Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

November, 2015
Volume 5, Issue 3

In this issue:

System Categorization "Step by Step"	1
What is STIG Viewer?	2
Top Ten—STIGs	3
Security Control Spotlight—A Little Good News	4
Training for Today... and Tomorrow	5

System Categorization "Step by Step"

By Lon J. Berman, CISSP

In the last issue of *RMF Today and Tomorrow*, we examined the importance of System Categorization ("Step 1" of RMF) and discussed its overarching principles. In this issue, we will walk through the categorization process step by step.

Step 1: Identify Information Types

The first and perhaps most important step in the system categorization process is the determination of the "information types" that are stored and processed by the system. So what exactly is an information type? The formal definition, per FIPS 199, is "A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation." In practice, each system owner or organization needs to determine the types of information stored and processed on their own system(s).

NIST Special Publication (SP) 800-60 is a key resource to aid system owners in identifying information types. SP 800-60 is entitled "Guide for Mapping Types of Information and Information Systems to Security Categories". Volume 1 is concerned mostly with the categorization process itself, while Volume 2 ("Appendices") is essentially a "catalog" of information types commonly stored or processed by government information systems, along with suggested categorizations for each type.

System owners should carefully review SP 800-60 Volume 2 and identify the relevant information types. A complete "description" is given for each information type to aid in identifying the ones most relevant to any particular information system. In most cases, only a handful of the numerous information types described in Volume 2 will be applicable. If there is information stored or processed by the system that does not readily "fit" into any of these predefined information types, system owners are free to "invent" their own information type(s) as needed.

Steps 2 and 3 then need to be completed for each identified information type.

Step 2: Provisional Categorization

SP 800-60 Vol 2 provides "provisional" categorization for each information type. The provisional categorization is essentially a recommendation for categorization of the particular information type in the absence of any "special factors" (see below).

SP 800-60 Vol 2 provides the provisional categorization for each information type in the following format:

"Security Category = {(confidentiality, X), (integrity, X), (availability, X)}"
In each case, "X" can be either High, Moderate or Low.

This is followed by a narrative description that provides justification for each of the three elements of the provisional categorization, i.e., confidentiality, integrity and availability.

If the system owner has identified information categories that are not listed in SP 800-60 Vol 2, it is his/her responsibility to come up with provisional categorization levels for confidentiality, integrity and availability, as well as providing justification for each.

See *System Categorization*, Page 2

Risk Management Framework Today
... And Tomorrow

What is STIG Viewer (and why are there two answers)?

By Kathryn M. Farrish, CISSP

Security Technical Implementation Guides (STIGs) are published periodically by the Defense Information Systems Agency (DISA). STIGs contain very detailed lists of security settings for commonly used IT system components, such as operating systems, database management systems, web servers, network devices, etc.

Compliance with applicable STIGs is one of the key requirements of the RMF Assessment and Authorization (A&A) process. Applying and reviewing multiple STIGs across numerous information system components can present a daunting administrative challenge. A number of tools have been developed to assist system owners and their support staff.

DISA itself publishes a tool called the STIG Viewer. This is an application that runs on a Windows workstation. STIGs, published by DISA in XML format, can be uploaded into this tool and used to create checklists into which assessment results can be entered and managed. Additional features allow for searching of individual STIGs (or multiple STIGs) for particular subject areas or keywords.

Completely separate, but similarly named, is www.stigviewer.com. This is a web-based service provided by a company called Unified Compliance. It provides access to *Unclassified* STIG content, along with various searching and reporting functions. It is regularly updated as DISA releases new STIG content.

***System Categorization*, from Page 1**

Step 3: Adjust for Special Factors

SP 800-60 Vol 2 describes various "special factors" that may affect the provisional categorization. The system owner needs to review these, determine if any are applicable, and adjust the categorization for that information type accordingly.

Once Step 2 and Step 3 have been completed for each identified information type, it is time to proceed to Step 4.

Step 4: Categorize the Information System as a Whole

To determine the "final" categorization of the information system as a whole, the system owner simply chooses among all the information types for the highest value for Confidentiality, the highest value for Integrity, and the highest value for Availability.

The overall categorization of the information system is expressed as: Confidentiality-X, Integrity-X, Availability-X (where "X" is either High, Moderate or Low) - for example "Confidentiality-Moderate, Integrity-Moderate, Availability-Low" ("M-M-L" for short).

This is the complete categorization process for DoD systems, as well as for National Security Systems (NSS) located outside DoD. For non-NSS located outside DoD, the system owner takes the additional step of choosing the highest value among the categorization levels for confidentiality, integrity and availability, resulting in a single system-wide categorization level of High, Moderate or Low.

Step 5: Document Results

The system owner should carefully document each of the categorization steps, with appropriate justification, and be prepared to brief the Authorizing Official (AO) if requested.

"The system owner … should be prepared to brief the Authorizing Official (AO) if requested ..."

Top Ten—STIGs

By Annette Leonard

The Defense Information Systems Agency (DISA) is responsible for developing security guidance for configuring DoD information systems. An extensive collection of Security Technical Implementation Guides (STIGs) is published at http://iase.disa.mil/stigs/Pages/index.aspx. STIGs contain detailed configuration guidance (settings) for commonly-used software products and other system components. Most of these documents are updated on a regular basis.

CCI-000363 (part of security control CM-6) states "The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed." The assessment procedure for this CCI goes on to state "DoD has defined the security configuration checklists as DoD security configuration or implementation guidance, e.g., STIGs, SRGs…"

Our "Top Ten" list in this issue highlights the STIGs (or families of STIGs) that DoD information system owners are most likely to encounter.

10. Application Security and Development STIG. This STIG is a little different than most because it concerns the software development *process* rather than configuration of a particular system component. Any system where there is software development activity going on will need to comply.

9. Remote Desktop STIGs. This family of STIGs covers remote desktop technologies such as Citrix, which will be applicable to any system utilizing such technologies.

8. Network STIGs. This is an extensive family of STIGs that cover everything from specific network devices, such as routers and firewalls, to network design features such as infrastructure and DMZ. Systems encompassing networks, such as data centers, will need to pay attention to STIGs in this family.

7. Office Automation STIGs. Many systems (not just workstations) include office automation products such as Microsoft Office (Word, Excel, etc.). There are available STIGs for numerous versions of these products.

6. Host Based Security System (HBSS) STIGs. DoD policy requires HBSS on all information systems. These STIGs provide configuration specifications for numerous HBSS modules.

5. Antivirus STIGs. All systems are required to incorporate antivirus technologies and there are STIGs available to cover the most popular commercial products, such as Symantec and McAfee.

4. Web Browser STIGs. Systems that include web browsers will need to pay attention to this family of STIGs that covers products such as Internet Explorer, Mozilla Firefox and Netscape.

3. Web Server and Application Server STIGs. Modern information systems rely on at least some web technology. This family includes STIGs for popular web servers such as Apache and Microsoft Internet Information Server (IIS), as well as application servers such as Tomcat and JBoss.

2. Database STIGs. Most systems rely on database technology. The STIGs in this family cover the most popular commercial database management systems (DBMS), including Oracle and Microsoft SQL Server. A more general Database Security Requirements Guide (SRG) is available to cover other DBMS.

1. Operating System STIGs. Nearly every system owner will need to be concerned about the STIGs that pertain to the specific operating systems in use within the system boundary. STIGs in this family include Windows (numerous versions for both servers and workstations), UNIX/LINUX (numerous versions), Mainframe, Mac, and Virtualization (VMWARE).

Security Control Spotlight—A Little Good News?

By Kathryn M. Farrish, CISSP

Imagine this dialog between Edward, a System Owner, and Christine, his Information System Security Manager (ISSM):

Edward (System Owner): "Now that we've completed our System Categorization, have you built the Security Control Baseline for our system?"

Christine (ISSM): "Yes, sir, I have. Our system has been categorized as "Moderate-Moderate-Moderate (M-M-M)". There are about 400 Security Controls in our baseline, and these break down into a little over 1,600 CCIs (Control Correlation Identifiers, roughly equivalent to assessment objectives)."

Edward: "So we need implementation statements and documentation artifacts supporting 1,600 items?"

Christine: "I'm afraid so. But I do have good news. I just saved 15% on my car insurance……."

Oh, wait, wrong dialog. What she really said was:

Christine: "I'm afraid so. But I do have good news. About 25% of those have been declared 'automatically compliant' by DoD!"

"Automatically compliant?" What exactly does that mean? Simply put, it means that *every* DoD system is compliant by virtue of an existing policy or procedure at the DoD level. Let's look at a couple of examples:

CCI-000101 (part of security control AT-1) states: "The organization disseminates a security awareness and training policy to organization-defined personnel or roles." The DoD-provided assessment procedure for this CCI states: "DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01." In other words, the existence of the DoD-level policy gives every DoD system an automatic "pass" on this CCI.

CCI-000348 (part of control enhancement CM-5(2)) states: "The organization defines a frequency to conduct reviews of information system changes." The DoD-provided assessment procedure for this CCI states: "The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems." In other words, the existence of DoD-mandated minimum review frequencies gives every DoD system an automatic "pass".

In most cases, only one or two of the CCIs associated with a particular control will be automatically compliant. The system owner will still be responsible for implementation and documentation artifacts to address the remainder of the control.

Even after subtracting the automatically compliant items, there is still a frighteningly large number of items that must be addressed by the system owner. Still, we'll take any "freebies" we can get!

Just for fun, here are the statistics on automatic compliance for a few of the possible system categorizations:

Moderate-Moderate-Moderate system:
- 403 controls/enhancements
- 1,631 CCIs total
- 426 automatically compliant CCIs (26%)

Moderate-Moderate-Low system:
- 381 controls/enhancements
- 1,584 CCIs total
- 419 automatically compliant CCIs (26%)

Low-Low-Low system:
- 310 controls/enhancements
- 1,376 CCIs total
- 388 automatically compliant CCIs (28%)

"...the existence of the DoD-level policy gives every DoD system an automatic pass..."

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 three 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)** – recommended for all; prior knowledge of RMF recommended. This is a three-day "In Depth" program.

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

RMF for DoD IT (Fundamentals and In Depth)

- **7-10 DEC 2015 (Colorado Springs / Online Personal Classroom™)**
- **25-28 JAN 2016 (National Capital Region / Online Personal Classroom™)**
- **15-19 FEB 2016 (Virginia Beach)**
- **22-25 FEB 2016 (Huntsville / Online Personal Classroom™)**
- **21-24 MAR 2016 (Colorado Springs / Online Personal Classroom™)**

RMF for Federal Agencies (Fundamentals and In Depth)

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

Information Security Continuous Monitoring

- **16-18 FEB 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**.

On-line 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.