WHITEPAPER

FISMA VS. FEDRAMP:

CONTROLS AND AUTHORIZATION DIFFERENCES

ABEL SUSSMAN | CISSP, CCSP, PMP
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 third-party assessment organization (3PAO), 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 (CSPs). To answer this question, it is important to know the differences in federal policy, the security 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 that 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 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 SP 800-53A Revision 4 Recommended Security Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev 4) for the selection and implementation of security controls based on the system impact level. The control selection, implementation, and testing is where IT professionals responsible for "FISMA compliance" perform the majority of work 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 and to streamline the IT procurement process. This policy requires that government agencies move IT services to cloud solutions. FedRAMP has been developed as a program for CSPs to receive an independent security assessment, conducted by a 3PAO. Since these assessments are also based on NIST SP 800-53 Rev 4, FedRAMP can be thought of as "FISMA for the cloud" as it inherits the NIST baseline of controls and is tailored for cloud computing initiatives.

Both FedRAMP and FISMA categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk impact system levels (Low, Moderate, and High). The table below provides the number of controls tested for at each system impact level for both FedRAMP and FISMA. As FedRAMP contains additional security requirements for cloud computing, the number of controls is correspondingly higher.

IMPACT SYSTEM LEVEL	FISMA ASSESSMENT	FedRAMP ASSESSMENT
Low	124	125
Moderate	261	326
High	343	421

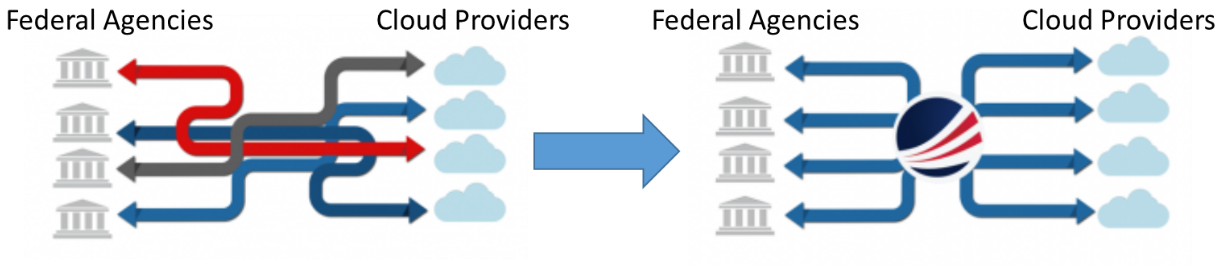
NIST CONTROL FAMILIES FOR FISMA AND FEDRAMP

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.

		FISMA			FEDRAMP		
	Control Family	Low	Mod	High	Low	Mod	High
Mapping of NIST 800-53 controls by system impact level to FISMA and FedRAMP	Access Control (AC)	11	35	43	11	43	54
	Awareness and Training (AT)	4	5	5	4	5	7
	Audit and Accountability (AU)	10	18	28	10	19	31
	Security Assessment & Authorization (CA)	7	10	12	8	15	16
	Configuration Management (CM)	8	21	31	8	27	36
	Contingency Planning (CP)	6	22	35	6	24	35
	Identification & Authentication (IA)	15	22	24	15	27	31
	Incident Response (IR)	7	12	16	7	18	26
	Maintenance (MA)	4	9	13	4	11	14
	Media Protection (MP)	4	9	12	4	10	12
	Physical & Environmental Protection (PE)	10	18	26	10	20	27
	Planning (PL)	3	6	6	3	6	6
	Personnel Security (PS)	8	8	9	8	9	10
	Risk Assessment (RA)	4	7	8	4	10	12
	System & Services Acquisition (SA)	7	14	18	7	22	26
	System & Communications Protection (SC)	10	24	30	10	32	39
	System & Information Integrity (SI)	6	21	27	6	28	39
	Totals	**124**	**261**	**343**	**125**	**326**	**421**

RECEIVING ATO AND P-ATO

Receiving a system authorization is the goal of both FISMA and FedRAMP assessments. The result of a FISMA assessment is the award of an authority to operate (ATO) from the authorizing Agency to the organization – a one-to-one process. Through FedRAMP, any CSP that is successfully assessed 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.



> *"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, 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 regularly. Having many ATOs from multiple agencies indicates that 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. Additionally, there are two paths CSPs can use for FedRAMP compliance summarized as follows:

- **Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO)**: This path entails a high level of effort and requires the security authorization package to undergo an extensive review and approval process by the FedRAMP Project Management Office (PMO) and ultimately the JAB. The JAB is comprised of officials from the General Services Administration (GSA), Department of Homeland Security (DHS), and the Department of Defense (DoD). The CSP is assigned a FedRAMP ISSO to facilitate the documentation development, review, and overall assessment process. This path proves to be the most rigorous due to the JAB's high level of scrutiny and low risk tolerance.
- **FedRAMP Agency Authority to Operate (ATO)**: For this path, the CSP must be sponsored by an Agency. The Agency is responsible for taking on the risk associated with the CSP cloud service offering. Therefore, there are varying levels of risk acceptance based on business needs and specific Agency's risk tolerance. This path also allows for some level of customization or variance in regards to the security authorization package content and overall authorization process. The level of risk tolerance is solely up to the sponsoring Agency.

FISMA AND FEDRAMP: FINDINGS FROM THE FIELD

Coalfire recommends the following actions for firms pursuing either FISMA or FedRAMP:

- Accurate System Boundary –The system boundary includes a complete inventory of assets comprised of all network components, hardware, and software/applications supporting federal operations. Boundaries should clearly state where they begin and end including when there is a relationship with another CSP entailing stacking of cloud services.
- Complete System Security Plans – The System Security Plan (SSP) is the core document describing how security controls are implemented. Too often SSPs do not have the technical depth required. Instead, the SSP should be an encompassing document that provides detailed understanding of the security operations in-place in terms of tools, technologies, and services.
- Define Gaps – Once the system has been documented, the organization will have an understanding of which controls are not being met and can plan to remediate these findings. Ideally, the gaps can be prioritized in relation to the protected assets.
- Implement Automated Processes – There are many opportunities to create integrated and automated security processes that provide system administrators accurate, timely, and actionable information. Effective areas to automate are in detection, auditing, inventory, network scanning, and configuration modification.

SUMMARY

In summary, FedRAMP and FISMA are separate initiatives that are closely tied by the NIST 800-53A controls, but there are distinct differences:

- FISMA is a law that covers all processing and storage of federal data, and each federal Agency must implement the law via NIST requirements/standards and guides.
- FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- While all federal agencies are required to have an independent assessment of their control implementation, FedRAMP is the only implementation that has accredited independent assessors via the 3PAO program.
- A FedRAMP accreditation granted by the JAB or an Agency can be leveraged by another Agency, instead of being fully assessed again.

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

Nick Son | Vice President

Nick Son leads FISMA and FedRAMP solutions and provides Cyber Risk Advisory solutions serving U.S. Federal, state, local and commercial clients. Nick has over 20 years of experience in information assurance, cybersecurity program management and legislative compliance. He is a subject matter expert in the area of FISMA, FedRAMP and Third-Party Reporting.

Abel Sussman | Public Sector Practice 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.

Andrew Williams | Senior Consultant, Public Sector

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.

Published November 2014. Updated September 2016.

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client’s specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com

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_090716