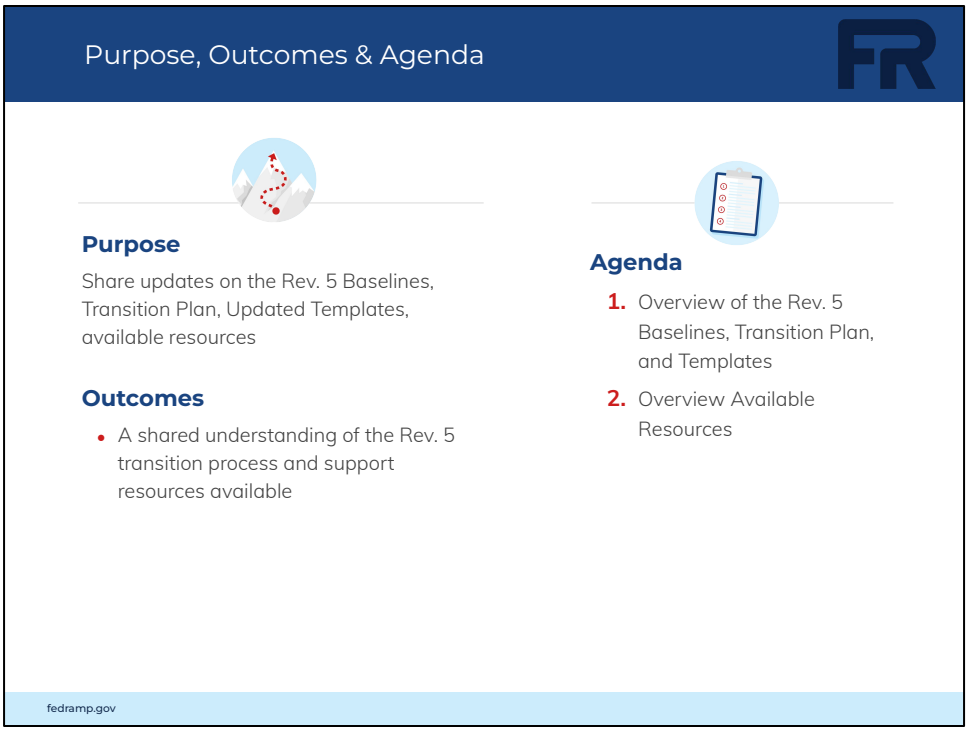
FedRAMP

Rev. 5 Transition Overview

2023

GSA

info@fedramp.gov
fedramp.gov

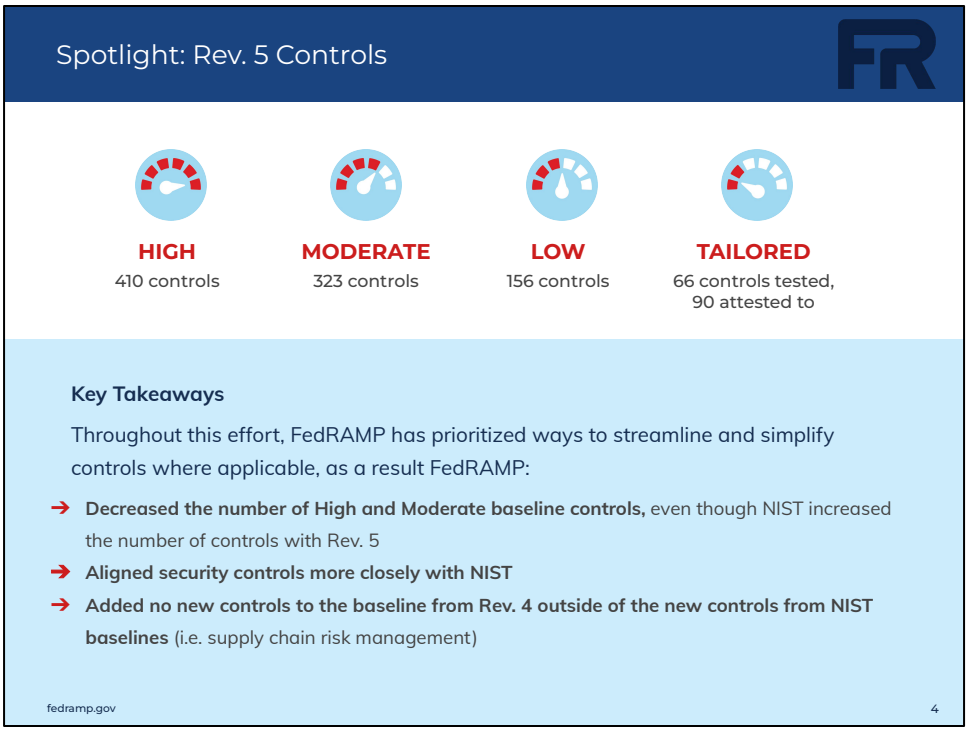


The purpose of the presentation is to share updates on the Rev. 5 baselines, updated templates, the transition plan, and available support resources.

The intended outcome is a shared understanding of the Rev. 5 transition process and support resources available

This presentation will cover several subjects that are important for our stakeholders to understand and that will help in the successful implementation and transition to the Revision 5 FedRAMP baselines

Rev. 5 Updates

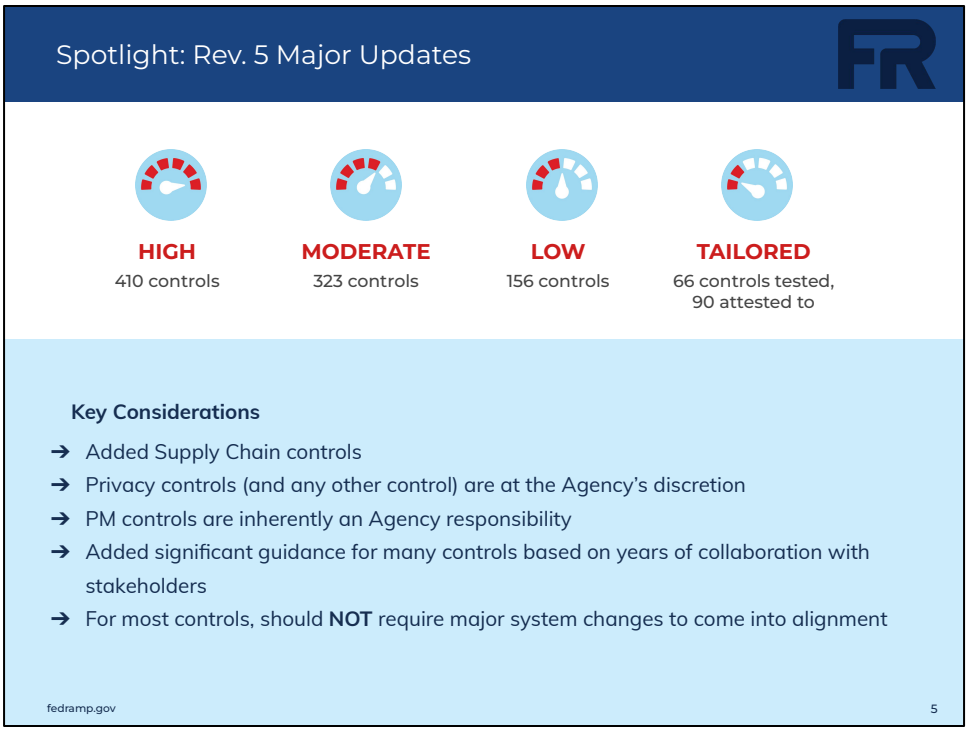


In this presentation we'll touch on the Rev.5 controls in our baselines, updated templates, the transition plan, and available support resources.

We did reduce the number of controls on the high and moderate baselines, though the low baseline did increase relatively significantly from 125 controls to 156. This was because the NIST baseline included 149 controls; we started with the NIST baseline and added 7 controls on top of that. We didn't remove any controls from the NIST baselines and didn't add any new controls compared to Rev. 4 other than new controls from the NIST baselines.

We tried to align more closely with NIST. As you'll see, NIST did incorporate some of what we had in Rev. 4 that was above the NIST baselines in Rev. 4. They ended up including those and especially in our high baselines. A lot of the controls that we had above this baseline are now included in the NIST baseline.

The biggest addition was the supply chain risk management family of controls, but beyond that there wasn't a significant change or add from from our control perspective.



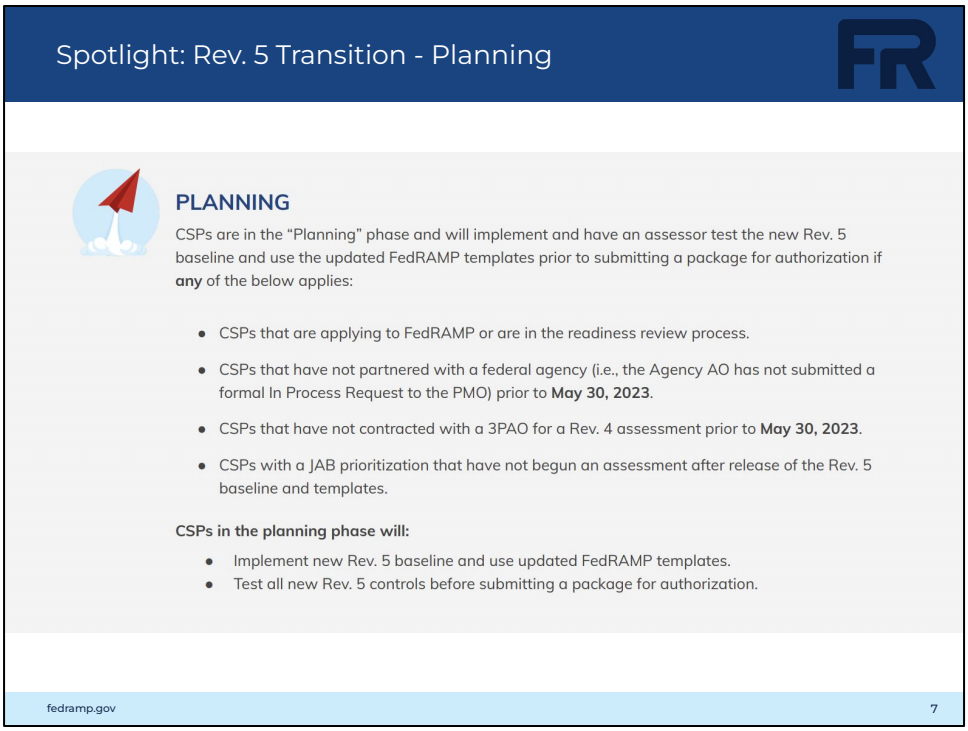
As mentioned, the biggest change was the addition of the supply chain risk management family of controls, but no other significant change or add from from our control perspective.

Like with Rev 4, we did not include any of the privacy controls. There are some privacy related controls that are part of the standard NIST baseline that we included, but we didn't include any of the additional privacy overlay controls or any of the PT control families. We've been getting a lot of questions around that, but that was purposeful. We are asking the agencies to apply those requirements based on your data types to the cloud service providers.

The guidance we've been giving cloud service providers regarding privacy controls is they should be looking at their data types. If it's a software as a service, and they know there's going to be certain privacy implications there, then they should be working with the agencies early to determine what the potential requirements are above the standard Rev. 5 baseline for FedRAMP.

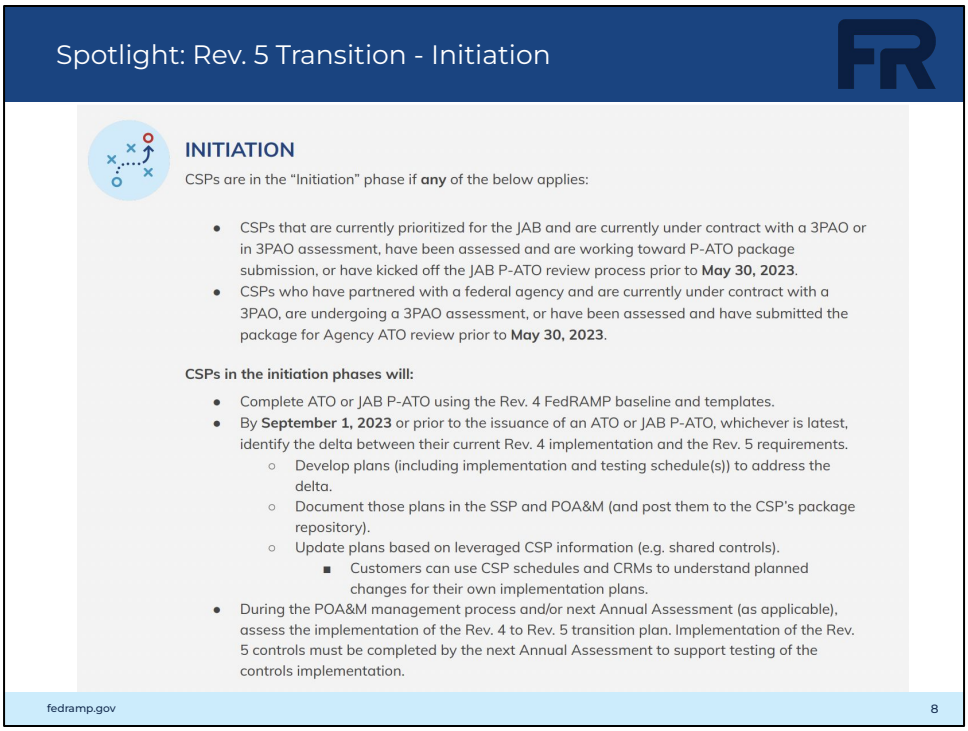
CSPs should start with our baselines. On top of that, we ask that the cloud service providers work with the agency authorizing officials to determine those requirements early as they can.

Rev. 5 Transition Plan



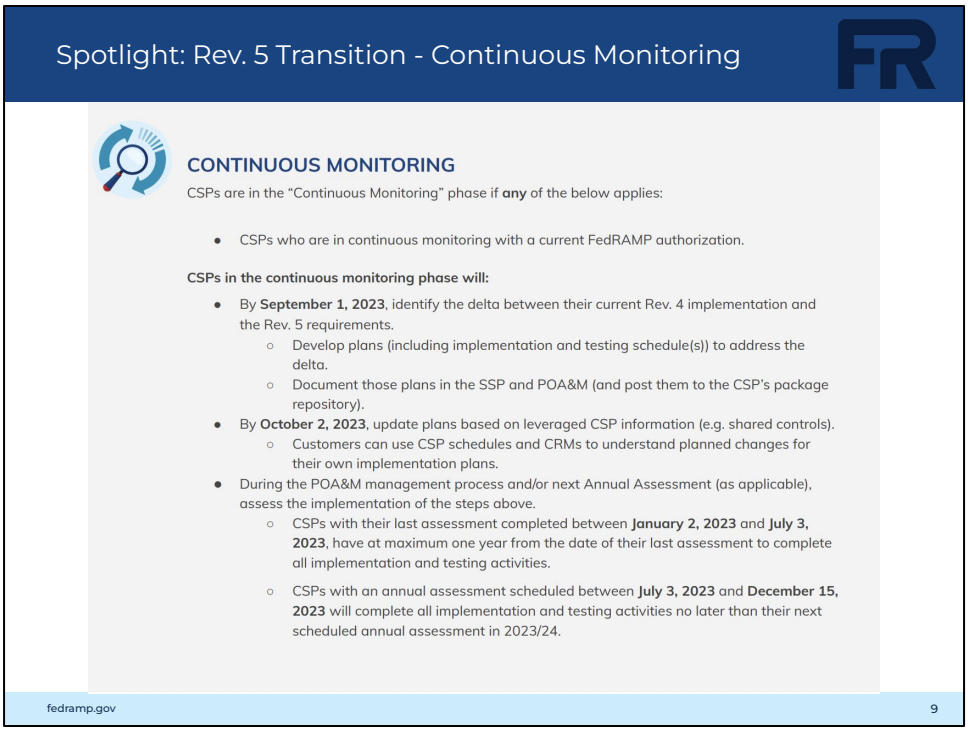
There are three phases outlined in the Rev. 5 Transition Plan: Planning, Initiation and Continuous Monitoring. The material on this slide, and the next two, comes directly out of the Rev 5 Transition Plan. Please refer to the Transition Plan for details on requirements and timing.

If a CSO is in the planning phase, meaning as of May 30, 2023, they're not far along in the path and they haven't partnered with any agencies or contracted with a 3PAO on an assessment, then they should be start with the Rev. 5 baselines.



A CSO is in the Initiation phase if, by May 30, 2023, they are working towards a FedRAMP authorization and are working with an agency (or JAB) and have at least contracted with a 3PAO to perform an assessment.

These CSOs can continue towards authorization at Rev 4, however, they need to be assessing their implementation against Rev 5, and by September 1, 2023 (or prior to ATO issuance) should have provided a transition plan, a POAM that includes controls specific implementation plans, and an estimated CIS/CRM to provide to customers to give them an understanding of likely responsibilities once Rev 5 is implemented within the offering. After authorization, at the first annual assessment, they should migrate to Rev 5.



CSOs in the Continuous Monitoring Phase must migrate to Rev 5 according to the schedule in the Rev 5 Transition Plan:

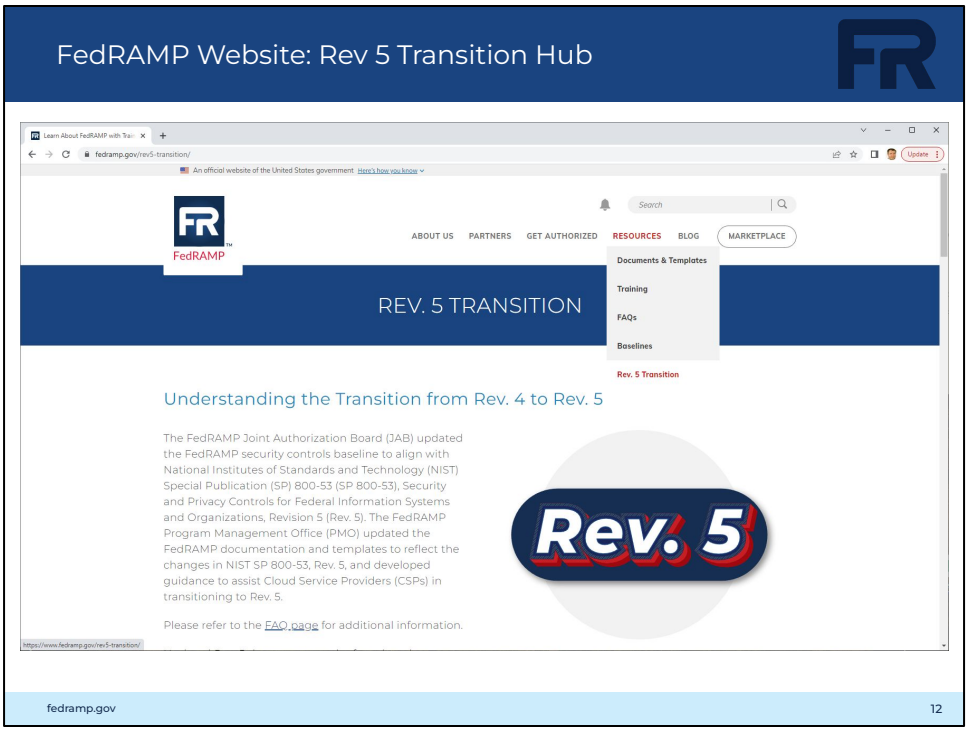
- If the previous assessment (whether an initial or annual assessment) was conducted between January 2, 2023 and July 3, 2023, the CSP will have a maximum of one year from the date of their last assessment to complete all implementation and testing activities associated with Rev 5.
- If the upcoming annual assessment is scheduled before December 15, 2023, CSPs must complete all implementation and testing activities no later than their next scheduled annual assessment after December 15, 2023. In other words, if a CSP is already planning for an upcoming annual assessment against the Rev 4 baselines, we want them to proceed with the assessment versus delaying it in order to incorporate the delta Rev 5 controls.

Like CSOs in the Initiation Phase, CSPs need to be assessing their implementation against Rev 5, and by September 1, 2023 should have provided a transition plan, a POA&M that includes controls specific implementation plans, and an estimated CIS/CRM to provide to customers to give them an understanding of likely responsibilities once Rev 5 is implemented within the offering. If they are leveraging another CSO, they have another month, until October 2, 2023 to update their plan based on the plan of the leveraged service. At their next annual assessment, they should migrate to Rev 5.

Not everything's going to fit perfectly into the three categories we have here. We

encourage cloud service providers to work with their Authorizing Official on their specific, unique scenarios. The FedRAMP PMO is happy to help CSPs and agencies to determine appropriate plans.

FedRAMP's Rev. 5 Transition Page



On the fedramp.gov webpage, there is a “Rev. 5 Transition” link under the Resources Tab. https://www.fedramp.gov/rev5-transition/
That is where all things related to the FedRAMP Rev. 5 transition reside. We will continue to keep this page updated as new templates and documents are released.

This page includes links to:

-FAQ
Rev 5 related FAQs (which can also be found under the FAQs page)

-Documents and Templates
In the Documents section, we give an overview of which documents were consolidated from Rev. 4 to Rev. 5. This is a grid mapping out what was previously released in Rev 4, and then the corresponding documents for what is now released in Rev 5.

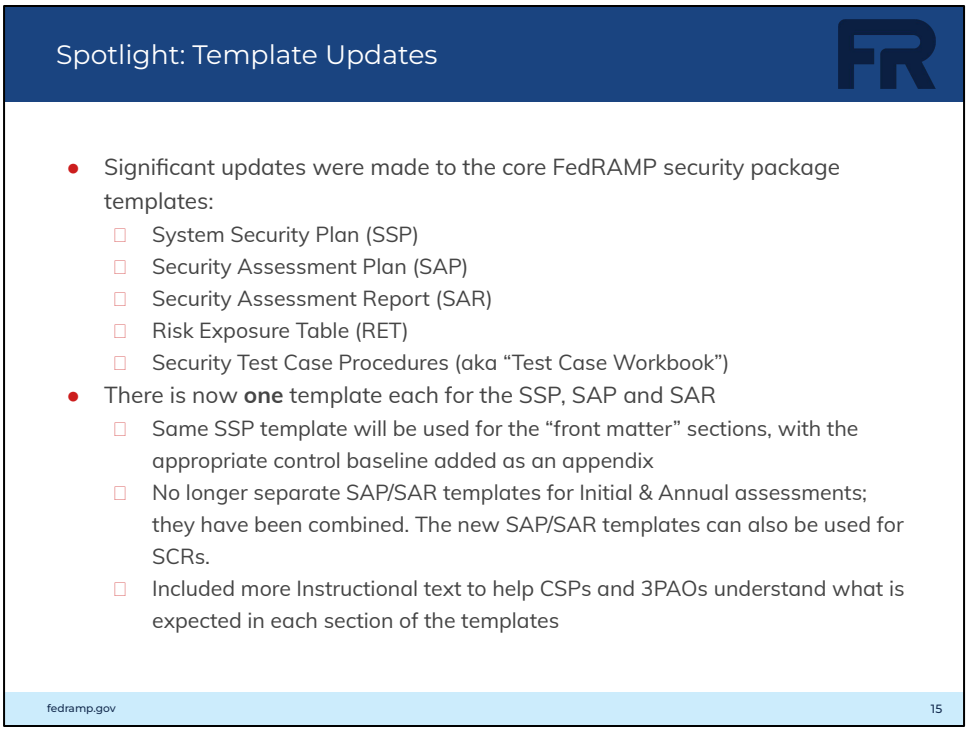
-GitHub

Also on this page is a link to our GitHub automation site. Anything that we release and produce going forward regarding Rev 5 is going to be on this page. Please be sure to take a look at this periodically, as you're working with your cloud service providers, since we continue to release information on this page.

- Transition documents

The other area that we have is our blogs, which is linked here as well. Our blog is where we will post new information. As we release blogs announcing that we're releasing new templates, the Rev 5 transition page will be kept up to date.

Rev 5 Documents that Have Been Released



Next is an overview of the changes that were made to the the core FedRAMP security package templates as part of the Rev 5 transition, specifically the SSP, SAP, SAR, RET and Test Case Workbook.

In addition to updating the templates to align with Rev 5, we looked for opportunities to consolidate and streamline the content. For example, there's now one template each for the SSP, SAP and SAR.

Regardless of whether the CSP is pursuing FedRAMP, high, moderate, low or LI-Saas, they will use the same template to complete those front matter sections of the SSP. The front matter sections include all the general system information, leveraged services, the boundary and data flow diagrams, and so on.

CSPs will use the same template for all of the front matter content, but the section that includes all of the security controls has been stripped out. The security controls sections of the template are being provided separately. The CSP will just complete and attach whichever baseline applies to their system as an appendix.

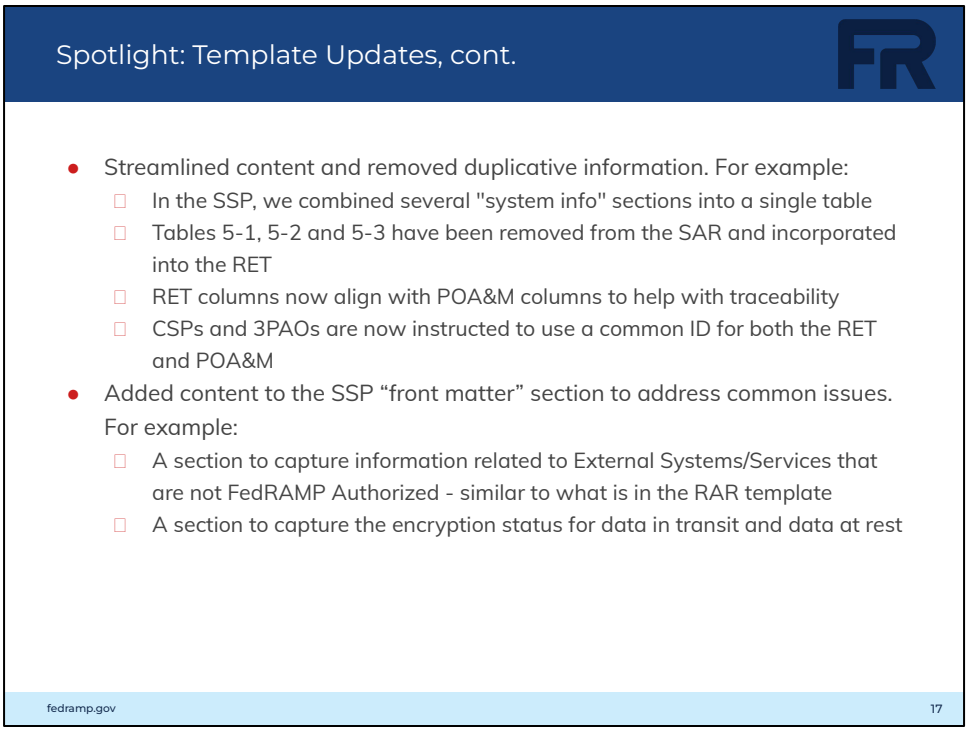
The main reason for doing it this way - that is, separating out the front matter section from all the control baselines - is simply to minimize the number of templates we have to touch when we need to make updates to those front matter sections in the future.

The same is true for the SAP and SAR. There are no longer separate SAP and SAR templates for initial and annual assessments; they've been combined. The new templates can also be used to document test plans and results for significant change requests.

We also included more, and hopefully better, instructional text to help CSPs and 3PAOs understand what's expected in each section of the templates.

If you've ever downloaded a fresh copy of the templates, you would have noticed blue italicized instructional text that explains what we expect to see in each section, then CSPs and 3PAOs are told to delete the instructions before submitting the final version of the document. We've expanded on that instructional text to address some of the common issues we continue to see in authorization packages. So for example, we've included very specific instructions for the boundary, network, and data flow diagrams and corresponding narratives because we continue to have issues in those areas.

We've also included an example of the level of detail we're expecting when describing all the services, components, tools, etc. that make up the system. If you have team members that are new to reviewing FedRAMP packages, we recommend that they download a fresh copy of the template to see that instructional text and kind of have it side by side with the package that they're reviewing. This will help them, as the reviewer, understand the level of detail that CSPs and 3PAOs should be providing.



We also looked for ways to streamline content and remove duplicative information, in hopes that it results in less reading for you and reduces room for error on the part of the CSP and 3PAO.

For example, in the previous SSP template, there was roughly eight different sections to capture just general system information. There was a whole section for service model and another section for the deployment model.
We combined all of that into a single table in hopes of making it easier on the reader.

Many of you are familiar with Tables 5-1, 5-2 and 5-3 in the SAR. Those have now been removed and incorporated into the Risk Exposure Table. The Risk Exposure Table now includes one tab for risks that were corrected during testing; what was previously documented in Table 5-1. And it includes another tab for risks that remained at the end of testing. In addition, the columns on the open risks tab now mirror the columns in the POA&M. AND we are instructing CSPs and 3PAOs to use a common ID for both the RET and POA&M deliverables. So again, all of this was done to reduce duplicative information which can always lead to errors, reduce the amount of cross-checking you have to do when reviewing these deliverables, and it was done to provide better traceability between the RET and the POA&M.

Even though we consolidated a lot of content, we also added a couple sections to the SSP front matter. This was done to address issues that we continue to see in authorization packages. We added a whole new section to capture information

related to external systems and services that are not FedRAMP authorized. It's similar to what is in the RAR template today, for those of you that might be familiar with the RAR. In this new section, CSPs are required to describe the connection details and data flows to and from the external service. This is all to help reviewers better understand the impact to the cloud offering and the federal data it holds if the C-I-A of the external system is compromised. The intent of this table is to give the reviewer better visibility into all of those external services that are being leveraged.

We also added a new appendix where CSPs are required to document details about all the encryption functions performed on the system. This includes data at rest, data in transit, authentication, digital signatures, hashes, everything. This has also been an area where we see deficiencies and gaps, so we created this table to try to consolidate all that information and easily identify where there might be gaps.

These are just a few examples of the changes we made to the templates to hopefully improve readability, and also address some of the common issues that we see with package deliverables.