Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

July, 2015
Volume 5, Issue 2

In this issue:

System Categorization—Take the Time to Get it Right!	1
Common Controls and Inheritance	2
Top Ten—Data Breaches that Made the News	3
Security Control Spotlight—Privacy Overlay	4
Training for Today… and Tomorrow	5

System Categorization-Take the Time to Get it Right

By Lon J. Berman, CISSP

The story is told of an intern who is asked by his boss to pick up some items from the supply room in the basement. The young man is not sure how to get down there, but, seeing an open door, assumes it is the stairway and steps through. Unfortunately the door turns out to be an elevator shaft and he crashes to the floor below. Luckily he seems unhurt, and just dusts himself off and proceeds to find the supplies for his boss. Before leaving, he asks the supply clerk if there is “another way” to get back upstairs. Puzzled, the clerk asks him if there’s something wrong with the way he came down. “It’s OK, I suppose”, he says, “but if you plan to use it, you’d better watch out for that first step – it’s a real doozie!”

The young intern goes about his day’s work feeling none the worse for his “adventure”. Next morning, though, he is in pain and barely able to get himself out of bed.

At some level, RMF is a little like that! The first step, System Categorization, can be a “real doozie” … and the pain may not come until later.

Allow me to explain. The intent of System Categorization is to ensure an appropriate level of security is provided to an information system (and the information it stores or processes), based on the potential adverse effect of a loss of confidentiality, integrity or availability. System Categorization is one of the principal factors that drives the selection of security controls to be applied to the system – the higher the categorization, the more stringent the set of controls. If our system is categorized too low, we will apply a set of security controls that is not strong enough to provide adequate protection. The pain may come later down the road in the form of a preventable security breach. On the other hand, if we categorize our system too high, we will end up committing resources (and money!) to implement an unnecessarily high level of security – and a different kind of pain will hit us come budget time.

DoD Information Systems (IS) are categorized as High, Moderate or Low for each of the three fundamental security objectives – Confidentiality, Integrity and Availability. A rating of Low indicates a “limited adverse effect” on organizational operations, organizational assets or individuals, Moderate indicates a “serious adverse effect” and High indicates a “severe or catastrophic adverse effect”. For example, the most critical system processing the most sensitive information (e.g., a real-time battlefield information system) might potentially be categorized as Confidentiality-High, Integrity-High and Availability-High (“High-High-High” for short), while the least critical system processing the least sensitive information (e.g., a public website) might be categorized as “Low-Low-Low”. Most DoD IS will be categorized somewhere between these extremes. If you “do the math”, you’ll see there are 27 possible categorization levels for DoD IS.

Outside of DoD, this categorization scheme applies only to systems designated as National Security Systems (NSS). In most agencies, NSS represent only a small minority of the IS in place. For all other IS, a much simpler categorization scheme is used. Non-NSS outside of DoD are categorized simply as “High”, “Moderate” or “Low”, so there are only three possible categorization levels rather than 27.

See *System Categorization*, Page 2

Common Controls and Inheritance

By Kathryn M. Farrish, CISSP

Common Controls are security controls whose implementation results in a security capability that is *inheritable* by multiple information systems (IS). For example, the information systems hosted in a data center will typically inherit numerous security controls from the hosting provider, such as:

- Physical and environmental security controls
- Network boundary defense security controls

Other inheritance scenarios include agency or departmental-level policies or procedures that can be leveraged by all IS within the organization, organization-side security monitoring capabilities, public key infrastructures (PKI), etc. Organizations implementing common controls are referred to as *Common Control Providers*.

The obvious benefit of common controls is to eliminate the need for redundant development and operation of security controls by multiple system owners. Additionally, common controls provide for uniformity that would just not be possible if each system owner "rolled their own".

> *"...Common Controls eliminate the need for redundant development and operation of security controls ..."*

In order for an IS to inherit a particular security control, the following should be true:

- The control is implemented and managed outside the system boundary of the inheriting IS
- The Common Control Provider has designated the particular control as inheritable
- The Common Control Provider has an Authorization to Operate (ATO) or equivalent evidence that the control is in fact in place

It is possible for an IS to inherit just part of a control from a Common Control Provider, with the remainder of the control provided within the system boundary. This is referred to as a *hybrid control*.

Also, it is possible for an IS to inherit a control from two or more Common Control Providers. For example, an IS whose system boundary spans multiple sites (i.e., a primary site and an alternate processing site) will most likely inherit physical and environmental security controls from the data center providers at both sites.

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

The System Categorization process for DoD IS (and NSS outside DoD) is documented in the Committee on National Security Systems Instruction (CNSSI) 1253. The System Categorization process for non-NSS outside of DoD is documented in Federal Information Processing Standard (FIPS) Publication 199.

Both of these methodologies are based on an analysis of the types of information stored or processed by the IS. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 includes a substantial "catalog' of information types commonly found within federal IS. For each information type, NIST provides "provisional" categorization levels for confidentiality, integrity and availability, along with a discussion of "special factors" that may lead a system owner to adjust the provisional levels.

In the next issue of *RMF Today … and Tomorrow*, we will examine the actual process of developing and documenting the system categorization.

Top Ten—Data Breaches that Made the News

By Annette Leonard

Many information security incidents are newsworthy, especially when they involve compromise of personal, financial and/or medical information.

Here is our “Top Ten” list of data breaches that have made the news over the past few years. While some of these compromises may have resulted from very sophisticated attack methods, others were traceable to basic lapses in good security practices—the very things the RMF security controls are intended to address.

10. Sony Online Entertainment (2013). Personal contact information and credit card information was stolen from over 100 million users of the PlayStation and Sony Online networks.

9. Adobe Systems (2013). Millions of customer records were stolen from a backup system with inadequate encryption.

8. Home Depot (2014). Point of sale systems were infected with malware posing as antivirus software; over 50 million card numbers were exposed.

7. **Ameriprise Financial (2005).** A laptop containing over 250,000 customer records was stolen; files on this laptop were not properly encrypted.

6. Tricare (2011). Several million users of the government health service had their medical information compromised due to “employee error” on the part of a contractor.

5. Anthem (2015). Tens of millions of records containing personal information were stolen from this health insurance company.

4. Edward Snowden (2014). A former government contractor illegally removed and published classified documents from the National Security Agency (NSA).

3. National Archives and Records Administration (2008). 76 million records of military veterans were inadvertently exposed when a malfunctioning hard drive was sent out for repair without being properly sanitized.

2. Target Stores (2013-2014). Over 40 million credit and debit card numbers were stolen by unauthorized access to the electronic cash register system that was apparently traced to a utility monitoring system that had an uncontrolled connection to the stores’ data networks.

1. Office of Personnel Management (OPM) (2015). Several million records on government employees, including applications for security clearances, were exfiltrated by hackers possibly tied to a foreign government. It has been reported that many of the systems in use at OPM had *known security weaknesses*, but had not been upgraded or replaced due to “lack of funds”.

Access control, physical security, media protection, encryption, system interconnection, supply chain protection, employee training … the list goes on. Each of these types of security controls (or lack thereof) somehow played a role in this list of notorious data breaches.

And they’re all part of RMF!

Security Control Spotlight—Privacy Overlay

By Lon J. Berman, CISSP

According to NIST Special Publication (SP) 800-53, an overlay is a "fully specified set of security controls, control enhancements and supplemental guidance derived from the application of tailoring guidance to security control baselines". The intent is to streamline the process of developing a security control set for specific communities of interest. The Committee on National Security Systems (CNSS) website, www.cnss.gov, is the official "repository" of overlays that are approved for use in DoD. Several overlays are published there, including ones for classified systems, space systems and intelligence systems. The one we will look at in this issue is the most recent one published, the Privacy Overlay.

The Privacy Overlay is intended for use with systems that store or process information that is subject to additional privacy protection, i.e., Personally Identifiable Information (PII) and Protected Health Information (PHI). It turns out the Privacy Overlay is actually four overlays in one. There are three separate overlays for systems processing PII, as well as an overlay for systems processing PHI. Systems containing PII will use one of the three PII overlays. In addition, the PHI overlay is used for systems that also store or process PHI.

> *"...the Privacy Overlay is actually four overlays in one."*

The choice of which PII overlay to use depends on the "PII Sensitivity Level" (aka. PII confidentiality sensitivity level), which can be Low, Moderate or High. The process of determining the PII Sensitivity Level is documented in NIST Special Publication (SP) 800-122, entitled *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

The factors that must be considered include:

- Identifiability – how easily can PII be used to identify specific individuals?
- Quantity of PII – how many individuals are identified?
- Data Field Sensitivity – are specific PII data items more sensitive than others?
- Context of Use – what is the purpose of collecting, storing, processing, disclosing or disseminating PII?
- Obligation to Protect Confidentiality – is the organization subject to laws, regulations of mandates governing the obligation to protect personal information?
- Access to and Location of PII – what is the nature of authorized access to PII?

It is important to note the PII Confidentiality Sensitivity Level is completely separate and distinct from the RMF Confidentiality categorization level.

The PII and PHI Overlays tailor the RMF baseline in two ways:

- By providing supplemental guidance and/or organization-defined values for various controls in the RMF baseline.
- By adding specific controls from the "Privacy Control Catalog" in NIST SP 800 -53, Appendix J.

Control families in the Privacy Controls Catalog include:

- Authority and Purpose (AP)
- Accountability, Audit and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DR)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

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

Regularly-scheduled classes for July-December 2015 are as follows:

RMF for DoD IT (Fundamentals and In Depth)

- ♦ **20-23 JUL 2015 (National Capital Region and Online Personal Classroor**
- ♦ **17-20 AUG 2015 (Huntsville and Online Personal Classroom™)**
- ♦ **14-17 SEP 2015 (Colorado Springs and Online Personal Classroom™)**
- ♦ **5-8 OCT 2015 (National Capital Region and Online Personal Classroor**
- ♦ **2-5 NOV 2015 (Huntsville and Online Personal Classroom™)**
- ♦ **7-10 DEC 2015 (Colorado Springs and Online Personal Classroom™)**

RMF for Federal Agencies (Fundamentals and In Depth)

- ♦ **21-14 SEP 2015 (Online Personal Classroom™)**

Information Security Continuous Monitori

- ♦ **22-24 SEP 2015 (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, and Washington, DC/National Capital Region.

Online Personal Classroom^{TM} 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 training online to a "private" group of students from *your* organization.