SELECTING RMF CONTROLS FOR NATIONAL SECURITY SYSTEMS

SAND2015-1524C

Edward L. Witzke

Sandia National Laboratories[1]
Albuquerque, NM 87185
elwitzk@sandia.gov

ABSTRACT

In 2014, the United States Department of Defense started transitioning the way it performs risk management and accreditation of information systems to a process entitled Risk Management Framework for DoD Information Technology or RMF for DoD IT. There are many more security and privacy controls (and control enhancements) from which to select in RMF, than there were in the previous Information Assurance process. This paper is an attempt to clarify the way security controls and enhancements are selected.

After a brief comparison of RMF for DoD IT with the previously used process, this paper looks at the determination of systems as National Security Systems (NSS). Once deemed to be an NSS, this paper addresses the categorization of the information system with respect to impact levels of the various security objectives and the selection of an initial baseline of controls. Next, the paper describes tailoring the controls through the use of overlays and scoping considerations. Finally, the paper discusses organization-defined values for tuning the security controls to the needs of the information system.

INTRODUCTION AND HISTORY

Information Assurance (IA) consists of the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation [7]. Accreditation is the acceptance of the residual risk by a senior official after the IA measures have been applied to a system, or stated more officially, accreditation is a formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards [7]. Since 2007, the United States Department of Defense (DoD) certifies and accredits information systems through a standardized, enterprise process for identifying, implementing, and managing IA capabilities and services [3] called the DoD Information Assurance Certification and Accreditation Process (DIACAP).

In 2014 the DoD started a transition to performing this process through the Risk Management Framework for DoD Information Technology (RMF for DoD IT) [8]. The RMF process itself is described in several referenced publications [1, 4, 8] and has been used in other parts of the United States Government. Many of the terms in RMF differ from those in DIACAP, such as an Authorizing Official (AO) rather than a DAA, security controls rather than IA controls, and even a change from calling it IA to now referring to it as Cybersecurity. A big change comes in the controls.

Under the DIACAP, there were 157 IA controls [2, 6] to be selected from, based upon the security level (classified, sensitive, public) and the mission assurance category (MAC I, II, or III). RMF for DoD IT has over 860 security, privacy, and program management controls and enhancements [9, 10]. These RMF security controls provide for a finer grain of applicability to a system than the DIACAP IA controls and are selected based upon values of low, moderate, or high for each of confidentiality, integrity, and availability. The control families are summarized in Table 1 in the Appendix to this paper.

This paper extracts material from numerous sources, so the reader does not have to pore through many pages of many documents to gain a fundamental understanding of RMF control selection. It attempts to clarify the way security, privacy, and program management controls are selected in this brave, new world of RMF for DoD IT.

[1] Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

INITIAL SELECTION OF CONTROLS AND ENHANCEMENTS

In the DIACAP there were a fixed set of (potentially overlapping) controls for each of the 3 security levels and the 3 MACs, giving 9 possible combinations of control sets. Under RMF there are potentially different controls for low, moderate, and high confidentiality, L, M, and H integrity, and L, M, and H availability. At first glance, one might think that there are 3x3x3, or 27 combinations of security controls, but that is not the way to approach control selection under RMF for DoD IT! It seems that each security control and enhancement should be examined separately. Fortunately, through the help of various tables in Appendix D of [10], this task is not as arduous one might think.

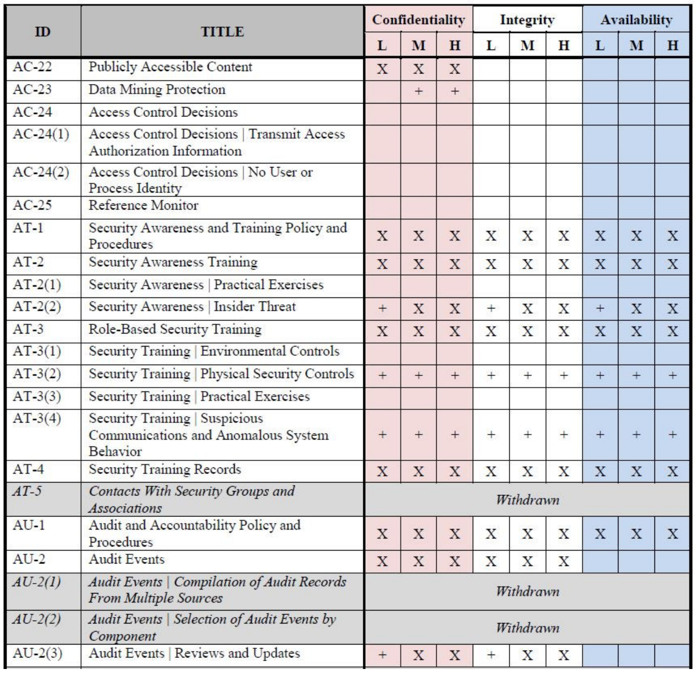
But first, we need to back up several steps. In DIACAP a system was categorized with respect to sensitivity and Mission Assurance Category. For RMF, we need to start by determining if it is a National Security System (NSS). Use sections 2 and 3, and appendix A of SP 800-59 [5] to determine if it is an NSS. A system is an NSS if it meets any of the criteria in [5]. Generally speaking, that would include intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, systems critical to the direct fulfillment of military or intelligence missions, or systems storing, processing, or communicating classified information.

Now that it has been determined that the system is an NSS, a security categorization must be performed. Although national security systems are outside the scope of NIST and FIPS publications, it is instructive to read through Table C-2 and Section 3 of Appendix D in SP 800-60, Vol. 2 [12] and Section 3 of FIPS PUB 199 [11] to gain background and perspective. Security objectives and impact levels associated with national security systems are determined by the head of each agency exercising control of the system [12, pg. 114].

That said, a good starting point for determining the low, moderate, or high levels for each of the confidentiality, integrity, and availability security objectives can be found in Section 3 of [11] and especially Table 1 of that section. There is a common thread that runs through the impact levels, for each of the security objectives. For low confidentiality, the unauthorized disclosure of information could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. For a confidentiality level of moderate, the unauthorized disclosure of information could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. System confidentiality would be assigned an impact of high, if the unauthorized disclosure of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

Similarly, unauthorized modification or destruction of information that could be expected to have a **limited**, **serious**, or **severe/catastrophic** adverse effect, will result in low, moderate, or high impacts to integrity. Likewise availability impact levels of low, moderate, or high would arise from the disruption of access to, or use of, information or an information system that could be expected to have a **limited**, **serious**, or **severe/catastrophic** adverse effect on organizational operations, organizational assets, or individuals. Hence, an impact level of low, moderate, or high would be assigned for each of confidentiality, integrity, and availability objectives, depending if the disclosure, modification or destruction, and disruption of access to or use of information, could be expected to have limited, serious, or severe/catastrophic adverse effects.

Now, it is time to select the initial set of controls and enhancements from Table D-1 of CNSSI 1253 [9] and Appendix J of SP 800-53 [10]. Select from the baseline security controls identified in Table D-1 of Appendix D corresponding to the security category of the system (i.e., the impact values determined for each security objective [confidentiality, integrity, and availability]). In each column for L, M, and H, grouped under confidentiality, integrity, and availability, there will be an 'X', a '+', or a blank space. A blank space indicates the control was either not selected (if the blank extends across all 9 columns) or is not allocated to a particular security objective for the purposes of CNSSI 1253. 'X's in the table indicate that security control or enhancement applies to the indicated impact level of the security objective per the NIST specifications in SP 800-53. A '+' in the table indicates additional Committee on National Security Systems specifications, by security objective and impact value, for all National Security Systems. Therefore, select the controls and enhancements from Table D-1 that have either an 'X' or a '+' in the appropriate impact level for confidentiality, integrity, or availability. Controls that are designated as "withdrawn" indicate that they are no longer in the NIST SP 800-53 security control catalog and are not used by CNSSI 1253. An excerpt of Table D-1 from CNSSI 1253 is shown in Figure 1. The controls and enhancements are described in Appendix F of SP 800-53.



ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-22	Publicly Accessible Content	X	X	X						
AC-23	Data Mining Protection		+	+						
AC-24	Access Control Decisions									
AC-24(1)	Access Control Decisions | Transmit Access Authorization Information									
AC-24(2)	Access Control Decisions | No User or Process Identity									
AC-25	Reference Monitor									
AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X
AT-2	Security Awareness Training	X	X	X	X	X	X	X	X	X
AT-2(1)	Security Awareness | Practical Exercises									
AT-2(2)	Security Awareness | Insider Threat	+	X	X	+	X	X	+	X	X
AT-3	Role-Based Security Training	X	X	X	X	X	X	X	X	X
AT-3(1)	Security Training | Environmental Controls									
AT-3(2)	Security Training | Physical Security Controls	+	+	+	+	+	+	+	+	+
AT-3(3)	Security Training | Practical Exercises									
AT-3(4)	Security Training | Suspicious Communications and Anomalous System Behavior	+	+	+	+	+	+	+	+	+
AT-4	Security Training Records	X	X	X	X	X	X	X	X	X
AT-5	*Contacts With Security Groups and Associations*	*Withdrawn*								
AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X
AU-2	Audit Events	X	X	X	X	X	X			
AU-2(1)	*Audit Events | Compilation of Audit Records From Multiple Sources*	*Withdrawn*								
AU-2(2)	*Audit Events | Selection of Audit Events by Component*	*Withdrawn*								
AU-2(3)	Audit Events | Reviews and Updates	+	X	X	+	X	X			

Figure 1. Portion of the NSS Security Control Baseline table.

The PM series controls listed at the end of Table D-1 are program management controls and are described in Appendix G of SP 800-53. There are no control enhancements for the PM control family.

Appendix J of SP 800-53 lists and describes privacy controls and enhancements. These privacy controls and enhancements are the administrative, technical, and physical safeguards especially applicable to protect and ensure the proper handling of personally identifiable information (PII). There is an “Implementation Tip” section in Appendix J of SP 800-53 that states:

> *View the privacy controls in Appendix J from the same perspective as the Program Management controls in Appendix G—that is, the controls are implemented for each organizational information system irrespective of the FIPS 199 categorization for that system.*

This indicates that both, the PM family of controls and the privacy controls and enhancements, should be allocated to each system (regardless of impact levels of the security objectives) and then, if necessary, any controls that do not apply can be tailored out. Organizations should analyze and apply each program management and privacy control with respect to their distinct mission/business and operational needs, and their legal obligations. Many of these controls can potentially be implemented as common controls, inherited from a higher level within the subject organization.

TAILORING THE CONTROLS

After the initial set of security controls is identified, organizations initiate the tailoring process to modify and align the controls more closely with the specific conditions within the organizations. This tailoring can include:

- Applying scoping considerations to the baseline security controls and selecting compensating or additional security controls, if needed (i.e. determining which controls may not apply or which additional or substitute controls are needed);
- Assigning specific values to organization-defined control parameters;
- Providing any necessary additional specification information for control implementation; and
- Identifying and designating common controls that may be inherited from other entities.

Organizations may use overlays to tailor the baseline controls for specific conditions that apply to many systems in their community of interest. Overlays provide tailoring guidance from a community-wide perspective to address specialized requirements, missions/business functions, technologies, or environments of operation. Overlays provide uniformity and efficiency of security control selection by presenting tailoring options developed by security and other subject matter experts, to information system owners responsible for implementing and maintaining the systems [10, Appendix I].

There is a wide range of options that can be used to construct overlays, depending upon how specific the overlay developers wish to be. Some overlays may be very specific with respect to the hardware, firmware, and software that make up the key components the information system and its environment. Other overlays may be more abstract in order to apply to a large class of information systems that may be deployed in different environments.

Overlays that provide more specific guidance are typically developed by organizations with authority over the information system owners and environments of operation. Overlays that provide less specificity can be developed by security and subject matter experts for application to large classes of information systems, especially in situations where full knowledge about the specific implementation details related to the systems are not known or can vary much from one implementation to another. Less specific overlays may require additional tailoring to customize the set of controls or parameters for the specific information system implementation, by the organization that owns and operates the system.

An advantage of overlays for certain types or classes of information systems is to explicitly and consistently define the variables, parameters, and conditions that apply commonly to those systems. Overlays are most effective when communities of interest work together to create consensus-based overlays that reflect the common interests and concerns of the community, and are not unnecessarily redundant.

Tailored baselines produced using the concept of overlays can be published independently in a variety of venues and publications including, for example, OMB policies, CNSS Instructions, NIST Special Publications, industry standards, and sector-specific guidance [10]. Some examples of these are found in Attachments 2 (Space Platform Overlay) and 3 (Cross Domain Solution Overlay) to Appendix F of CNSSI 1253. Examining the Space Platform Overlay, one can readily see which controls generally apply and which ones are usually not applicable to space platforms. The overlay contains the rationale for the selection or omission of each control it addresses. An example of this, from the Space Platform Overlay is,

AC-11, Session Lock

Control Enhancement: 1

Space Supplemental Guidance: A publically viewable pattern placed over a display (e.g., screen saver), is not necessary on space platforms as there are no human readers.

More specific tailoring may still have to be performed depending on the environment and mission of the specific system. The Committee on National Security Systems overlays are published on the CNSS website along with the CNSS Instructions.

The tailoring process, as part of control selection and specification, is part of a comprehensive organizational risk management process. Organizations use risk management guidance to facilitate risk-based decision making regarding the applicability of security and privacy controls in the control baselines. Organizations use the tailoring process to achieve cost-effective, risk-based security that supports organizational mission/business needs.

Organizations have the flexibility to perform the tailoring process at the organization level for all information systems (either as a required tailored baseline or as the starting point for system-specific tailoring activities), in support of a particular line of business or mission/business process, or at the individual information system level. Controls can be added in, to make a system more robust for a particular mission, or tailored out if not applicable to a given system. Security controls may not be applicable or appropriate if implementing those controls has the potential to degrade, debilitate, or otherwise hamper critical organizational missions and/or business functions [10]. Security and privacy controls are NOT to be removed for operational convenience. Tailoring decisions regarding controls should be defensible, based on mission/business needs, accompanied by explicit risk-based determinations and rationale, and documented appropriately.

Tailoring activities are approved by authorizing officials in coordination with selected organizational officials (e.g., the risk executive, chief information officer, senior information security officers, information system owners, common control providers) prior to implementing the security controls. The Authorizing Official will need to accept the resulting level of risk in the information system.

Finally, any organization-defined values can be allocated to the selected security controls. Security controls and enhancements containing embedded parameters (i.e., assignment and selection statements) give organizations the flexibility to define certain portions of the controls and enhancements to support specific organizational requirements and missions. After the initial selection of controls and enhancements, and adding or deleting any necessary ones, organizations should review the set of security controls and enhancements for assignment/selection statements and determine appropriate organization-defined values for the identified parameters. These parameter values may be numbers, time periods, frequencies (of occurrence), personnel, position titles, roles, etc.

Parameter values may be prescribed by applicable federal laws, Executive Orders, directives, regulations, policies, or standards [10]. Once organizations define the parameter values for security controls and control enhancements, the assignments and selections become a part of the control or enhancement for that system. Organizations may choose to specify the values for security control parameters before selecting compensating controls since the specification of the parameters completes the control definitions and may affect compensating control requirements [10]. Guidance and minimum values for affected controls in National Security Systems can be found in Appendix E and Table E-1 of CNSSI 1253.

SUMMARY

There are many documents available that delve into much greater detail about RMF controls than this paper. The author has tried to extract an overview of a procedure to select the appropriate RMF controls and enhancements from the multitude available for an NSS.

In short, for National Security Systems, 1) perform the security categorization; 2) select the initial baseline controls; 3) apply any overlays and tailor the control set; and 4) fill in organization-defined values. Obviously, for a full treatment of this topic, consult the source documents listed in the References section of this paper. The latest versions of the National Institute of Standards and Technology (NIST) Special Publications (SP 800 series), Federal Information Processing Standards Publications (FIPS PUBS), and more, can be downloaded from the Computer Security Resource Center at the NIST web site, csrc.nist.gov.

ACKNOWLEDGEMENTS

The author would like to thank Phil Campbell and Mayuri Shakamuri of Sandia National Laboratories, and Mike Feuerlein of Kratos SecureInfo for their reviews of, and comments on this paper.

REFERENCES

1. Broad, James, Risk Management Framework, Syngress/Elsevier, Waltham, MA, 2013.
2. Campbell, Phillip L., “An Analysis of Department of Defense Instruction 8500.2 ‘Information Assurance (IA) Implementation’”, SAND2012-0110, Sandia National Laboratories, Albuquerque, NM, 2012.
3. *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, DoD Instruction 8510.01, November 28, 2007.
4. *Guide for Applying the Risk Management Framework to Federal Information Systems*, SP 800-37, revision 1, National Institute of Standards and Technology, Gaithersburg, MD, February 2010.
5. *Guideline for Identifying an Information System as a National Security System*, SP 800-59, National Institute of Standards and Technology, Gaithersburg, MD, August 2003.
6. *Implementation Assurance (IA) Implementation*, DoD Instruction 8500.2, February 6, 2003.
7. *National Information Assurance (IA) Glossary*, CNSSI 4009, Committee on National Security Systems, Ft. Meade, MD, April 26, 2010.
8. *Risk Management Framework (RMF) for DoD Information Technology (IT)*, DoD Instruction 8510.01, March 12, 2014.
9. *Security Categorization and Control Selection for National Security Systems*, CNSSI 1253, Committee on National Security Systems, Ft. Meade, MD, March 27, 2014.
10. *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, revision 4, National Institute of Standards and Technology, Gaithersburg, MD, April 2013.
11. *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199, National Institute of Standards and Technology, Gaithersburg, MD, February 2004.
12. *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, SP 800-60 Volume 2, revision 1, National Institute of Standards and Technology, Gaithersburg, MD, August 2008.

APPENDIX

The following table, on the next page, summarizes the RMF control families and the control enhancements. There are 862 controls and enhancements.

Table 1. Control Family and Enhancement Summary.

Family ID	Control Family Name	Number of Controls	Number of Enhancements
Security Controls:			
AC	Access Control	23	89
AT	Awareness and Training	4	6
AU	Audit and Accountability	16	42
CA	Security Assessment and Authorization	8	14
CM	Configuration Management	11	39
CP	Contingency Planning	12	36
IA	Identification and Authentication	11	45
IR	Incident Response	10	24
MA	Maintenance	6	20
MP	Media Protection	8	14
PE	Physical and Environmental Protection	19	31
PL	Planning	6	4
PS	Personnel Security	8	7
RA	Risk Assessment	5	8
SA	System and Services Acquisition	20	66
SC	System and Communications Protection	41	75
SI	System and Information Integrity	16	66
Privacy Controls:			
AP	Authority and Purpose	2	0
AR	Accountability, Audit, and Risk Management	8	0
DI	Data Quality and Integrity	2	3
DM	Data Minimization and Retention	3	3
IP	Individual Participation and Redress	4	2
SE	Security	2	0
TR	Transparency	3	2
UL	Use Limitation	2	0
Program Management Controls:			
PM	Program Management	16	0