Cloud Hosted Applications

As of June of 2014, all federal organizations are restricted to using Cloud Service Providers (CSP) that have been FedRAMP authorized, or that are in the process of obtaining their FedRAMP authorization to operate. Visit GSA's FedRAMP site, the FedRAMP Marketplace, for more information and to see a list of ready, in-process, and authorized CSPs.

According to NIST's Special Publication 800-145, *The NIST Definition of Cloud Computing*, Cloud based systems are typically leased infrastructure and use one or more of the following service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). System owners who use a CSP should understand the compliance requirements for such environments because they do vary some from traditional infrastructure solutions. Federal agencies that use cloud services fall under the auspices of both the Federal Risk Authorization Management Program (FedRAMP) program, which is managed by the GSA, and by NIST's 800-37 Risk Management Framework, which outlines how traditional FISMA assessments are conducted. When choosing a cloud service provider you should first ensure that the provider has a FedRAMP issued or recognized Authorization to Operate (ATO). Please visit GSA's list of authorized CSPs to find the current list of FedRAMP authorized CSPs.

FedRAMP is the FISMA based authorization process that cloud service providers must follow before government agencies may use their cloud service offering (CSO). Once a CSP has its FedRAMP authorization, Federal agencies may use them but are still subject to internal agency review and endorsement of the FedRAMP authorization. The agency authorization includes a review of the FedRAMP package, but also requires agencies to implement and assess non-fully managed controls. Agencies are asked to submit their own authorization leveraging the FedRAMP authorization acknowledging that they are approving the use of the CSO by their agency and attesting that they will separately implement, assess, and maintain the agency or customer managed controls not covered by the CSP. Agency endorsements or ATOs are posted on the FedRAMP Marketplace so that other agencies can determine who else uses the CSO and avoid duplicating effort by their agency.

At the NCI, we work closely with the NIH, with other ICs, and with the HHS security offices to ensure cloud offerings are properly vetted and approved, and that we do not duplicate work where not needed.

There are two ways CSPs can get their CSO through and approved by FedRAMP: 1) the FedRAMP Joint Authorization Board (JAB) can assess and approve; or 2) Agencies can partner with and conduct the FedRAMP process with the CSP. Both result in FedRAMP ATOs, but will be marked as either a JAB or an Agency ATO. The process is the same, but Agency sponsorship has both some pros and cons over JAB sponsorship. On the pro side, Agency sponsorship tends to be faster and allows some latitude for risk tolerance that the JAB may not be able to exercise. On the con side, Agency sponsorship means more work for the agency especially when it comes to continuous monitoring and re-authorization, and other agencies may not share the same risk tolerance and may not endorse your FedRAMP ATO.

1. Categorize the Application

Use the NCI Security Starter Kit for templates and guidance on completing the Federal Information Processing Standard (FIPS)-199 form, the e-Authentication Threshold and Risk Analysis (eTA/eRA) forms, and the Privacy Impact Assessment (PIA). All three forms are required to ensure that you select the appropriate security controls for your application based on its security-impact rating, authentication needs, and privacy concerns. This step is consistent with other types of federal information systems whether hosted internally, externally, or in the cloud.

2. Select Security Controls

Once you have completed categorizing your application you can determine which system specific and portions of shared controls are needed for your system. Since your application is hosted in a cloud environment, many of the controls are likely to be inheritable partially or fully from the CSP and should already have been assessed under the CSPs FedRAMP authorization. Any portion of a hybrid control and any system-specific controls that are not provided by the CSP will need to be separately implemented by you for your application, and evaluated during your application's assessment step (Step 4). Since you are using a cloud based solution, you must follow the appropriate FedRAMP control baseline rather than the normal FISMA/NIST baseline that would be used for non-cloud systems. This control selection matrix can be used as a starting point, but you need to review both FedRAMP guidance and work with your cloud service provider at the project initiation to ensure you identify all controls that they provide and those that you will be responsible for.

3. Implement Security Controls

As part of the implementation, you may need to update your application's design requirements to account for new or modified security requirements. You may also need to implement or develop specific tools to satisfy required controls. If the cost of developing or implementing a new security control is impractical or if it is not cost effective when compared to the potential risk of not implementing the control, you can apply for a security waiver to the NIH chief information security officer (CISO). You should discuss any waiver requests first with your Contracting Officer Representative (COR), and with the NCI ISSO (link sends email).

) before actually submitting the request, to determine if there are any compensating control options and whether the waiver is likely to be approved.

4. Conduct the Security Assessment

It is important to note that FedRAMP's Joint Advisory Board (JAB) may directly act as the authorizing official for a CSP, or a federal agency may sponsor a CSP's assessment using the FedRAMP controls, templates, and processes. In either case — whether a JAB or an agency sponsored ATO is sought – all CSP assessments must be carried out by an approved third party assessment organization (3PAO) and all documentation and artifacts must be deposited in the FedRAMP repository.

In addition to the FedRAMP assessment process that all CSPs are to follow, which focuses solely on the common (i.e., inheritable) controls from the CSP, federal application owners are also responsible for conducting an assessment of non-inherited controls in their applications to ensure the privacy and security of data and applications implemented and deployed in the cloud. Together, the FedRAMP authorization decision (of the inheritable controls) and the application specific security assessment (of the non-inheritable and hybrid controls) that are conducted form the basis of the final federal authorization package and decision.

During this phase of the Risk Management Framework, (RMF) a qualified – and usually an independent 3rd party – security assessor will evaluate the effectiveness of your application's non-inherited security controls. This process must be completed before your application goes into production (i.e., is live with real data being collected, processed, or stored). Because your system is hosted in the cloud, your organization will likely bear the full cost of assessing these residual non-inherited CSP controls. The security assessor shall be experienced in using the National Institute of Standards and Technology (NIST) RMF as outlined in NIST 800-37.

Your final SA&A package must contain the minimum set of artifacts required by NIH. Visit the NCI SA&A Package Checklist for more information.

5. Authorize the Application

In addition to the required JAB or Agency sponsored FedRAMP assessment and ATO, you are required to obtain an application specific ATO from the designated authorizing official (AO) for your application. This application specific ATO takes into account the CSP's existing provisional ATO as well as the application specific security control assessment. Your designated AO will review the assessment package in total to determine if identified residual risks are acceptable to the organization before issuing a written formal authorization to operate (ATO) your application, which is valid for up to 3 years.

blocked URL

Your AO will most likely be either your Contracting Officer Representative (COR) or your Federal Program Manager (PM), sometimes one and the same. If you have trouble determining who the AO will be for your system, email the NCI ISSO (link sends email).

for assistance in making a determination.

6. Conduct Continuous Monitoring and Reauthorization

Continuous monitoring (CM) is the sixth and final step in the RMF, and includes both automated and manual security monitoring and remediation activities. The routine security-control monitoring and remediation that occur after an application has been authorized to operate often includes a combination of automated diagnostics services such as vulnerability management, intrusion detection and prevention, system and application event log collection and analysis, and patch management. Along with these, manual assessment and remediation procedures such as annual assessments (AA), security impact reviews, plan of action and milestones (POA&M) management, and ongoing authorization (OA) or re-authorization must be performed.

Annual Assessments

The NIH SA&A policy requires application owners to assess a set of controls that is roughly 1/3 of the total applicable controls, each year after the ATO has been issued. Each year NIH issues guidance on which controls must be annually assessed. This list is available from the NCI ISSO upon request, or may be provided by your C.O.R. This approach helps owners address the most prevalent security threats on an ongoing basis while maximizing efficiency and supports the system's re-authorization decision every three years. If a system owner fails to keep up with the annual assessments, then every three years the system must be fully re-assessed. These controls need only be assessed to the extent they are not already covered under the FedRAMP inherited controls.

Security Impact Reviews

When significant changes to your application are proposed (while it is operational and has an active ATO), you must ensure that new security risks are identified, evaluated, and addressed before those changes are implemented. This may require re-testing of any new or modified controls and, possibly, reauthorization of your application. However, if you follow a defined change control process, and if you adequately identify and address potential risks that may result from a proposed significant change, re-authorization may not be required. The idea is to be transparent about such changes, adequately identify and address potential risks, and to keep a record of such assessments. Some changes may be so significant that the system must be re-authorized, such as changing the operating location of a system or a complete re-design of a system. When in doubt about when a re-authorization may be needed, please consult with your ISSO.

POA&M Management

The Plan of Action and Milestones (POA&M) is a key management tool that lists, prioritizes, and tracks an application's identified weaknesses and progress. Any new security findings that are generated from ongoing security assessment and risk impact reviews should be added to the application specific POA&M and remediated in a timely manner. You should not track the CSPs POA&M items as those will be monitored by the FedRAMP Project Management Office (PMO) or by the agency that sponsored their FedRAMP assessment.

Ongoing Authorization and Re-authorization

The NIH is currently developing its ongoing authorization (OA) model so we are not using a true ongoing authorization approach at this time. However, by demonstrating that you have conducted annual assessments, applied sound configuration and change control, scanned for and closed technical and security vulnerabilities, addressed your POA&M items in a timely manner, and patched your systems and applications in accordance with NIH standards, you will be able to seek re-authorization as required every three years and should find the process less time consuming and less expensive than starting from square one.