BAI Information Security Consulting & Training

Risk Management Framework (RMF) Resource Center

www.rmf.org

# RMF Consulting Services for DoD & Federal Agencies

## 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 Standard 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 Program Manager's Dilemma

The Program Manager/System Owner'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 an ATO. The Program Manager must therefore ensure that RMF activities are integrated into the system life cycle. Normally there is a support contractor in place to provide system development services, however additional information security support is often needed to oversee RMF activities. In response to this need, BAI is pleased to offer RMF consulting services to DoD and Federal programs.

## RMF Consulting Services

Our RMF consulting services include, but are not limited to, the following:

- Supporting the Program Manager in identifying key personnel, forming an RMF team, and conducting a successful RMF "project kickoff"
- Supporting the RMF team in determining system categorization and selecting/augmenting the baseline security controls (security requirements)
- Supporting the RMF team in initiating and executing a System Security Plan (SSP)
- Supporting the system development team in implementation of security controls and developing documentation, such as policies, operating procedures, "as built" documentation and other "artifacts", in support of the RMF process
- Supporting the RMF team in evaluating compliance with security controls
- Supporting the Program Manager and development contractor to ensure system information is appropriately entered into the organization's RMF support system (e.g., eMASS for DoD)
- Supporting the Program Manager and development contractor to properly prepare for independent assessment (testing)
- Supporting the Program Manager during the assessment process
- Supporting the Program Manager in developing the Authorization Package, including the System Security Plan (SSP) and Plan of Action & Milestones (POA&M)
- Supporting the Program Manager in maintaining Authorization, conducting annual reviews as required by FISMA, and conducting re-Authorization as required
- Supporting the Program Manager in transitioning from DIACAP to RMF (where applicable).

# RMF Consulting Services for Federal Agencies



## Contractual Arrangement and Fees

If the scope of work and expected deliverables are well-defined, RMF consulting engagements can be done on a “firm fixed price” basis. If, however, there are significant uncertainties, a “time and materials” arrangement may be more appropriate, in which case an initial estimated number of hours will be provided, and adjusted thereafter based on progress and issues encountered. In either case, BAI can work as a direct contractor to DoD or as a subcontractor to an existing system developer/integrator. BAI is listed in the Central Contractor Registry (CAGE Code 1TGB3), and holds a SECRET facility clearance.

## 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 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 Us

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.