



FISMA RESOURCE CENTER

FISMA/NIST CONSULTING SERVICES FOR FEDERAL INFORMATION SYSTEMS

“Establish a fundamental level of security ‘due diligence’ for federal agencies ... based on minimum security requirements...”

... Dr. Ron Ross, NIST

FISMA/NIST BACKGROUND

It is federal government policy that all information systems receive formal Security Authorization (authority to operate) from a designated senior official, based on a technical analysis of the system's compliance with an assigned set of Security Controls (i.e., requirements) that provides an assessment of the system's risk level. This process of compliance analysis and formal authorization is also known as certification and accreditation (C&A).

Formal Security Authorization of information systems is part of a broader Risk Management Framework (RMF) established by federal agencies in accordance with FISMA, the Federal Information Security Management Act. RMF roles and responsibilities, process steps, and documentation deliverables are detailed in National Institute of Standards and Technology (NIST) Special Publication 800-37. Security Controls are detailed in NIST SP 800-53.

THE PROGRAM MANAGER'S DILEMMA

The Program Manager/System Manager's primary responsibility is to oversee the development and maintenance of a system that fulfills its stated mission. However, in order for the system to be put into operation, it must receive authorization to operate (accreditation). The Program Manager must therefore ensure the appropriate risk management activities are integrated into the system life cycle. Usually there is a support contractor in place to provide system development and integration services, but additional Information Security support is often needed to oversee risk management activities.

In response to this need, the FISMA Resource Center is pleased to offer information security consulting services to federal program and system managers.

FISMA/NIST CONSULTING SERVICES

Our FISMA/NIST consulting services include, but are not limited to, the following:

- Supporting the Program Manager in identifying key personnel, forming a risk management team, and conducting a successful “project kickoff”
- Supporting the team in determining the FIPS 199 categorization, then selecting and augmenting the baseline security controls
- Supporting the team in initiating and executing a security authorization (C&A) project plan
- Supporting the system development team in design/implementation of assigned security controls



- Developing documentation, such as policies, procedures and other “artifacts”, in support of the authorization process
- Supporting the team in evaluating compliance with assigned security controls, both technical and non-technical
- Supporting the Program Manager during the security controls assessment process
- Developing the authorization (C&A) package, including the System Security Plan (SSP), Risk Assessment (RA), Security Assessment Report (SAR), and Plan of Action & Milestones (POA&M)
- Supporting the Program Manager in maintaining “continuous monitoring” of security posture, conducting annual reviews as required by FISMA, and conducting re-authorization as required

CONTRACTUAL ARRANGEMENTS AND FEES

FISMA consulting engagements may be done on a “firm fixed price” or “time and materials” basis. If a firm fixed price arrangement is desired, the quoted cost will be dependent upon the number and complexity of systems, and the breadth of desired services. For “time and materials” engagements, an initial estimated number of hours will be given, and adjusted thereafter based on progress and issues encountered.

FISMA/NIST TRAINING

FISMA Resource Center also offers classroom training to government and industry. We currently offer a one-day *FISMA/NIST Risk Management Fundamentals* and a three-day *FISMA/NIST Risk Management In Depth* course. Both courses are presented on a regularly-scheduled basis in Washington, DC, and at selected locations nationwide. If you have a group (normally 8-10 trainees or larger), we can also arrange to bring one of our instructors to your site. A registration form for the regularly-scheduled courses is available at www.fedca.org. For an on-site training quotation, please contact us at 540-808-1050.

ABOUT US

FISMA Resource Center is an independent consulting organization dedicated to assisting federal agencies and their suppliers in understanding and implementing the RMF.

FISMA Resource Center is a division of BAI Information Security Consultants. BAI has been a provider of information technology and security consulting services since 1974, specializing in security authorization (certification and Accreditation) of federal information systems. BAI founder and principal consultant Lon Berman has over 35 years’ experience and is a recognized authority on certification and accreditation of federal information systems.

CONTACT US

For more information, please contact FISMA Resource Center:

Phone: 540-808-1050

FAX: 540-808-1051

E-mail: fedca@fedca.org



**Information Security Consultants
Federal C&A Resource Center**

7467 Bluff View Dr • Fairlawn, VA 24141
540-808-1050 • FAX 540-808-1051
fedca@fedca.org • www.fedca.org