Risk Management Framework Today

Formerly DIACAP Dimensions

… and Tomorrow

February, 2016
Volume 6, Issue 1

In this issue:

Building A Security Control Baseline "Step-by-Step"

By Lon J. Berman, CISSP

In the last issue of *RMF Today and Tomorrow*, we walked through the System Categorization process step-by-step. Now that we've categorized our system, let's take a look at the steps for creating a Security Control Baseline.

Step 1: Create Initial Control Set

Your System Categorization defines the initial set of Security Controls for your baseline. NIST SP 800-53 is the source of the controls themselves, but it is CNSSI 1253 that lists the controls that are applicable to your particular categorization level.

For example, suppose your system is categorized as Confidentiality-Moderate, Integrity-Moderate, Availability-Low. Using Table D-1 in CNSSI 1253, you can readily determine the controls and control enhancements that will comprise your initial control set. Each row in the table that contains an "X" or a "+" under *one or more* of your three categorization levels belong in your control set.

Step 2: Apply Overlays

Security Control Overlays have been developed for several "communities of interest," including classified systems, intelligence systems, space platforms, and privacy systems. If your system meets one or more of these criteria, you'll need to carefully read and apply each element of the overlay to your initial control baseline. Overlays typically add numerous new controls or control enhancements to the baseline, and also provide supplemental guidance for various controls.

Overlays are published on the CNSS website, **www.cnss.gov**.

Note that if you are using an automated tool such as eMASS (Enterprise Mission Assurance Support Service), these first two steps can be accomplished by "checking the boxes" for your system categorization levels and applicable overlays.

Step 3: Apply Scoping Guidance

Once you have a control set with any applicable overlays, you are in a position to review each of the controls to see if any of them are Not Applicable to your system. For example, some of the technical controls refer to specific technologies you may not be using. Note that any control deemed Not Applicable should be accompanied by appropriate justification.

Step 4: Supplement the Control Set

Perhaps your system employs unique technologies or exists in an environment containing unique threats. In such cases, consider adding security controls to your baseline to ensure appropriate safeguards are implemented.

Fortunately, NIST SP 800-53 contains numerous Security Controls that are not in any of the "standard" baselines. Rather, they are intended for use, if needed, to address unique technologies or threats.

The ideal way to identify those areas requiring control set supplementation is to conduct an initial risk assessment of your system.

Step 5: Determine Organization-defined Values

As you examine the security controls in your nearly completed baseline, you'll

See *Security Control Baseline*, Page 2

System Scans in eMASS ... Think Before You Upload!

By Kathryn M. Farrish, CISSP

eMASS, short for Enterprise Mission Assurance Support Service, is a comprehensive tool provided by DoD for managing the RMF life cycle. Among its well-known features and capabilities are generating security control baselines, managing RMF workflow, maintaining a repository of documentation artifacts, accepting system owner provided "self assessment" of security control implementation and compliance, accepting validation results from independent assessors, managing Plan of Action and Milestones (POA&M), and providing a variety of reports , including the System Security Plan and Security Assessment Report.

Now available in eMASS is a module called the Asset Manager. Using this capability, system owners can enter information about each asset (e.g., server, workstation, network device) comprising their system. The Asset Manager also offers the ability to "ingest" system scans from vulnerability scanners such as ACAS (Assurance Compliance Assessment Solution) and configuration compliance scanners such as SCC (SCAP Compliance Checker).

Before getting all excited about this capability, keep in mind the rather primitive access control in eMASS. At present, anyone with an eMASS account has read-only access to every record in the database. What this means is if you upload scans of your system that reveal technical vulnerabilities, you are in essence revealing those vulnerabilities to the entire eMASS user community!

Consider yourself warned.

***Security Control Baseline* from Page 1**

see that many of them are really not 100% complete. They are replete with "blanks" that need to be filled in with what are called "organization-defined values". For example, security control CM-6 states:

The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization - defined information system components] based on [Assignment: organization-defined operational requirements]; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

It is up to the System Owner to "fill in" each of the bracketed items with the actual values for the system.

In some cases, DoD will provide a "default" for an organization-defined value. This is often the case with numerical parameters like frequencies for review of policies and procedures. The general rule of thumb is that system owners are free to provide their own value, so long as it "equals or exceeds" the DoD-specified "minimum."

Step 6: Document Results

If automated tools like eMASS are in use, generating a System Security Plan report will provide documentation of the full Security Control Baseline. As is the case for the System Categorization, the System Owner should be prepared to brief the Authorizing Official (AO) on the Security Control Baseline if requested.

"The System Owner should be prepared to brief the Authorizing Official (AO) on the Security Control Baseline if requested."

Top Ten—Questions for your Authorizing Official

By Annette Leonard

The importance of the Authorizing Official (AO) in the RMF process is self-evident. As the individual charged with signing your Authorization to Operate (ATO), the AO is obviously a key player. Ideally, the AO's role is not limited to that final signature—he/she should be an active participant in the process from the very beginning.

Since most AOs are senior level officials, they often employ AO Designated Representatives (AODRs) to work directly with the system owners.

This edition of the RMF Top Ten focuses on some questions you might want to ask your AO or AODR.

10. Are you available to participate in our periodic RMF status meetings? It's great to have AO representation at your meetings so the AO can be kept abreast of your progress and questions can be addressed promptly.

9. Do you need a copy of our RMF project schedule? Most AOs and AODRs like to stay in touch with their system owners to make sure they are progressing in their RMF efforts. A copy of your project schedule (and periodic updates as necessary) will help them to stay up-to-date.

8. Are there any documentation artifacts you particularly want to see? If you are using eMASS, the AO/AODR should have access to your eMASS record and therefore have visibility into all your documentation artifacts. However, there may be one or two that he/she is particularly interested in. If you know that as a system owner, you can take actions (e.g., sending an offline copy of the particular artifact) that can ingratiate you with the AO.

7. What are your expectations for our Continuous Monitoring program? Other than the "standard" DoD monitoring tools (HBSS, ACAS), the AO may have a particular desire to see other forms of monitoring or periodic review.

6. How do we go about arranging for independent assessment? Each DoD Component (Army, Navy, Air Force, Marine Corps, etc.) is responsible for developing its own methodology and "style" of independent assessment. The AO/AODR should be able to point you to any online resources or potentially even "recommend" an assessor team.

5. Do you need a brief when we have completed our System Categorization? Some AOs insist on a formal brief of the categorization process and results. Others will agree to look at your documentation and nothing more. Still others will brush it off with "well, if that's what you think your system categorization is, then that's what it is."

4. Do you need a brief when we have completed our security control baseline? Again, some AOs will want to see a formal presentation of overlays, tailoring, etc. Others are content the system owner is best qualified to make these decisions.

3. Do you need a brief when we have completed our independent assessment? It's rare, but some AOs like to get preliminary feedback on assessments as they take place rather than waiting for an "official" Security Assessment Report.

2. Do you need a brief when the authorization package comes to you from the SCA? Many AOs will rely on the SCA recommendation, but others will insist on a formal "decision brief" from the System Owner, highlighting the residual risks and POA&M items, prior to signing the ATO.

1. Is there anything else you need us to do to be successful? It sounds trite to say, but AOs are human beings too. Each of them may have particular things they want to see happen—or don't want to see happen—during the RMF process. It's best to find out about any such "quirks" sooner rather than later.

Security Control Spotlight—STIGs and Controls

By Kathryn M. Farrish, CISSP

"...there is most definitely a tie-in between Security Controls and STIGs..."

One of the primary goals of the RMF life cycle is for a system to achieve and maintain compliance with a baseline of Security Controls in accordance with NIST SP 800-53 and CNSSI 1253. Security controls provide specific safeguards in numerous subject areas (aka. "families"), including access control, audit and accountability, identification and authentication, contingency planning, incident response, configuration and change management, physical and environmental security, etc.

Systems are also required to maintain compliance with applicable Security Technical Implementation Guides (STIGs). STIGs, published by DISA, provide configuration specifications for operating systems, database management systems, web servers, network devices, etc.

When confronted with these two major components of the RMF process, system owners may wonder if the Security Controls and STIGs are completely independent entities, or if there is some sort of relationship between them. As you might expect, Security Controls and STIGs are closely related.

To better understand the relationship, let's take a look at one of the configuration settings in the Windows STIG.

Vulnerability ID: V-63461

Rule Title: The system must be configured to generate error reports

Vulnerability Discussion: Enabling Windows Error Reporting generates information useful to system administrators and forensics analysts for diagnosing system problems and investigating intrusions. If Windows Error Reporting is turned off, valuable system diagnostic and vulnerability information may be lost.

This STIG setting requires the Windows Error Reporting feature to be enabled, and provides a specific procedure to check the status of this feature in the system services. If the specified service is not present or not running, this is a finding. The STIG then provides the following reference for this finding:

CCI: CCI-001312

That is precisely the tie-in between STIGs and Security Controls that we're looking for! What is tells us, in essence, is that if this STIG item is incorrectly set, CCI 001312 (part of Security Control SI-11) should be considered non-compliant.

This tie-in is not a new concept. For several years, each STIG item contained a reference to the corresponding DIACAP IA Control from DoDI 8500.2.

To say the least, it is challenging to find Security Controls or CCIs that precisely "map" to many of the STIG specifications. In such cases, the "catch-all" is to map these STIG specifications to CCI-000366, which is part of Security Control CM-6. CM-6 as a whole is concerned with the use of security configuration checklists. CCI-000366 specifically states:

The organization implements the security configuration settings.

Other CCIs within CM-6 specify the DISA STIGs and SRGs as the preferred source documents for security configuration specifications.

Historically, the "catch-all" for DIACAP control references was ECSC-1.

For some time now, DISA has been revising each of the STIGs to include CCI references; however, there still may be some legacy STIGs that do not include CCI references.

Contact Us!

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

Phone: 1-800-RMF-1903
Fax: 540-808-1051
Email: rmf@rmf.org

Training for Today … and Tomorrow

BAI currently offers <u>three</u> training programs:

- **RMF for DoD IT** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; covers the new RMF life cycle and NIST security controls, the CNSS enhancements, *and* the transition from DIACAP to RMF. The program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **RMF for Federal Agencies** – recommended for federal "civil" agency employees and contractors (non-DoD); covers RMF life cycle and NIST security controls. Program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **Information Security Continuous Monitoring (ISCM)** – open to all, however prior knowledge of RMF is recommended. This is a three day "In Depth" program.

Regularly-scheduled classes through June, 2016 are as follows:

RMF for DoD IT (Fundamentals and In Depth)

- **29 FEB-3 MAR 2016 (National Capital Region)**
- **21-24 MAR 2016 (Colorado Springs / Online Personal Classroom™)**
- **18-21 APR 2016 (National Capital Region)**
- **25-28 APR 2016 (Online Personal Classroom™)**
- **16-19 MAY 2016 (Huntsville)**
- **23-26 MAY 2016 (Online Personal Classroom™)**
- **13-16 JUN 2016 (Colorado Springs)**
- **20-23 JUN 2016 (Online Personal Classroom™)**

RMF for Federal Agencies (Fundamentals and In Depth)

- **14-17 MAR 2016 (Online Personal Classroom™)**
- **6-9 JUN 2016 (Online Personal Classroom™)**

Information Security Continuous Monitoring

- **10-12 MAY 2016 (Online Personal Classroom™)**

For the most up-to-date training schedule, pricing information, and any newly-added class dates or locations, please visit **http://register.rmf.org**.

Online registration and payment is available at **http://register.rmf.org**. Payment arrangements include credit cards, SF182 forms, or purchase orders.

Classroom training. We offer regularly-scheduled classroom training at our training centers in Colorado Springs, Huntsville, National Capital Region (DC area) and Virginia Beach.

Online Personal Classroom™ training. This method enables you to actively participate in our regularly-scheduled instructor-led classes from the comfort of your home or office.

On-site training. Our instructors are available to present one or more of our training programs at *your* site. All you need is a group of students (normally at least 8-10) and a suitable classroom facility. Cost is dependent upon class size, so please contact us at 1-800-RMF-1903 (763-1903) to request an on-site training quotation. Note we can also provide Online Personal Classroom™ training to a "private" group of students from *your* organization.