security policy and ends with automated compliance reports that map back to the management, operational and technical controls outlined in NIST 800-53.

CSC's Approach

CSC's approach to security management consists of five major phases:

Phase 1 - Organizational and Technical Enterprise Assessment

Phase 2 - Design and Implementation of Enterprise Security Compliance Architecture

Phase 3 - Customization and Optimization of Architecture

Phase 4 - Establishment of Enterprise Security Compliance Outreach Program

Phase 5 - Ongoing Solution Expansion and Support

Each phase is part of an integrated solution that combines proven processes, tailored commercial off-the-shelf (COTS) software and experienced and knowledgeable security experts.

The phases are also compliant with federal agency, NIST, and industry best practice security guidelines and regulations.

CSC's approach will provide senior federal information security managers with report improvements for their required yearly FISMA response. More importantly, following these steps will secure an agency's network assets, as well as provide a scalable, repeatable and maintainable security solution.

Turnaround at the EPA

Federal agencies are graded annually on their security performance. In 2000, the Environmental Protection Agency (EPA) was 35 percent compliant based on internal technical measures. In 2002, the agency received a D- on its Federal Computer Security Report Card. Determined to improve its performance, the EPA brought in CSC, a Tier 1 global systems integrator.

CSC developed a FISMA compliance solution for the EPA based on a coordinated enterprise-wide approach to security operations, as well as the handling and management of computer security incidents and policy. CSC's solution centralizes security services and management into a unified architecture, making it easy to follow, repeatable, adaptable to pilot program certification and scalable.

CSC has provided EPA with dramatic improvements within the information systems security arena. EPA's last three consecutive "A" ratings on their FISMA Report Card demonstrate CSC's ability to deliver a sound FISMA solution for federal agencies.