RISCPoint

FedRAMP Revision 4 to Revision 5 Transition Guidebook

Background

On May 30, 2023, FedRAMP officially approved and released their new National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) Revision 5 baselines along with their Cloud Service Provider (CSP) Transition Plan.

For those just starting their journey with the Federal Risk and Management Program (FedRAMP), its purpose is to provide the US Federal Government with a cybersecurity assessment framework that is consistent across government agencies and systems. FedRAMP incorporated an "*assess once and use many*" philosophy when it was established in 2011; the intent was *"to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information."*

The FedRAMP control baseline is a tailored baseline using NIST 800-53 as its authoritative basis. In 2020, NIST released NIST SP 800-53, Revision 5, and everyone has been anticipating FedRAMP's update to Revision 5. FedRAMP release their updates in May of 2023, with the CSP Transition Plan, updated FedRAMP Baselines, and updated FAQ. RISCPoint is working to help organizations ensure they're prepared and able to meet the new transition requirements by explaining the new baselines, transition timelines for CSPs, and key changes and technical efforts needed for FedRAMP Rev. 5.

FedRAMP Rev. 5 Baseline Overview

The controls for Low, Moderate, and High baselines have changed. From a high-level perspective regarding controls, the most changes have occurred with the Low baseline. Here is a quick reference chart:

	High	Moderate	Low	Tailored
Rev. 4 Control Total	**421**	**325**	**125**	**126**
Rev. 4 Controls *Removed*	*-60*	*-47*	*-3*	*-3*
Rev. 5 Controls *Added*	*+49*	*+45*	*+34*	*+33*
Rev. 5 Controls Total	**410**	**323**	**156**	**156**

Table 1: Control changes for each baseline as it relates to FedRAMP Rev. 4 and Rev. 5

Of the controls removed, many were re-incorporated back into other FedRAMP Rev. 5 controls as subsets or additional parameters: 28 for High, 22 for Moderate, and 2 for Low.

FedRAMP Revision 5 Transition Summary

The FedRAMP Baseline Revision 5 Transition Guide and the FedRAMP FAQ provide guidance on the transition from FedRAMP Rev. 4 to FedRAMP Rev. 5. The transition guide categorizes CSPs into one of three phases: Planning, Initiation, and Continuous Monitoring. At a very high level, the Transition Guide can be summarized as follows:

Planning:

- As of **May 30, 2023**, if a CSP has not secured an Agency Partner (Sponsor) or contracted with a 3PAO. If the CSP has not started a FedRAMP authorization assessment, your organization most likely falls under the planning phase.
- The CSP must implement the new FedRAMP Rev. 5 baseline and use the updated FedRAMP templates to be assessed by a 3PAO.

Initiation:

- As of **May 30, 2023**, a CSP is in the Initiation phase if they are currently undergoing a FedRAMP Authorization Assessment or completed an assessment but not been authorized. In practical terms, a CSP should be listed as “In Process” or at the very least be under contract with a 3PAO with a committed Agency Partner.
- The CSP will complete their current assessment process under FedRAMP Rev. 4 and develop a plan to address any FedRAMP Rev. 5 gaps/deltas by **September 1, 2023**. Any gaps/deltas should be listed in the POA&M and FedRAMP Rev.5 gaps will be assessed at the CSP’s next assessment along with relevant documentation updates.

Continuous Monitoring:

- A CSP is in the Continuous Monitoring phase if they have an “Authorized” status on the FedRAMP Marketplace.
- As with the Initiation Phase, the CSP must develop a transition plan by **September 1, 2023**.
- Updates to transition plans based on leveraged CSP information (e.g., shared controls) are due by **October 2, 2023**.
- If the CSP’s annual assessment is scheduled between **January 2, 2023**, and **July 3, 2023**, the FedRAMP Rev. 5 gaps/deltas must be implemented with the relevant documentation updates within 1 year of their annual assessment.
- If the CSP’s annual assessment is scheduled between **July 3, 2023**, and **December 15, 2023**, then the CSP will complete all implementation and testing activities no later than their next scheduled annual assessment.

RISCPoint strongly recommends CSPs review the transition guide in its entirety to fully understand your responsibilities to meet FedRAMP Rev. 5 requirements.

Key Changes

RISCPoint estimates a significant amount of work in transitioning from FedRAMP Rev. 4 to address Rev. 5 requirements, and we're here to help. Key changes to overall requirements for Low (L), Moderate (M), and High (H) baselines are:

Supply Chain Risk Management (SR) – New Control Family

- Added to the now 18 control families for Rev. 5
- Development of process to identify and manage risks or weaknesses in the supply chain for Low, Moderate, and High baselines
- Requires policies, procedures, and plan documentation added to the System Security Plan (SSP) and related attachments
- CSPs should consider software and supply chain processes, including pre-deployment code scanning and centralized development protections

Configuration Management (CM-6) – DoD STIGs / CIS Level 2

- Requires Department of Defense Security Technical Implementation Guides (DoD STIGs), or:
    - Center for Internet Security (CIS) Level 2 for Moderate and High
    - Center for Internet Security (CIS) Level 1 or Level 2 for Low
- Significant increase from only CIS Level 1 requirements in Rev. 4
- More stringent system component settings can have an operational impact on CSP systems if not implemented appropriately
- Validation required through a Security Content Automation Protocol (SCAP) validated or compatible scanner or method.

Cryptography (SC-8, SC-13, SC-28)

- Requires data in transit and data at rest to be encrypted using FIPS-validated (FIPS 140-2 / FIPS 140-3) or NSA-approved cryptographic modules for Low, Moderate, and High baselines
- FIPS 140 validation and timelines can be found at the NIST Cryptographic Module Validation Program (CMVP)

Authentication (IA)

- Requires Multi-Factor Authentication (MFA) methods to be phishing-resistant for Low, Moderate, and High baselines
- Requires passwords for Low, Moderate, and High baselines be:
    - checked against a list of commonly used or compromised values
    - stored using an approved salted key derivation (i.e., keyed hash)
    - allow long passwords and a minimum of 14 characters for non-MFA compatible accounts (such as emergency accounts)

Red Team / Penetration Testing (CA-8)

- Penetration testing was added to the Low baseline (requiring routine testing for all impact levels now)
- Red Team exercise added to the Moderate and High baselines to simulate realistic attacks with broader focus on reconnaissance, evasion, and overall security goals

Privacy Requirement Updates

- Privacy elevated to equal footing with security across multiple control families for Low, Moderate, and High baselines including AT, CA, CM, CP, PL, and SA
- Privacy risk assessment required for systems processing Personally Identifiable Information (PII)

Technical Efforts

RISCPoint has reviewed the key changes identified in the new FedRAMP Rev. 5 baselines and estimates the key technical considerations for CSPs by Low, Moderate, and High categorization to be:

Key Technical Efforts	High	Moderate	Low
Perform TLS Inspection on Network Firewalls	X		
Review role-based policies for API access	X		
Conduct Red Team exercises	X	X	
Implement resource tagging	X	X	
Automated inventorying of sensitive data types	X	X	
Hardening session limits	X	X	X
Automate user onboarding workflow	X	X	
Build, maintain a software bill of materials (SBOM)	X	X	X
Implement centralized development supply chain protections: - package manager - repository firewall	X	X	X
Harden components and perform compliance scans against more stringent benchmarks (i.e., STIGS, CIS L2)	X	X	X
Perform vulnerability scanning on open-source components (i.e., SCA)	X	X	
Procure extended software support, where necessary	X	X	X
Establish supply chain processes for external system/service acquisitions	X	X	X
Establish supply chain processes for software packages	X	X	X

With RISCPoint's support, CSPs can accelerate their FedRAMP Rev. 5 uplift efforts. RISCPoint will leverage a CSP's complete FedRAMP Rev. 4 authorization package documentation and determine an optimal project timeline based on system categorization, status of Rev. 4 documentation, complexity of the system, etc. Support by a FedRAMP advisor should cost anywhere from $10k-$35k for Low systems, $30k-$135k for Moderate systems, and $45k-$170k for High systems. *Actual FedRAMP Rev. 5 Efforts and Costs will depend on a CSP's actual Cloud Service Offering implementation and several factors including size of the system, complexity, etc.*

What's Next?

FedRAMP Next Steps

Per FedRAMP, updated templates and documentation for the transition will be released on or around **June 30, 2023**.

CSP Next Steps

CSPs within the *Initiation* or *Continuous Monitoring* phase will need to identify the gaps between their current FedRAMP Rev. 4 implementation and the new requirements, providing updated plans to address the delta for the transition before September **1, 2023**.

Those that are in the *Planning* phase or have not started their FedRAMP journey yet will need to implement the FedRAMP Rev. 5 baseline altogether.

RISCPoint Experienced Guidance

The good news? You don't have to go through it alone – we've got your back. RISCPoint's tight-knit team of experienced professionals will seamlessly integrate with your unique solution and provide a comprehensive suite of services to guide you successfully through this challenging transition.

Reserve your spot with us today and we'll include the work identifying the Rev. 4 to Rev 5. delta in controls, and development of plans to address them (required by FedRAMP no later than September 1, 2023), for **free** as part of our support services.

Feel free to reach out and learn how we can help, we're just one call or email away.