FedRAMP *Tailored*

Security Requirements for   
Low Impact-Software as a Service (LI-SaaS) Cloud Services



Version 2.0

July 11, 2017

**Revision History**

| Date | Version | Page(s) | Description | Author |
| --- | --- | --- | --- | --- |
| 1/30/2017 | 1.0 | Entire Document | Initial version for public comment | FedRAMP PMO |
| 6/19/2017 | 2.0 | Entire Document | Final version for public comment | FedRAMP PMO |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1. Purpose 1](#_Toc485217415)

[2. Authority 2](#_Toc485217416)

[3. FedRAMP *Tailored* LI-SaaS Requirements 3](#_Toc485217417)

[3.1. NIST SP 800-37 Step 1 - Categorize Information System 3](#_Toc485217418)

[3.2. NIST SP 800-37 Step 2 - Select Security Controls 4](#_Toc485217419)

[3.3. NIST SP 800-37 Step 3 - Implement Security Controls 4](#_Toc485217420)

[3.4. NIST SP 800-37 Step 4 - Assess Security Controls 5](#_Toc485217421)

[3.5. NIST SP 800-37 Step 5 - Authorize Information System 5](#_Toc485217422)

[3.6. NIST SP 800-37 Step 6 - Monitor Security Controls 6](#_Toc485217423)

[Appendices 7](#_Toc485217424)

1. Purpose

The Federal Risk and Authorization Management Program (FedRAMP) *Tailored* policy and requirements provide a more efficient path for Low Impact-Software as a Service (LI-SaaS) providers to achieve a FedRAMP Agency Authorization to Operate (ATO). Through digital services teams, Chief Technology Officers (CTOs) and Chief Information Officers (CIOs) across the U.S. Government, FedRAMP has identified many cloud services for low-risk use cases, for which a traditional enterprise-wide baseline with a “one-size-fits-all” approach does not work. While all requirements identified in the FedRAMP Low Baseline are required, FedRAMP *Tailored* identifies those requirements typically satisfied by a LI-SaaS customer or underlying service provider, allowing the provider to focus only on relevant requirements. Further, FedRAMP *Tailored* allows agencies to independently validate only the most important of these requirements.

The FedRAMP *Tailored* Baselineis consistent with the National Institute of Standards & Technology (NIST) Special Publication (SP) 800-37, the NIST Risk Management Framework (RMF). Through this approach, FedRAMP has created criteria that allow agencies to approve certain types of cloud services currently in use or planned for use in support of agency-specific unique business and/or mission needs, such as collaborative management tools. This will reduce the time, money, and effort for agencies to approve low-impact systems for use, while maintaining compliance with applicable Federal laws, policies, and mandates.

Although the FedRAMP *Tailored* Baseline provides a *minimum* set of security control requirements, each agency’s Authorizing Official (AO) still has the responsibility of determining if additional security controls are required for compliance with agency-specific policies, procedures, and risk tolerance in order to issue an informed, risk-based, formal ATO.

1. Authority

The Federal Information Security Management Act[[1]](#footnote-1) (FISMA) requires agencies to authorize information systems for use. Agencies must follow the Office of Management and Budget (OMB) guidance in Circular A-130[[2]](#footnote-2) in order to authorize services using the NIST RMF.[[3]](#footnote-3) Additionally, when a cloud system is being used, OMB requires that agencies use the FedRAMP requirements[[4]](#footnote-4) when completing the RMF.

The Joint Authorization Board (JAB), comprised of Chief Information Officers (CIOs) of Department of Homeland Security (DHS), General Services Administration (GSA) and Department of Defense (DoD); and the FedRAMP Management Office (PMO), established the minimum security requirements for cloud technology systems and the standardized policies and procedures for Government-wide adoption of FedRAMP. The FedRAMP requirements incorporate the applicable NIST SP 800-53 security controls, with tailoring of those controls to address implementations specific to cloud technology.

The FedRAMP *Tailored* Baseline is specific to U.S. Federal Departments and Agencies and provides guidance to AOs in issuing ATOs to cloud services that meet security requirements for specific business needs and use cases requiring protection of Government data with low impact for loss or confidentiality, integrity, and availability.[[5]](#footnote-5)

FedRAMP follows the guidance specified in OMB A-130 and the RMF to tailor the security implementations and NIST security controls and baselines[[6]](#footnote-6) for cloud usage. To aid in re-use by agencies, FedRAMP develops mandatory templates that agencies and CSPs must use when completing a FedRAMP *Tailored* LI-SaaS authorization.

1. FedRAMP *Tailored* LI-SaaS Requirements

FedRAMP follows the NIST RMF in order to determine the current FedRAMP security control baselines, and applies the steps specified in NIST SP 800-37 to determine a set of security controls for FedRAMP *Tailored* LI-SaaS services.

The FedRAMP *Tailored* Baseline is applicable only to cloud services that are implemented in FedRAMP-authorized cloud system with a current JAB Provisional Authorization (P-ATO) or an Agency FedRAMP ATO. If the LI-SaaS provider is providing the entire cloud stack, we may accept other certifications on a case-by-case basis, such as ISO-27001 or SOC 2, Type 2.

* 1. NIST SP 800-37 Step 1 - Categorize Information System

To date, FedRAMP has prepared baselines for extremely broad and varied cloud systems and the information that can reside in them defaulting to L-L-L, M-M-M, or H-H-H data types of information.

Federal Information Processing Standard 199[[7]](#footnote-7) (FIPS 199), however, allows for a full range of information types. In order to meet specific, unique needs of systems, agencies can specify the types of information being placed in the cloud environment. For FedRAMP *Tailored*, agencies must specify the type of information that can reside in LI-SaaS systems.

To be considered a FedRAMP *Tailored* LI-SaaS cloud service, the answer to all the following questions must be “yes:”

1. Does the service operate in a cloud environment?
2. Is the cloud service fully operational?
3. Is the cloud service a Software as a Service (SaaS), as defined by *NIST SP 800-145, The NIST Definition of Cloud Computing*?
4. The cloud service does not contain personally identifiable information (PII), except as needed to provide a login capability (username, password and email address)?[[8]](#footnote-8)
5. Is the cloud service low-security-impact, as defined by *FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems*?
6. Is the cloud service hosted within a FedRAMP-authorized infrastructure?

Such low-impact cloud services are the target for FedRAMP *Tailored*.

The only PII allowed in the system is the minimum necessary to provide login capabilities. This is limited to user name, email address, and password. The existence of any other PII disqualifies the system as a LI-SaaS. Where a system provides login capabilities, FedRAMP strongly encourages the CSP to use an agency directory covered under an existing ATO to eliminate even limited login-related PII from the LI-SaaS.

SaaS systems are allowed either where the CSP is leveraging an underlying a Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) with an existing ATO; or, where the CSP is also providing the underlying cloud infrastructure and has undergone a recognized independent audit, such as required for a Federal ATO or to obtain an ISO 27001 certificate, PCI or SOC 2, Type 2 assessment.

* 1. NIST SP 800-37 Step 2 - Select Security Controls

The L-L-L, M-M-M, or H-H-H information in SaaS systems in cloud environments has been tailored above the NIST-recommended baselines. This was intended to maximize re-use by having enterprise-wide services that would fit all definitions of information in that environment.

For low-impact SaaS services, the L-L-L baseline requires some CSPs to implement more security controls than needed based on the type of use and information agencies place in the system. FedRAMP *Tailored* will allow agencies to select a smaller set of controls, based on information types and use, allowing them to more easily obtain authorization for these types of services. This tailoring process is explicitly allowed within NIST SP 800-53 revision 4.

Appendix A contains the FedRAMP recommended tailoring actions that have been carved out as security controls for the FedRAMP *Tailored* Baseline in accordance with the tailoring criteria established by NIST and FedRAMP. There are two criteria for eliminating a security control or control enhancement from the FedRAMP *Tailored LI-SaaS* baseline:

* The control or control enhancement is uniquely Federal (i.e., primarily the responsibility of the Federal Government);
* The control or control enhancement does not directly impact the security of a cloud SaaS, as determined by FedRAMP.[[9]](#footnote-9)

In addition, the CSP is required to provide a self-attestation for those controls or control enhancements that are expected to be routinely satisfied by the CSP without further specification for implementation, and meet the intent of the security requirements. Appendix E contains the FedRAMP controls recommended for self-attestation by the CSP.

The CSP is also required to include those controls or control enhancements that are fully implemented by the infrastructure CSP and considered as FedRAMP “inherited” controls as part of the CSP self-attestation.

The criteria for tailoring of the FedRAMP *Tailored* Baseline and the results of the tailoring actions taken are documented in Appendix A, FedRAMP *Tailored* Security Controls Baseline

* 1. NIST SP 800-37 Step 3 - Implement Security Controls

CSPs must implement the controls and describe (in the FedRAMP *Tailored* templates) how the controls are employed within the information system and its environment of operation.

The FedRAMP *Tailored* Baseline also includes those controls and control enhancements that are implemented by the supporting infrastructure CSP and are indicated as “inherited” by the LI-SaaS CSP.

CSPs must also clearly delineate control implementations that the agency customer is responsible for in order to fully meet the intent of the security requirement.

* 1. NIST SP 800-37 Step 4 - Assess Security Controls

Appendix B provides mandatory templates and tailored test cases specific for FedRAMP *Tailored*. These must be used and applied to assure that the FedRAMP *Tailored* controls have been implemented correctly, operate as intended, and produce the desired outcome to meet the security requirements of the system. The CSP is required to complete the templates; however, an agency may also assist the CSP in completing the documents.

Assessment of the implemented controls may be performed by an independent trusted third-party, such as a FedRAMP Accredited Third-Party Assessment Organization (3PAO), or the agency may perform the assessment. The degree of independence required is at the discretion of the Agency AO.

* 1. NIST SP 800-37 Step 5 - Authorize Information System

An Agency AO must examine the implementation of the system and the risks associated with it in order to make a risk-based determination of its security posture. This is the basis for the Agency AO to authorize the system[[10]](#footnote-10) for use in their agency.

CSPs are required to address all the controls as specified in the FedRAMP *Tailored* Baseline, whether the control is required for implementation, conditional for implementation, inherited from the infrastructure provider, and/or required for CSP self-attestation. The residual risks and determination of level of risk posture is based on those controls where the security requirements are not fully met by the CSP. Agency AOs will issue ATOs based on their agency-specific policies and procedures for their determination of an acceptable level of residual risk.

The evidence for this authorization rests in the ATO letter from the AO to the CSP. The letter should include the following:

1. Description of any agency-control tailoring.
2. Agency to use the system.
3. Who assessed the system.
4. Identification of the residual risks that were accepted by the AO in issuing the ATO.

Appendix C contains the FedRAMP *Tailored* ATO Letter Template.

Following the current FedRAMP processes and procedures, additional agencies can reuse a FedRAMP *Tailored* LI-SaaS authorization from another agency by reviewing the authorization package, making their own risk-based decision (including determining whether additional controls are required), and issuing their own ATO. There is currently no JAB P-ATO for LI-SaaS systems.

* 1. NIST SP 800-37 Step 6 - Monitor Security Controls

Agencies must monitor the effectiveness of security controls for all authorized systems. CSPs must employ a program of continuous monitoring that includes assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system. CSPs must report on this program to Agency AOs to continue using their security authorization.

FedRAMP provides guidance on how agencies must continuously monitor authorized systems for continued use and management of risk. FedRAMP *Tailored* provides specialized monitoring procedures targeted at the FedRAMP *Tailored* Baseline set of controls. Appendix D contains the FedRAMP *Tailored* Continuous Monitoring Requirements.

Appendices

APPENDIX A—FedRAMP *Tailored* Security Controls Baseline

The external file contains the FedRAMP *Tailored* Security Controls Baseline.

APPENDIX B—FedRAMP *Tailored* Template

The external file contains the FedRAMP *Tailored* Templates.

APPENDIX C—FedRAMP *Tailored* ATO Letter Template

The external file contains the FedRAMP *Tailored* ATO Letter Template.

APPENDIX D—FedRAMP *Tailored* Continuous Monitoring Guide

The external file contains the FedRAMP *Tailored* Continuous Monitoring Requirements.

APPENDIX E—FedRAMP *Tailored* Self-Attestation Requirements

The external file contains the FedRAMP *Tailored* Self-Attestation Requirements.

APPENDIX F—Acronyms

| Acronym | Definition |
| --- | --- |
| 3PAO | Third Party Assessment Organization |
| AO | Authorizing Official |
| ATO | Authorization to Operate |
| CIO | Chief Information Officer |
| CSP | Cloud Service Provider |
| DoD | Department of Defense |
| DHS | Department of Homeland Security |
| FIPS | Federal Information Processing Standards |
| GSA | General Services Administration |
| IaaS | Infrastructure as a Service |
| LI-SaaS | Low Impact Software as a Service |
| OMB | Office of Management and Budget |
| FedRAMP | Federal Risk and Authorization Management Program |
| FISMA | Federal Information Security Management Act |
| JAB | Joint Authorization Board |
| NIST | National Institute of Standards and Technology |
| PaaS | Platform as a Service |
| P-ATO | Provisional Authorization to Operate |
| PII | Personally Identifiable Information |
| RMF | Risk Management Framework |
| SaaS | Software as a Service |
| SP | Special Publication |

1. Federal Information Security Management Act of 2002; <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf> [↑](#footnote-ref-1)
2. *MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: Management of Federal Information Resources*, July 28, 2016; <https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource> [↑](#footnote-ref-2)
3. NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010 (NIST SP 800-37); <http://csrc.nist.gov/publications-nistpubs/800-37rev1/sp800-37> rev1-final.pdf. [↑](#footnote-ref-3)
4. *MEMORANDUM FOR CHIEF INFORMATION OFFICERS: Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011; <https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf> [↑](#footnote-ref-4)
5. Refer to the *Agency Guide for FedRAMP Authorizations Handbook* for specific, step-by-step details in completing initial FedRAMP ATOs and for re-using FedRAMP ATOs issued by other Government entities. [↑](#footnote-ref-5)
6. NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations controls*, April 2013; <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> [↑](#footnote-ref-6)
7. FIPS Pub 199: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION: *Standards for Security Categorization of Federal Information and Information Syste*ms, February 2004; <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> [↑](#footnote-ref-7)
8. Agencies have the responsibility of managing users and agency data to ensure that the LI-SaaS CSP services are utilized in accordance with Federal mandates and agency policies and procedures. [↑](#footnote-ref-8)
9. FedRAMP used guiding principles from NIST SP 800-171 and the NIST Cybersecurity Framework when determining if controls could be eliminated from the baseline for LI-SaaS solutions. [↑](#footnote-ref-9)
10. All authorizations using FedRAMP *Tailored* will be at the agency level and are not appropriate for Joint Authorization Board Provisional Authorizations, due to the unique scoping and specific use for each service authorized. [↑](#footnote-ref-10)