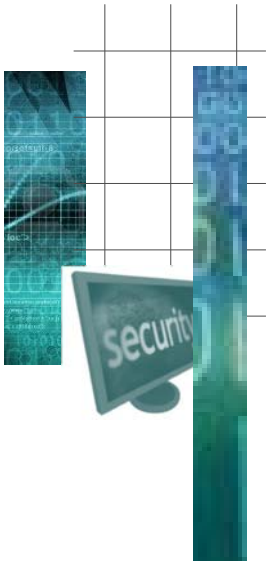
Risk Management Framework Today

... and Tomorrow



July, 2018
Volume 8, Issue 3

Find us on LinkedIn

In this issue:

NIST SP 800-37 Rev. 2

By Lon J. Berman CISSP, RDRP

The National Institute of Standards and Technology (NIST) is in the process of preparing Special Publication (SP) 800-37 Rev 2 for publication. As you may know, NIST SP 800-37 is the publication that defines the Risk Management Framework (RMF) roles, responsibilities and life cycle process. A review of the SP 800-37 Rev 2 Draft (hereafter referred to as simply "Rev 2") reveals several significant changes and new content.

The title of Rev 2 has been changed from "Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach" to "Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy." This re-titling is significant in two ways. Firstly, the word "Federal" has been removed from the title. This is reflective of NIST's desire to include private industry in its quest to make cyberspace a more secure place. Secondly, the word "Privacy" has been added, to further emphasize the critical connection between security and privacy – only with a strong security program can organizations protect the privacy of individuals.

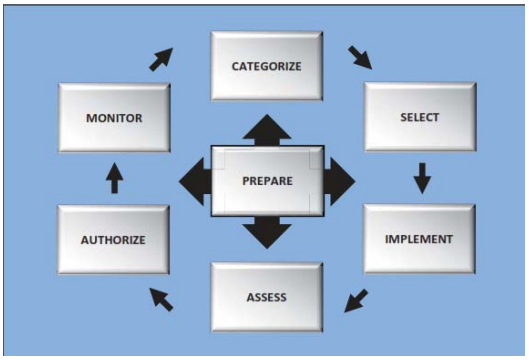
Rev 2 addresses alignment of RMF with the NIST Cybersecurity Framework by providing specific cybersecurity framework "mapping" within the various RMF steps and activities.

Privacy risk management concepts are now integrated into the RMF life cycle. Rev 2 also encourages use of the consolidated security and privacy controls catalog in NIST SP 800-53 Rev 5.

Rev 2 pays increased attention to supply chain risk management considerations, such as untrustworthy suppliers, counterfeiting, tampering, malicious code, etc.

Rev 2 also provides an alignment of RMF with the systems engineering process as documented in NIST SP 800-160.

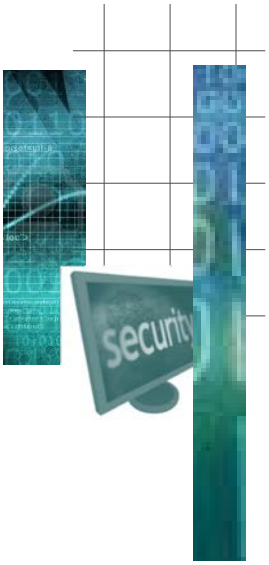
In terms of the RMF life cycle itself, a Prepare step has now been added in Rev 2, so the full life cycle now looks like this:



It is interesting to note that this Prepare step has long been a topic in BAI's RMF training, where it is referred to as "Step 0".

Rev 2 also offers an organization-generated control selection approach as an alternative to the traditional baseline control selection approach.

Another public draft is slated for publication in July, with final publication of NIST SP 800-37 Rev 2 planned for October.



NIST 800-171: Confusion & the Protest Docket

By Kathryn Daily, CISSP, RDRP

"... a lack of clarity on the requirements themselves will result in additional protests of contract awards ..."

I'm sure by now you've at least familiarized yourself with NIST 800-171, "Protecting Unclassified Information in Nonfederal Information Systems and Organizations." What wasn't made clear was how DoD will evaluate a contractor's System Security Plan (SSP). In May, DoD released draft DoD Guidance for Reviewing System Security Plans and the "NIST SP 800-171 Security Requirements Not Yet Implemented" which provided some answers but also included ambiguous evaluation criteria.

New Guidance suggests that the Government's evaluation of Contractors' SSP will be used as selection criteria in new contract awards. Additional guidance has been provided in the form of an SSP Priority Ranking Matrix which gives a value to each security requirement that is not implemented. The newly released guidance provides a few competing scenarios detailing different implementations in which the offeror's compliance with stated standards are considered in source selection.

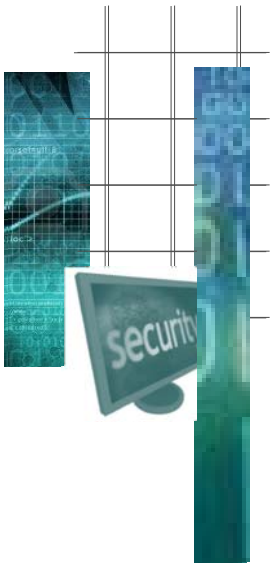
Scenario 1: The clause is included in the contract, but not evaluated at time of award; basically, the offeror self-attest to their compliance with NIST SP 800-171. The cybersecurity requirements will have no bearing on contract award or performance. Within this scenario, DoD could assess/track implementation of the 800-171 security requirements after contract award by including cybersecurity language in the statement of work and/or as data requirements.

Scenario 2: A DoD contracting office could evaluate an offeror's compliance with NIST SP 800-171 as part of source selection. DoD could make an acceptable/unacceptable decision based on the implementation status of the NIST 800-171 requirements.

Scenario 3: DoD acquisition evaluators could assess an offeror's implementation of its SSP as a separate technical evaluation factor with evaluation consisting of an assessment of the contractor's SSP as a stand-alone document or an independent government assessment to validate the implementation of each requirement of the SSP using evaluation tools identified in NIST SP 800-171A.

Regardless of the scenario, it is likely that evaluation of technical requirements by non-IT acquisition personnel coupled with a lack of clarity on the requirements themselves will result in additional protests of contract awards.

Questions regarding NIST 800-171 can be directed to kathryn@rmf.org.



Online Personal STIG Lab Technology™

By P. Devon Schall, M.S., MA.Ed. CISSP, RDRP

At BAI RMF Resource Center our primary focus is to provide the most relevant and advanced RMF and RMF ancillary service training in the cybersecurity industry. In delivering curriculum and instruction, learning theories are of paramount importance to us in effectively meeting the stated goal above.

A very popular model in the field of instructional design and technology is Bloom's Taxonomy. Bloom's model consists of six levels of knowledge types which are presented visually in the shape of a pyramid. An illustration of Bloom's Taxonomy is outlined in Figure 1.

As shown in Figure 1, Bloom's Taxonomy culminates in a tier titled Creating which demonstrates mastery of a specific topic. Bloom's states that the higher the student rises to the top of the knowledge type pyramid, the more mastery the student possesses of the subject being studied.

"... BAI's STIG 101 subject matter experts provide coaching assistance..."

Bloom's Taxonomy relates directly to the recent development of STIG 101 which supports our flagship *RMF for DoD IT* and *RMF for Federal Agencies* training programs. In creating STIG 101, our primary course developer was struggling in creating effective STIG curriculum. She did not want to create yet another PowerPoint deck in training a topic as technical as STIG's.

Her solution led to the creation of Online Personal STIG Lab Technology™. Via this training methodology, students are given access to individual virtual lab environments where they perform hands on application of STIG settings. Via Online Personal STIG Lab Technology™ BAI's STIG 101 subject matter experts provide coaching assistance as the students work through a variety of STIG implementation exercises.

By allowing the students to Create their own STIG settings, we have had immense success in providing them with the knowledge needed to leave our training and return to their work environment with the tangible technical skills necessary to begin the STIGing process.

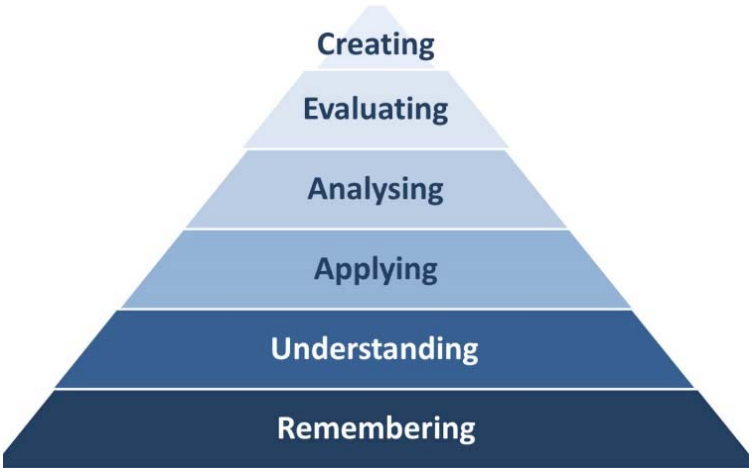
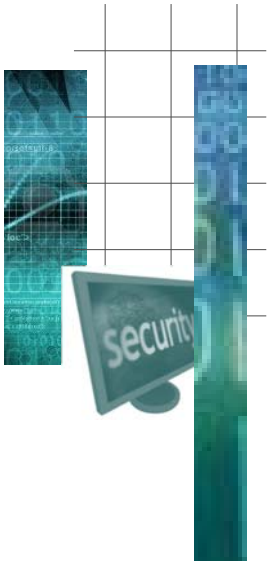


Figure 1. Bloom's Taxonomy.



RMF Efficacy Research

RMF Community:

In August of 2015, I began the pursuit of obtaining my Doctorate of Philosophy (Ph.D.) in Information Technology with the majority of my coursework focused on cybersecurity. Fast forward three years, and I am excited to have recently received dissertation topic approval which focuses on RMF effectiveness in relation to formalized RMF training. Over the coming months, I will be reaching out to the RMF community to collect survey data on the perceived shortfalls of RMF from an effectiveness and implementation standpoint.

After conducting a literature review of RMF related topics, I found RMF has been studied very minimally at an academic level. Most of the available literature on RMF consists of white papers and informal conference presentations. Literature reviewed to date indicates RMF practitioners and RMF decision-makers are frustrated and feel that RMF may not be meeting the goals and objectives it originally defined for itself, but as previously stated, minimal research has been conducted on viable solutions to combat these perceived RMF shortfalls. My research seeks to provide solutions in the ways in which RMF can be successful and hopefully curb the trend of frustration and finger pointing in blaming NIST for creating cumbersome ineffective policy.

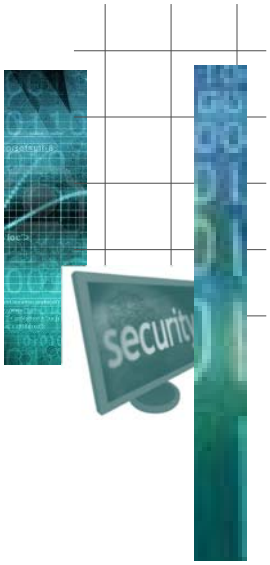
"...I plan to present the findings the RMF community provides me to the authoring team at NIST..."

I recognize this study of RMF efficacy cannot fix RMF entirely, but I hope I can collect enough data and the data collected indicates trends in the perception and real-world experiences of those attempting to implement RMF. Without getting into the granular details of research methodology, I will be reaching out to the RMF community at large by sharing a link to my data collection instrument. I recognize as a society, we have become inundated with questionnaires and they are quite the annoyance. With all of this being said, if you see a link sent from me to a questionnaire on RMF Efficacy in the coming months, I graciously ask you to take a few minutes of your time to provide your valuable experiences.

At BAI RMF Resource Center, we consider ourselves leading experts in RMF training as well as the study of RMF. As an RMF scholar, I hope to present the findings you provide me to the authoring team at NIST and hopefully take a step in the right direction of strengthening the cybersecurity posture of our nation.

Sincerely,

Devon Schall, MS, MAEd, CISSP, RDRP
Executive Director Training Services
BAI Information Security
devon@rmf.org



Training for Today ... and Tomorrow

Our training programs:

- **RMF for DoD IT** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, security controls, and transition from DIACAP to RMF.
- **RMF for Federal Agencies** – recommended for Federal "civil" agency (non-DoD) employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, and security controls.
- **eMASS eSSENTIALS** – designed as an add-on to RMF for DoD IT. This training program provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is utilized.
- **Continuous Monitoring Overview** – designed as an add-on to RMF for DoD IT. This is a one day "fundamentals" program.
- **RMF in the Cloud** – designed as an add-on to RMF for DoD IT. This one-day training program will provide students the knowledge needed to begin shifting their RMF efforts to a cloud environment.
- **Certified Authorization Professional (CAP) Preparation** – designed as a one-day add-on to RMF for DoD IT. CAP Prep provides preparation for the Certified Authorization Professional (CAP) certification administered through $(ISC)^2$.
- **STIG 101** – is designed to answer core questions and provide guidance on the implementation of DISA Security Technical Implementation Guides (STIGs).

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region (Pentagon/Crystal City area), Dallas, Pensacola, and San Diego.
- **Online Personal Classroom™** – regularly-scheduled training programs are also offered in an online, instructor-led format that enables you to actively participate from the comfort of your home or office
- **On-site training** – our instructors are available to deliver any of our training programs to a group of students from *your* organization at *your* site; please contact BAI at 1-800-RMF-1903 to discuss your requirements
- **TrainPlus! & Registered DoD RMF Practitioner (RDRP)** – BAI offers ancillary support services such as TrainPlus! which is a free monthly conference call offered to our alumni staffed with RMF subject matter experts. We also offer a program titled RDRP that provides registrants access to a valuable community of RMF for DoD practitioners.

Regularly-scheduled classes through December, 2018:

RMF for DoD IT—4 day program (Fundamentals and In Depth)

- **National Capital Region ▪ 1-4 OCT**
- **Huntsville ▪ 24 - 27 SEP ▪ 10 - 13 DEC**
- **Pensacola ▪ 13-16 AUG ▪ 5-8 NOV**
- **Colorado Springs ▪ 27-30 AUG ▪ 3-6 DEC**
- **San Diego ▪ 17-20 SEP**
- **Dallas ▪ 30 JULY - 2 AUG ▪ 29 OCT - 1 NOV**
- **Online Personal Classroom™ ▪ 20 - 23 AUG ▪ 24 - 27 SEP ▪ 22 - 25 OCT ▪ 26 - 29 NOV ▪ 10 - 13 DEC**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 6 SEP ▪ 13 NOV**
- **National Capital Region ▪ 5 OCT**
- **Huntsville ▪ 28 SEP ▪ 14 DEC**
- **Pensacola ▪ 17 AUG ▪ 9 NOV**
- **Colorado Springs ▪ 31 AUG ▪ 7 DEC**
- **San Diego ▪ 21 SEP**
- **Dallas ▪ 3 AUG ▪ 2 NOV**

Continuous Monitoring Overview —1 day program

- **Online Personal Classroom™ ▪ 25 JUL ▪ 30 OCT**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 8 AUG ▪ 15 NOV**

CAP Prep—1 day program

- **Online Personal Classroom™ ▪ 5 SEP ▪ 29 OCT**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 28 SEP ▪ 26 OCT ▪ 14 NOV ▪ 30 NOV ▪ 14 DEC**

Contact Us!

RMF Today ... and Tomorrow is a publication of BAI Information Security, Fairlawn, Virginia.

Phone: 1-800-RMF-1903
Fax: 540-518-9089
Email: rmf@rmf.org

Registration for all classes is available at https://register.rmf.org

Payment arrangements include credit cards, SF182 forms, and Purchase Orders.

BAI