



FISMA RESOURCE CENTER

FISMA/NIST CONSULTING SERVICES FOR SERVICE PROVIDERS

“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 SERVICE PROVIDER’S DILEMMA

As a commercial service provider offering (or wishing to offer) your service(s) for sale to the federal government, you will sooner or later run into the dreaded “FISMA wall.” Potential customers may ask you if your service or system has been authorized or accredited, or even ask for a copy of your “certificate.” However, unlike many other government product certification programs, you as a vendor cannot independently seek FISMA/NIST security authorization!

The RMF (and its Security Authorization component) is fundamentally a *government* process, carried out by government *people*. Agencies required “outsourced” service providers to undergo the authorization process as if they were government-owned systems. The question is – what can the government reasonably expect vendors to provide in support of this authorization effort?

First and foremost, the answer is *information* – in the form of documented evidence of compliance with applicable federal security requirements. Service providers can maximize their “readiness” for formal authorization by:

- thoroughly analyzing their organization and IT environment’s compliance with applicable security requirements
- making product improvements to enhance compliance where necessary
- documenting compliance in a manner that is readily *usable* and *understandable* by government customers and conducive to a determination of risk acceptability.

Secondly, the answer is *support and teamwork*. Even though RMF is the government’s own process, it is often not well understood by the government people tasked with carrying it out. The best way to ensure success is for the government and the service provider to work as a



team. A knowledgeable vendor can facilitate the process and gain valuable credibility with the DoD customer at the same time.

In response to these needs, the FISMA Resource Center is pleased to offer the following consulting services geared specifically to address the needs of product developers and vendors:

- *FISMA/NIST Compliance Survey* – a “short-turnaround” service to provide you with a basic view of your compliance with applicable federal security requirements, and a set of practical recommendations for compliance improvement.
- *FISMA/NIST Readiness Assessment* – a much more comprehensive service that includes extensive “hands on” testing to provide a detailed view of your compliance, detailed technical recommendations, and a security documentation package formatted according to government standards.
- *FISMA/NIST Liaison Consulting Services* – a consulting service designed to help “bridge the gap” between your organization and your current or potential federal customers.

FISMA/NIST COMPLIANCE SURVEY

Our *FISMA/NIST Compliance Survey* consulting engagement is designed to quickly provide an assessment of your level of compliance with federal security standards and offer practical recommendations for compliance improvement. A *FISMA/NIST Compliance Survey* can typically be completed in 21 days or less, and includes the following activities:

- Inbrief teleconference. In this meeting, we present a short overview of FISMA and RMF, receive an overview from your company, identify key individuals within your organization, and identify documents for review.
- Interview and document review. We will review the documents you have provided, supplemented by discussion with appropriate persons in your organization, in order to gather additional information about your service and its supporting IT infrastructure, and begin to evaluate its security functionality against the applicable federal information security controls and standards.
- On-site compliance review. We will meet with your team to review the federal information security requirements and assess your level of compliance.
- Written report. We will document the results of these activities in a *FISMA/NIST Compliance Survey Report*, consisting of an executive summary and an evaluation of your compliance, including recommended steps for compliance improvement.

FISMA/NIST READINESS ASSESSMENT

Our *FISMA/NIST Readiness Assessment* consulting engagement offers a much more detailed compliance evaluation, including “hands on” testing of your IT environment. Depending on the complexity of your environment, a *FISMA/NIST Readiness Assessment* may take 10-12 weeks, or more, to complete. Typically, the *FISMA/NIST Readiness Assessment* will entail the following activities:

- Inbrief. If you have not already completed a *FISMA/NIST Compliance Survey*, we will conduct an inbrief teleconference as described above.
- Document reviews and discussions. We will review your documentation at a technical level, and conduct interviews with appropriate personnel within your organization.



- Test plan. Based on review of your documentation and follow-up technical discussions, we will develop a comprehensive plan for testing your infrastructure's security functionality and compliance.
- On-site testing. We will spend several days at your facility conducting observations and "hands on" testing (with a variety of security testing tools), along with follow-up discussions, in order to evaluate the technical aspects of your service and IT infrastructure security.
- Analysis. Information from document reviews, discussions and on-site testing will be analyzed to produce a detailed assessment of compliance with each of the applicable federal requirements, and to develop a set of recommendations for compliance improvement and risk mitigation.
- In-process briefing. We will verbally present the "highlights" of our findings and recommendations.
- Development of deliverables. In addition to a comprehensive *FISMA Compliance Report* and executive summary, we will also provide a documentation package (*System Security Plan (SSP)*, *Security Assessment Report (SAR)*, *Risk Assessment Report (RAR)*, and *Plan of Action and Milestones (POA&M)*), formatted in accordance with federal standards.
- Outbrief meeting, in which we present our "final" set of findings and recommendations, based on the deliverable documents.

The deliverables from the *FISMA/NIST Readiness Assessment* will play a major role in facilitating formal authorization of your service's "installed base" of customers within the federal government. Also, they will serve as a powerful weapon in your company's marketing arsenal. In some cases, this can be the "competitive edge" that separates your service offering from that of your competitors.

FISMA/NIST LIAISON CONSULTING SERVICES

Our *FISMA/NIST Liaison* consulting engagement is designed to assist you in working with your government customers (and potential customers) on security-related matters. Services we can perform in this capacity include, but are not limited to:

- participation in pre- or post-sales meetings with your government customers as an information assurance "subject matter expert"
- assisting your government customers in understanding your service and IT infrastructure security features and regulatory compliance, or even the RMF itself
- assisting your staff in drafting appropriate security language for proposals and marketing material
- assisting your staff in drafting security-related language in technical documentation such as configuration and operation manuals, etc.

CONTRACTUAL ARRANGEMENTS AND FEES

FISMA/NIST Compliance Survey engagements are typically done on a "firm fixed price" basis.

FISMA/NIST Readiness Assessment 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 the environment to be analyzed, 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 Liaison consulting engagements are typically done on a “time and materials” basis. We initially recommend a “block” of hours to be allocated in the form of a purchase order. We will then track utilization of these hours and provide a monthly statement along with our invoice.

OTHER CONSULTING SERVICES

Policy and Procedures Development. If the compliance analysis of your service or IT infrastructure recommends development of additional policy and/or procedures documents, it may be worthwhile to consider using outside assistance to prepare them rather than diverting your valuable product development or support resources. Our consultants can develop the required documents at a reasonable cost and with minimal disruption to your staff.

Information Security Engineering. If the compliance analysis of your IT infrastructure or environment recommends development of additional technical security safeguards, our consultants can provide the needed engineering support to make such product enhancements efficiently. We are experienced in the implementation and integration of security technologies such as firewalls, intrusion detection systems, encryption devices, etc.

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: fisma@fisma1.org



Information Security Consultants
FISMA Resource Center

7467 Bluff View Dr • Fairlawn, VA 24141
540-808-1050 • FAX 540-808-1051
fisma@fisma1.net • www.fisma1.net