CHAPTER

FISMA Compliance Methodologies 3

It is common sense to take a method and try it. If it fails, admit it frankly and try another.

—Franklin Delano Roosevelt, Oglethorpe University, Atlanta, Georgia, May 22, 1932

TOPICS IN THIS CHAPTER

- The NIST Risk Management Framework (RMF)
- Defense Information Assurance C&A Process (DIACAP)
- Department of Defense (DoD) Risk Management Framework (RMF)
- DCID 6/3 and ICD 503
- The common denominator of all methodologies
- FISMA compliance for private enterprises
- Legacy methodologies

INTRODUCTION

There are five methodologies that agencies use as a basis to carry out FISMA compliance. The five methodologies are all slightly different, though the concepts among them are largely the same. Here's the list:

- NIST Risk Management Framework
- DIACAP
- DoD RMF
- DCID 6/3 ⇒ ICD 503
- FedRAMP

There are some legacy methodologies, none of which are used anymore, though you may come across them in reference materials and those are DITSCAP, NIACAP, JAFAN 6/3, and NISCAP. You'll notice that we are starting to get heavy on acronyms. Some of the acronyms used in FISMA compliance are so well known that many people don't remember what the acronyms stand for anymore. Before I dive into the differences between these methodologies, I'm listing the acronyms and complete name in Table 3.1 for reference. If you're new to FISMA, don't let acronyms scare you off—they're benign.

I won't be discussing much about the legacy methodologies, though I'll briefly touch on them near the end of this chapter for historical purposes. Some online job

Table 3.1 Acronyms for FISMA Compliance Methodologies

Acronym	Name	Era
NIST	National Institute of Standards & Technology Risk Management Framework	Up to date, in use today
DIACAP	Defense Information Assurance C&A Process	Up to date, soon to be phased out
DoD RMF	Department of Defense Risk Management Framework	Soon to replace DIACAP
DCID 6/3	Director of Central Intelligence Directive 6/3	Remnants still around
ICD 503	Intelligence Community Directive 503	Up to date, in use today
FedRAMP	Federal Risk and Authorization Management Program	Up to date, in use today
DITSCAP	Defense Information Technology	Legacy, not in use
NIACAP	National Information Assurance C&A Process	Legacy, not in use
NISCAP	NSA Information Systems C&A Process	Legacy, not in use
JAFAN 6/3	Joint Air Force Army Navy 6/3	Legacy, not in use

bulletin boards still reference the legacy methodologies, most likely because whoever wrote the job description doesn't realize that these methodologies are no longer in use. Similarly, some current government solicitations still reference these older methodologies—likely because the government contracting officer does not realize that these legacy methodologies are no longer in use. Many government RFPs are built from templates that don't often get updated. For those reasons, these legacy methodologies are worth a mention in case you're ever steered into a discussion or proposal where these terms come up.

Although all federal agencies base their FISMA compliance program on one of the current methodologies, each agency's program is at the same time unique to that particular agency. No two compliance programs are exactly alike, with the exception of FedRAMP. Chapter 23 is dedicated to FedRAMP, so I won't be discussing it much prior to that chapter.

THE NIST RISK MANAGEMENT FRAMEWORK (RMF)

The NIST Risk Management Framework (RMF) was designed for unclassified information. Unclassified information used to be referred to as Sensitive But Unclassified (SBU), however, that terminology has been replaced with Controlled Unclassified Information (CUI). The framework for the NIST RMF methodology is described in a publication known as *NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework*. A copy of it is available online at http://www.csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

The NIST standards and methodology are updated more frequently than any of the others. Additionally, the NIST high-level methodology document, SP 800-37 includes a vast amount of supporting documents that complement the foundational guidelines. Prior to updating their guidelines, NIST goes to a lot of trouble to solicit review and comments from both public and private industries, which greatly enhance the quality of their publications. They receive thousands of comments and painstakingly comb through each one of them—intellectual crowdsourcing at its best.

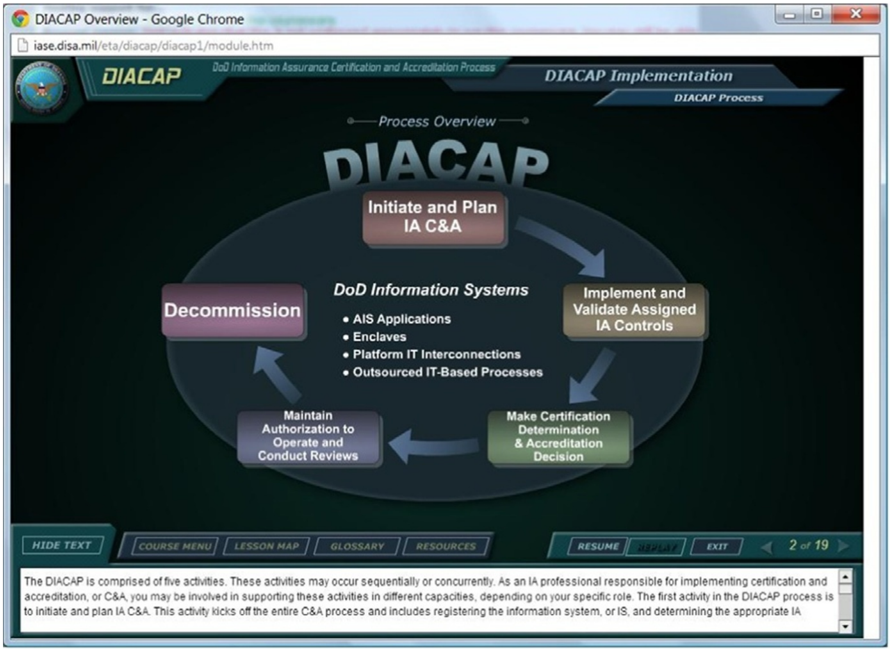
The NIST guidance is well written and easy to follow. SP 800-37, Revision 1 provides a framework—following it won't answer all your compliance questions as it leaves some room for interpretation to allow flexibility. Agencies and bureaus embracing the NIST RMF typically use NIST Special Publication 800-37, Revision 1 as a guide to develop their own internal process and handbook customized for their own unique requirements. In essence, NIST Special Publication 800-37, Revision 1 is a call to action and provides to agencies a "to do" list for information security program plans, information security control selection and implementation, policies, procedures, training, and security business processes that need to be put into place.

The NIST RMF process takes you through all the different steps of the security life cycle and this is discussed at a more in-depth level in Chapter 4. The different deliverables that are discussed in this book are consistent with the deliverables noted in the NIST RMF. I'll be talking more about the NIST RMF in Chapter 4.

DEFENSE INFORMATION ASSURANCE C&A PROCESS (DIACAP)

The Defense Information Assurance C&A Process (DIACAP) is the primary compliance methodology in place at U.S. Department of Defense agencies. DIACAP has been used by the Department of Defense since November 28, 2007. The overarching reference architecture for the DIACAP can be found in a document known as DoD Instruction 8510.01. That document can be found at the following URL: http://www.js.pentagon.mil/whs/directives/corres/pdf/851001p.pdf. DoD Instruction 8510.01 is comparable to the NIST SP 800-37, Revision 1—it provides the framework for the DoD C&A program. The baseline security controls that DIACAP uses can be found in DoDI 8500.2—an interesting read, even if you don't work for the Department of Defense. DoDI 8500.2 makes reference to various other security standards such as the Common Criteria Evaluation and Validation Scheme (CCEVS), NIST Federal Information Processing Standards (FIPS), and NIST FIPS 140-2. You can find 8500.2 at the following URL: http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf. The DIACAP life cycle is illustrated in Figure 3.1.

A unique element of DIACAP is that it focuses on the Global Information Grid (GIG). The GIG is a complex interconnection of systems, networks, and communication devices that operate with multilevel security using components that have well-defined mission assurance categories. Consisting of satellite systems, terrestrial systems, voice systems, and data systems, the GIG is an extremely complex and


DIACAP Overview - Google Chrome
iase.disa.mil/eta/diacap/diacap1/module.htm
DIACAP
DoD Information Assurance Certification and Accreditation Process
DIACAP Implementation
DIACAP Process
Process Overview
DIACAP
Initiate and Plan IA C&A
Implement and Validate Assigned IA Controls
Make Certification Determination & Accreditation Decision
Maintain Authorization to Operate and Conduct Reviews
Decommission
DoD Information Systems
• AIS Applications
• Enclaves
• Platform IT Interconnections
• Outsourced IT-Based Processes
HIDE TEXT
COURSE MENU
LESSON MAP
GLOSSARY
RESOURCES
RESUME
REPLAY
EXIT
2 of 19

The DIACAP is comprised of five activities. These activities may occur sequentially or concurrently. As an IA professional responsible for implementing certification and accreditation, or C&A, you may be involved in supporting these activities in different capacities, depending on your specific role. The first activity in the DIACAP process is to initiate and plan IA C&A. This activity kicks off the entire C&A process and includes registering the information system, or IS, and determining the appropriate IA

FIGURE 3.1

Free DoD DIACAP training course.

Table 3.2 GIG Networks

Acronym	Name	Security Classification
NIPRNet	Non-Classified Internet Router Network	Nonclassified
SIPRNet	Secret Internet Router Network	Secret
NSANet	National Security Agency Network	Top secret/SCI
JWICS	Joint Worldwide Intelligence Communications System	Top secret

evolving network of communication systems. The GIG is made up of four different networks that are integrated together in various capacities. The four networks are known as NIPRNet, SIPRNet, NSANet, and JWICS. The four GIG network acronyms and the network security classifications are listed in Table 3.2.

SIPRNet's primary purpose is to transmit military orders. JWICS primary purpose is to transmit intelligence information to the military. NIPRNet is used primarily for nonclassified combat support, and there is an air gap between NIPRNet and SIPRNet. NSANet is used by the National Security Agency/Central Security Service for signals intelligence, communications monitoring, cryptology, and research.

The Department of Defense offers a free online DIACAP training course that will help you better understand the DIACAP principles. You can access the course here: http://iase.disa.mil/eta/diacap/index.htm.

DEPARTMENT OF DEFENSE (DoD) RISK MANAGEMENT FRAMEWORK (RMF)

In the near future, the Department of Defense will be phasing out the DIACAP and replacing it with a new methodology known as the Department of Defense (DoD) Risk Management Framework (RMF). The DoD RMF is closely aligned with the NIST RMF and makes use of NIST security control baseline controls with additional controls added from *Security Categorization and Control Selection for National Security Systems* (CNSSI) 1253, published March 15, 2012. CNSSI 1253 is available at the following URL: http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf. CNSSI 1253 prescribes minimum standards that national security systems must use, based on the definition of National Security System (NSS) as described in FISMA section 3542 as

> *. . . any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—"(i) the function, operation, or use of which—"(I) involves intelligence activities;"(II) involves cryptologic activities related to national security; "(III) involves command and control of military forces; "(IV) involves equipment that is an integral part of a weapon or weapons system; or "(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions. . . .*

CNSSI was developed by the Joint Task Force Transformation Initiative Working Group and the Committee on National Security Systems (CNSS) working with representatives from the civil, defense, and intelligence communities. National Security Systems are systems that contain National Security Information (NSI). Classified NSI includes information determined to be either "Top Secret," "Secret," or "Confidential" under Executive order 12958,[1] which was released by the White House office of the Press Secretary in April 1995.

National security systems are those systems related to intelligence activities, equipment that is an integral part of a weapons system, command and control of military forces, cryptologic activities related to national security, or equipment that is critical to the direct fulfillment of military of intelligence missions. NIST clarified the definition of National Security Systems in August 2003 when it released, NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*. More information on the DIACAP to DoD RMF transition can be found on the URL for the Joint Task Transformation Initiative

[1] http://www.fas.org/sgp/clinton/eo12958.html.

Working Group here http://www.csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_dcussatt_dod-rmf-transition-brief.pdf.

ICD 503 AND DCID 6/3

Intelligence agencies that come under the purview of the Office of the Director of National Intelligence use ICD 503 and DCID 6/3 for FISMA compliance. DCID 6/3 is the older of the two, and the goal is to phase it out. Old systems are still following DCID 6/3 until they are up for reaccreditation. ICD 503 was signed and went into effect on September 15, 2008.

DCID stands for Director of Central Intelligence Directive and 6/3 refers to the process described in Section 6, part 3 of the compendious Director of Central Intelligence Directives.[2] The DCID 6/3 requires that systems be characterized by Protection Levels (PL), and DCID 6/3 defines five different protection levels. DCID 6/3 deals only with classified information, and its PL model was designed to ensure that only properly cleared people had access to classified information. The DCID Standards Manual defines the DCID 6/3 certification and accreditation process. DCID 6/3 makes use of the DCID 6/3 Policy Manual.

ICD 503 is more closely related to the NIST RMF than DCID 6/3. It refers to CNSS and NIST guidance and minimizes the amount of IC-specific guidance. An illustration of how ICD 503 incorporates CNSS and NIST documents is depicted in Figure 3.2. ICD 503 addresses policies for:

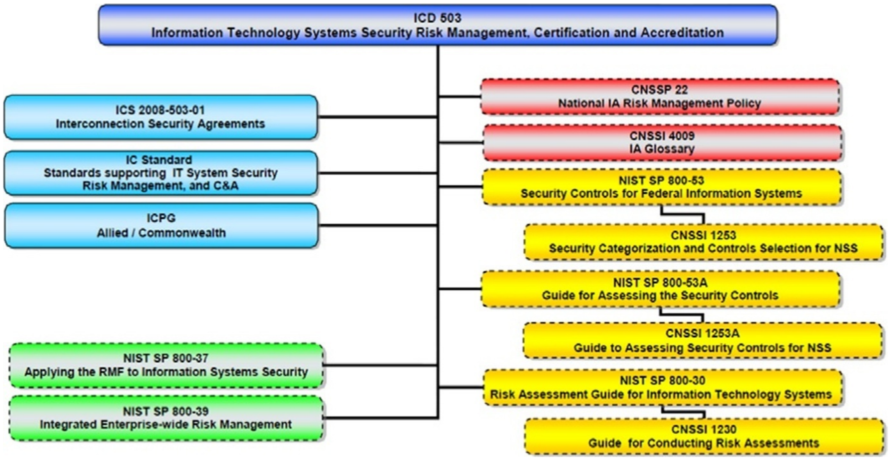

ICD 503
Information Technology Systems Security Risk Management, Certification and Accreditation
ICS 2008-503-01
Interconnection Security Agreements
IC Standard
Standards supporting IT System Security Risk Management, and C&A
ICPG
Allied / Commonwealth
NIST SP 800-37
Applying the RMF to Information Systems Security
NIST SP 800-39
Integrated Enterprise-wide Risk Management
CNSSP 22
National IA Risk Management Policy
CNSSI 4009
IA Glossary
NIST SP 800-53
Security Controls for Federal Information Systems
CNSSI 1253
Security Categorization and Controls Selection for NSS
NIST SP 800-53A
Guide for Assessing the Security Controls
CNSSI 1253A
Guide to Assessing Security Controls for NSS
NIST SP 800-30
Risk Assessment Guide for Information Technology Systems
CNSSI 1230
Guide for Conducting Risk Assessments

FIGURE 3.2

ICD 503 incorporation of other standards.

Source: National Industrial Security Program Policy Advisory Committee (NISPPAC).

[2] http://www.fas.org/irp/offdocs/dcid.htm.

- Risk Management
- Accreditation
- Certification
- Reciprocity
- Interconnections
- Governance and Dispute Resolution

A key element of ICD 503 is that ICD 503 established joint Department of Defense and Director of National Intelligence (DNI) reciprocity objectives.

Many of the requirements for IC certification and accreditation are based on physical security, as classified information must always be physically secured. Aside from physical security, the IC puts a lot of emphasis on encryption. The emphasis in these two areas is what really sets the DCID 6/3 and ICD 503 apart other methodologies.

THE COMMON DENOMINATOR OF FISMA COMPLIANCE METHODOLOGIES

The common denominator of all the FISMA compliance methodologies, and this book, is that they are all based on three attributes: Confidentiality, Integrity, and Availability of information and information systems. All the methodologies include definitions for categorizing Confidentiality, Integrity, and Availability qualitatively. In all of the methodologies, information technology assets and controls must be categorized qualitatively by sensitivity related to Confidentiality, Integrity, and Availability.

Confidentiality of information is assurance that the information will not be disclosed to unauthorized persons or systems. Integrity of information is assurance that the information will not be altered from its original and intended form. Availability ensures that the information will be available as planned. Though Availability might seem so obvious at first that it is not worth mentioning, the reason it is important is because it forces the information owner to make provisions for contingencies and outages. Because Availability is important, FISMA compliance requires that contingency plans are developed and tested.

All the compliance methodologies call for accountability. Security accountability of IT systems means that activities can be traced back to a person or a process and that system users will be held accountable for their actions. One of the reasons that roles and responsibilities are clearly defined in every Security Package is to make it clear who is responsible for what. The different compliance methodologies described in this chapter are very similar in numerous ways. If you read all the guidance documentation for each, you might come to the conclusion that the different methodologies are essentially the same thing written from different perspectives.

For the most part, the recommendations in this book will apply to all methodologies unless I point it out otherwise. The guidance I will refer to most often will be the NIST RMF since it is more up to date than the guidance for the other methodologies. NIST guidance is also publicly available for anyone to review, and in that sense, it is the most open source of the compliance methodologies. It is not my intent to republish any of the methodologies.

Something to remember is that every agency, bureau, and department in the government that has built a robust and thorough security assessment and authorization process has their own unique requirements built into it.

FISMA COMPLIANCE FOR PRIVATE ENTERPRISES

The security assessment and authorization methodologies discussed in this book are well entrenched in U.S. federal agencies. However, there is nothing that says that these methodologies and practices cannot be adopted and used by private businesses, publicly traded corporations, and nonprofit organizations. As discussed in Chapter 2, in order to obtain new contracts under government task orders, government contractors must now sign agreements that stipulate that they are in compliance with FISMA. However, any organization can make use of these methodologies, whether they have government contracts or not.

As a result of Executive Order 13636,[3] a group of experts is working on transforming much of NIST's guidance used for information security management of critical infrastructure which is primarily owned by the private sector. The group is known as the Integrated Task Force (ITF), and it is facilitated by the Department of Homeland Security. The ITF is composed of eight working groups with eight different focus areas:

Stakeholder Engagement
Cyber-Dependent Critical Infrastructure
Planning and Evaluation
Situational Awareness and Information Exchange
Incentives
Framework Collaboration with NIST
Assessments: Privacy, Civil Rights, and Civil Liberties
Research and development

Any organization that processes sensitive information should have a methodology for assessing and authorizing the security of their systems whether they are subject to regulatory laws or not. One of the goals of Executive Order 13636 is to create incentives for private sector companies to be more proactive about cyber security.

[3] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

LEGACY METHODOLOGIES

In your travails, you may come across references to various government legacy security assessment and authorization methodologies. These methodologies are no longer used. I've included information about them below for your reference in the event that you come across references to them.

NIACAP (National Information Assurance Certification and Accreditation Process)

Formerly, National Security Systems used the NIACAP which was based on *National Security Telecommunications and Information System Security Instructions*,[4] otherwise known as *NSTISSI No. 1000*. The NIACAP C&A model was developed by the CNSS, and its intent was to be used as guidance for the C&A of national security systems. NIACAP guidelines were described in a document known as *NSTISSI No. 1000*, which is still available at http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

DITSCAP (Defense Information Technology Certification and Accreditation Process)

DITSCAP was developed and published by the Defense Information Systems Agency (DISA), and it was applied to the acquisition, operation, and on-going support of any Department of Defense system that collects, stores, transmits, or processes unclassified or classified information. At one time, it was mandatory for use by all defense agencies. The DITSCAP guidance was described in a document known as DoDI 5200.40 and is still available for review at http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/i520040p.pdf.

DISTCAP used an infrastructure-centric approach and stressed that DoD systems were network-centric and interconnected. All the directives were named with numbers and begin with the numbers 5200. One of the most important DoD directives with which DITSCAP required was DoDD 5200.28. The subject of 5200.28 is *Security Requirements for Automated Information Systems (AIS)*. 5200.28 is still available at http://www.csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/i520040p.pdf. 5200.28 is a 32-page document that named numerous other directives that must be followed. 5200.18 was released in 1988 and is no longer in effect today. The DITSCAP model in particular emphasized accountability perhaps more so than the other methodologies.

JAFAN 6/3

JAFAN 6/3 was published on October 15, 2004 as a methodology to use for Department of Defense Special Access Programs (SAP). JAFAN 6/3 used a notion of protection levels and defined requirements for five protection levels using many of the processes and definitions found in traditional C&A techniques.

[4] http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

SUMMARY

FISMA compliance processes formally evaluate the security of an information system, determine the risk of operating the information system, and lead to a decision to either accept or not accept that risk.

There are various different methodologies in use today for performing FISMA compliance: NIST RMF, DIACAP, DCID 6/3, ICD 503, and FedRAMP. These different methodologies were developed for different audiences within the federal community: civilian federal departments and agencies with unclassified information, national security and defense agency information systems, information systems operated by the intelligence community, and cloud computing system. Despite the different nuances in these methodologies, they all have the goal of accomplishing the task of assessing and authorizing information systems from a cyber security standpoint.

The NIST model is very current, and NIST solicits and receives feedback from a much larger community of experts. Of all four methodologies, the NIST model is more "open source" than the others—if you can call a methodology open source.

The important thing is to make sure that whatever terminology is being used is well defined, understood by all, and consistent throughout all the other agency documents. Keep in mind that the goal of creating a FISMA compliance process is to create a well-defined repeatable process.

Notes

[1] National Information Assurance Certification and Accreditation Process (NIACAP). NSTISSI No. 1000. National Security Telecommunications and Information Systems Security Committee, http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf; April 2000.

[2] Ron Ross. Joint task force, guide for applying the risk management framework to federal information systems. NIST special publication 800-37, Revision 1. National Institute of Standards and Technology, http://www.csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf; February 2010.

[3] National Industrial Security Program Policy Advisory Committee (NISPPAC), meeting minutes. In: 34th meeting at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC; October 8, 2009.

[4] Executive Order 13636. The white house office of the press secretary, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; February 12, 2013.

[5] Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) application manual. DoD 8510.1-M. United States Department of Defense, http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf; July 31, 2000.