WHITEPAPER

FISMA VS. FEDRAMP®:

CONTROLS AND AUTHORIZATION DIFFERENCES

OMAR MALIK | CISA, FITSP
ABEL SUSSMAN | CISSP

ANDREW WILLIAMS
NICK SON | CISSP, CISA, CISM, CPA, CIA

COALFIRE℠

North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

INTRODUCTION

As a leading FedRAMP third-party assessment organization (3PAO) and FISMA Advisory, Coalfire Systems receives many questions on the difference between the Federal Information Security Management Act of 2002 (FISMA) and the Federal Risk and Authorization Program (FedRAMP) from federal agencies and cloud service providers (CSP's). The federal government is the largest single producer and consumer of information in the United States, so any changes that may affect federal agencies have the potential to significantly affect the private sector as well. To answer these questions, it is important to know the differences in the controls tested and the authorization processes for both FISMA and FedRAMP.

FISMA VS. FEDRAMP: SAME STANDARDS, ADDITIONAL CONTROLS

FISMA is a law enacted in 2002, which mandates a process to strengthen the security posture of government's information systems. When most agencies (and their vendors) discuss being "FISMA compliant," they are usually referring to meeting the controls identified in NIST 800-53, "Recommended Security Controls for Federal Information Systems." This is because the law is enforced through various processes (as described by the Office of Management and Budget Circular [OMB] A-130), which establish definitions, processes, and requirements for federal agencies to follow. FISMA (through A-130) recommends guidance issued by NIST, such as FIPS 199, FIPS 200 for impact-level categorization (low, moderate, or high-impact systems), and NIST 800-53A Revision 4 Recommended Security Controls for Federal Information Systems and Organizations (NIST 800-53 Rev 4) for the selection and implementation of security controls based on the system impact level. The control selection, implementation, and testing are where the rubber meets the road for many IT professionals responsible for "FISMA compliance," especially when meeting compliance is essential to receiving an authority to operate (ATO) by government agencies.

FedRAMP is a result of the "Cloud First" policy (PDF) issued in Feb. 2011, and OMB memo Security Authorization of Information Systems in Cloud Computing (PDF) requiring the use of FedRAMP authorized cloud services by agencies in an effort to reduce costs on underutilized IT infrastructure and to streamline the IT procurement process. This policy requires that government agencies move IT services to FedRAMP authorized cloud solutions. FedRAMP has been developed as a program for CSPs to receive an independent security assessment, conducted by a 3PAO, which is then evaluated by the FedRAMP Joint Authorization Board (JAB) for approval. The FedRAMP JAB is made up of CIOs from Department of Defense (DoD), Department of Homeland Security (DHS), and the General Services Administration (GSA). The successful result of the assessment should be a provisional authority to operate (P-ATO) that may be considered by government agencies that are adopting the "Cloud First" policy. Any commercial provider that provides cloud services to the government must have a FedRAMP P-ATO. FedRAMP is FISMA for the cloud as it inherits the NIST baseline of controls but is tailored for the cloud. Like FISMA, FedRAMP assessments follow guidance established in NIST 800-53a. In addition, the GSA has developed and published additional security control requirements for implementation and testing as part of the FedRAMP program. These additional controls and security test cases for a FedRAMP security assessment can be found on the FedRAMP.gov resources web page. Instances of cloud infrastructure in use by the government must be compliant with FedRAMP as of June 2014.

IMPACT SYSTEM LEVEL	FISMA ASSESSMENT BASED ON NIST 800-53-REV 4	FEDRAMP ASSESSMENT
Low	124	125
Moderate	261	326
High	343	N/A*

*FedRAMP authorizations are for low and moderate impact level systems.

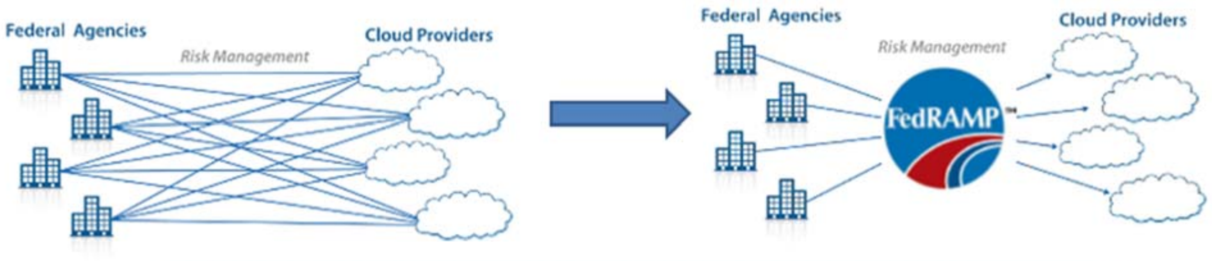
NIST CONTROL FAMILIES FOR FISMA AND FEDRAMP

Of the security control families in NIST 800-53 Rev 3 and Rev 4, 17 closely align with the minimum security requirements for federal information and information systems in FIPS-199 and FIPS-200. We have compiled a summary table of these 17 control families as they compare to FedRAMP. One key difference between the required controls for FISMA and FedRAMP is that FedRAMP has defined required parameters linked to specific controls for a CSP to implement.

		NIST 800-53 REV 3			NIST 800-53 REV 4			FEDRAMP	
		Low	Mod	High	Low	Mod	High	Low	Mod
Mapping of controls and control enhancements by system impact level to NIST 800-53 Rev. 3, Rev. 4, and FedRAMP	Access Control (AC)	11	35	39	11	35	43	11	43
	Awareness and Training (AT)	4	4	4	4	5	5	4	5
	Audit and Accountability (AU)	10	16	22	10	18	28	10	19
	Security Assessment & Authorization (CA)	6	7	8	7	10	12	8	15
	Configuration Management (CM)	6	17	30	8	21	31	8	27
	Contingency Planning (CP)	6	22	34	6	22	35	6	24
	Identification & Authentication (IA)	9	15	17	15	22	24	15	27
	Incident Response (IR)	7	11	15	7	12	16	7	18
	Maintenance (MA)	4	11	14	4	9	13	4	11
	Media Protection (MP)	3	9	13	4	9	12	4	10
	Physical & Environmental Protection (PE)	11	23	30	10	18	26	10	20
	Planning (PL)	4	5	5	3	6	6	3	6
	Personnel Security (PS)	8	8	8	8	8	9	8	9
	Risk Assessment	4	5	10	4	7	8	4	10
	System & Services Acquisition (SA)	8	15	19	7	14	18	7	22
	System & Communications Protection (SC)	9	29	35	10	24	30	10	32
	System & Information Integrity (SI)	5	20	25	6	21	27	6	28
	Totals	**115**	**252**	**328**	**124**	**261**	**343**	**125**	**326**

RECEIVING ATO AND P-ATO

Receiving a system authorization from a senior agency official is the goal of both FISMA and FedRAMP assessments. A FedRAMP system authorization allows agencies and vendors to contract for services. The result of a FISMA assessment is the award of an ATO from the authorizing agency to the organization – a one-to-one process. Through FedRAMP, any CSP that is awarded a P-ATO can then be leveraged by any government agency; a one-to-many process that supports the “do once, use many” framework as stated in the “Cloud First” policy. Once the P-ATO is issued, individual agencies are able to leverage this authorization for their own ATO as they enter into contract(s) for cloud services.



> *"FedRAMP establishes a standardized approach to security assessment, authorization and continuous monitoring. It will save cost, time, money and staff associated with doing this work.“*
>
> **- Steven Van Roekel, Federal Chief Information Officer**

FISMA AUTHORIZATION PROCESS

Under FISMA guidelines, individual government agency’s senior officials may authorize an information system and accept the risks to the agency based on the security control implementation. Agencies may require commercial organizations to meet requirements unique to the agency. As a result, commercial service providers tend to obtain multiple ATOs based on individual agency’s standards and requirements. As it is up to each agency’s senior official to accept the risk associated with the information system, it is understood that there is little official reciprocity among agencies for recognizing the authorization and assessment of a commercial vendor. What is required for one agency may not meet another agency’s needs. In an effort to maintain each ATO, a commercial service provider must be reassessed at least every three years. Having many ATOs from multiple agencies means the organization must have the budget and resources for the many assessments required to maintain them.

FEDRAMP PROVISIONAL AUTHORIZATION PROCESS

The FedRAMP process is intentionally more rigorous, as it is intended to be a one-stop shop for agencies to procure services from authorized CSPs that meet FedRAMP requirements.

The JAB, comprising officials from GSA, DHS, and the DoD, will grant a P- ATO to a CSP based on their ability to successfully demonstrate that their solution meets the more stringent set of baseline controls through an independent assessment performed by a 3PAO. The 3PAO must assess and document the results of the assessment and submit the results for review by the JAB. Once reviewed and accepted by the JAB, the CSP is granted the P-ATO. Once a CSP has been granted a P-ATO, then any agency may choose to procure services from that CSP. Part of the contract process includes an agreement for the CSP to meet additional agency-specific requirements and the award of an ATO. Once a P-ATO is issued, the CSP must meet the stringent requirements of the FedRAMP continuous monitoring program. These requirements are detailed in the FedRAMP Continuous Monitoring and Strategy Guide.

FISMA AND FEDRAMP: FINDINGS FROM THE FIELD

Organizations pursuing a FedRAMP authorization fall into two camps. One camp includes CSPs that are focused on pursuing and attaining a FedRAMP P-ATO. While this is a goal, it often comes with challenges. In some instances, CSPs have struggled to meet an initial step of establishing a complete and accurate system security plan (SSP). In other cases, CSPs have undergone an assessment, submitted their assessment package for JAB review, and have been rejected (in some cases, numerous times). These rejections have come as a result of failing to meet a minimum acceptable baseline or as a result of the 3PAO performing an incomplete or inadequate assessment. These costly rejections have caused the CSPs to look for additional help, sometimes hiring an independent 3PAO to advise the organization on how to improve before attempting to reengage in the FedRAMP assessment process. Often times, the level of improvement necessary to meet FedRAMP requirements can be drastic. For example, we have seen organizations start with a FISMA based SSP of less than 200 pages, revise the documentation to meet FedRAMP requirements, and finish with an SSP that range from 600 to more than 1000 pages. The FedRAMP provided templates alone exceed 300 pages, and the bulk of the documentation is built on a significant level of technical depth and detail for each security control.

The second camp is those that will pursue FedRAMP over a longer timeframe and are preparing for it by first understanding their current level of preparedness and building a plan to improve. Many organizations begin by updating their current FISMA documentation to leverage FedRAMP templates and include additional FedRAMP controls and enhancements (for their next assessment). They are taking time to educate themselves on the process and learn how FedRAMP affects their company both technically and from a business perspective. Some are also electing to conduct their FISMA assessment with an accredited 3PAO. They are pursuing this as a preparatory measure to pursue FedRAMP sometime in the future. Contact Coalfire Public Sector if you are seeking help with mapping control requirements between FISMA assessments and FedRAMP assessments for low- or moderate-impact systems.

In summary, FedRAMP and FISMA are distinct initiatives, and are closely tied by the NIST 800-53a controls. FedRAMP is a cloud-centric security directive based on FISMA's controls and baselines. Furthermore, under FedRAMP, providers undergo third-party assessments to ensure they meet all requirements before supporting federal agency customers.

FOR MORE INFORMATION

Visit Coalfire.com for more resources related to FedRAMP.

- **Learn** – Coalfire provides updated educational tools, templates, news, and support to help organizations address cloud security requirements.
- **Build** – Coalfire provides support in developing documentation, processes, and procedures to build a secure cloud.
- **Authorize** – Coalfire provides independent assessment support, helping CSPs achieve authorization quickly and maintain an ongoing authorization.

ABOUT THE AUTHORS

Abel Sussman | Director

Abel Sussman is a director and leverages his deep experience with developing cloud solutions, architecture, and strategic planning to advise cloud service providers (CSPs) in their ability to identify security risk and control gaps as well as implementing viable solutions.

Omar Malik | IT Security Senior Consultant

Omar Malik serves as an IT security senior consultant, responsible for supporting FISMA, FedRAMP, and ECSB assessment and advisory services to commercial and government organizations.

Andrew Williams | Consultant, Public Sector / Federal

Andrew Williams serves as a consultant for the public sector and federal assessments team performing advisory and assessment services for some of the largest cloud service providers pursuing FedRAMP, FISMA, and DISA ECSB authorization.

Nick Son | Managing Director

Nick Son is a managing director, leading FISMA and FedRAMP solutions for business serving U.S. federal, state, local, and commercial clients; he has more than 20 years of experience in information assurance, cybersecurity program management, and legislative compliance.

Published November 2014. Updated April 2016.

ABOUT COALFIRE

Coalfire is the global technology leader in cyber risk management and compliance services for private enterprises and government organizations. Our professionals are renowned for their technical expertise and unbiased assessments and recommendations. Coalfire's approach builds on successful, long-term relationships with clients to achieve multiple cyber risk management and compliance objectives, tied to a long-term strategy to prevent security breaches and data theft.

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

WP_FISMAvFedRAMP_050616