BAI Information Security Consulting & Training

Risk Management Framework (RMF) Resource Center

www.rmf.org

RMF Consulting Services for Service Providers

RMF Background

DoD and Federal agencies require that all information systems receive formal Authorization to Operate (ATO) from a senior official prior to being placed into operation, and periodically thereafter. The decision to grant ATO is based on an assessment of risk that includes a comprehensive analysis of compliance with an extensive set of technical and non-technical security controls. This is all part of an overarching life cycle process called the Risk Management Framework (RMF). RMF roles and responsibilities, process steps, and documentation deliverables are detailed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and in DoD Instruction (DoDI) 8510.01. Security controls are published in NIST SP 800-53.

The Developer's Dilemma

As a commercial service provider offering (or wishing to offer) your services to DoD and federal agencies, you will sooner or later run into the dreaded RMF requirement. Potential customers may ask you if your organization has been "RMF approved," or even ask for a copy of your "authorization." However, unlike many other government authorization programs, you as a vendor cannot independently seek RMF approval!

RMF is fundamentally a government process, carried out by government people. DoD and federal agencies are required to assess and authorize their information systems in accordance with RMF. DoD/Federal agencies require "outsourced" commercial services to have ATO just as they do for government owner/operated information systems. The question is – what can the government reasonably expect vendors to provide in support of the RMF effort?

First and foremost, the answer is information – in the form of documented evidence of compliance with applicable security requirements. Service providers can maximize their "readiness" for RMF by:

- thoroughly analyzing their IT environment's compliance with RMF security controls (requirements)
- making 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 *their* 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 vendor to work as a team. A knowledgeable vendor can facilitate the process and gain valuable credibility with the DoD/Federal customer at the same time.

In response to these needs, BAI is pleased to offer the following consulting services geared specifically to address the needs of "outsourced" service providers:

- RMF Compliance Survey – a "short-turnaround" service to provide you with a basic view of your compliance with applicable security requirements, and a set of practical recommendations for compliance improvement.
- RMF 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 key RMF documentation.
- RMF Liaison Consulting Services – a consulting service designed to help "bridge the gap" between your organization and your current or potential DoD/Federal customers.

BAI Information Security Consulting & Training

Risk Management Framework (RMF) Resource Center

www.rmf.org

RMF Consulting Services for Service Providers

RMF Compliance Survey

Our RMF Compliance Survey consulting engagement is designed to quickly provide an assessment of your level of compliance with RMF security standards and offer practical recommendations for compliance improvement. An RMF Compliance Survey can typically be completed in 30 days or less, and includes the following activities:

- Inbrief teleconference. In this meeting, we present a short RMF overview, receive a service 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, gather additional information about your organization and IT environment, and begin to evaluate its security functionality against the applicable RMF controls and standards.
- Compliance review. We will meet with your team to review the RMF security requirements and assess your level of compliance.
- Written report. We will document the results of these activities in an RMF Compliance Survey Report, consisting of an executive summary and an evaluation of your compliance, including recommended steps for compliance improvement.

RMF Readiness Assessment

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

- Inbrief. If you have not already completed an RMF Compliance Survey, we will conduct an inbrief teleconference as described above.
- Document reviews and discussions. We will review your system 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 security functionality and compliance.
- On-site testing. We will spend a few 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 IT security. Alternatively, this can be accomplished by arranging for “remote access” to your IT infrastructure.
- 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 RMF requirements, and a set of recommendations for compliance improvement and risk mitigation.
- In-process briefing. We will verbally present the “highlights” of our findings and recommendations.

RMF Consulting Services for Service Providers

- Development of deliverables. In addition to a comprehensive RMF Compliance Report and executive summary, we can also provide RMF documents such as System Security Plan (SSP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M).
- Outbrief meeting, in which we present our "final" set of findings and recommendations, based on the deliverable documents. The deliverables from the RMF Readiness Assessment will play a major role in facilitating assessment and authorization of your outsourced service by your DoD/Federal customer. 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.

RMF Liaison Consulting Services

Our RMF 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 current or potential DoD/Federal customers as an information assurance "subject matter expert"
- assisting your government customers in understanding your environment's security features and regulatory compliance, or even the RMF process itself
- acting as your "in house" security expert during the "full life cycle" of RMF evaluation by your current or potential DoD/Federal customers
- assisting your staff in drafting appropriate security language for proposals and marketing material
- assisting your staff in drafting security related language for operating manuals, etc.

Contractual Arrangements and Fees

Compliance Survey engagements are typically done on a "firm fixed price" basis. RMF 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 infrastructure 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. RMF 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.

BAI Information Security Consulting & Training

Risk Management Framework (RMF) Resource Center

www.rmf.org

RMF Consulting Services for Service Providers

Policy and Procedures Development

If the compliance analysis (either RMF Compliance Survey or RMF Readiness Assessment) 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 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 organization recommends development of additional technical security safeguards, our consultants can provide the needed engineering support to make such IT enhancements efficiently. We are experienced in the implementation and integration of security technologies such as firewalls, intrusion detection systems, encryption devices, etc.

Next Steps

BAI would be pleased to work with you to explore the ways in which our consulting services can be beneficial to your organization and program. Please contact us at 1-800-RMF-1903 (763-1903) or e-mail rmf@rmf.org to schedule a discussion of your requirements.

Need Training?

In addition to consulting services, BAI also offers instructor-led training to government and industry. We currently offer a four-day RMF training program, consisting of a one-day Fundamentals class and a three-day In Depth class. Additionally, we offer training in Continuous Monitoring and other RMF-related subject matter. Training is presented on a regularly-scheduled basis at selected locations nationwide, and in an online, instructor-led format. Training can also be provided to a group of students at your site. Registration for regularly-scheduled classes is available at https://register.rmf.org. If you are interested in on-site training, please contact BAI at 1-800-RMF-1903 (763-1903).

About BAI

BAI is a small business specializing in information security training and consulting. Principal consultant Lon Berman has 40+ years IT and information security experience and is a recognized RMF subject matter expert.