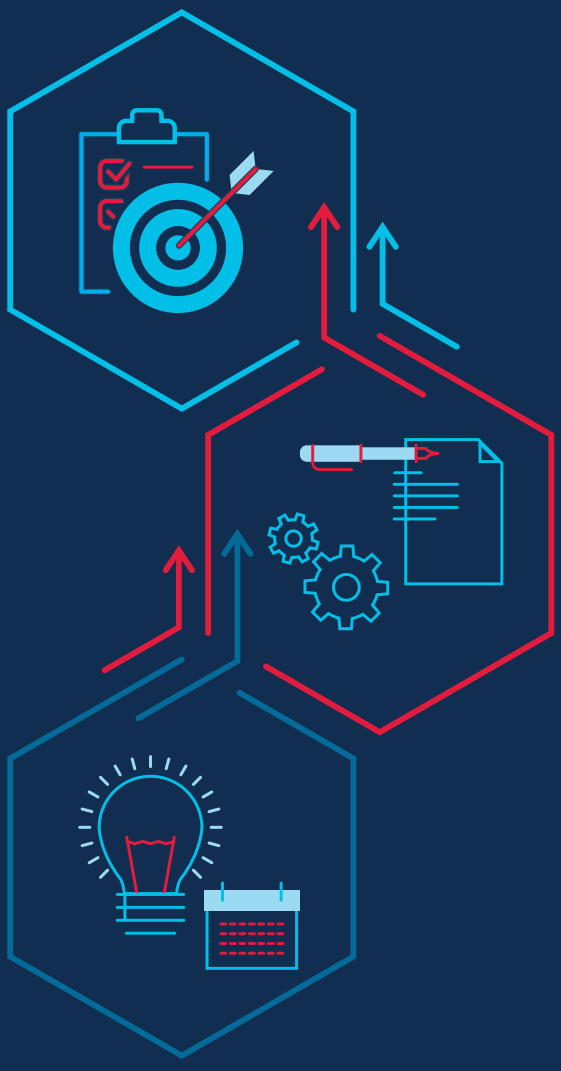
AGENCY AUTHORIZATION

BEST PRACTICES FOR AGENCIES

FedRAMP



PLANNING YOUR AUTHORIZATION

- Determine who the Agency Authorizing Official is.
- Confirm your resources. An Agency should have at least one technical reviewer (TR) (ISSO/ISSM) assigned to the authorization process.
- Develop an initial project plan. Map out authorization milestones and resources to specific dates. Provide to Cloud Service Provider (CSP) in advance to manage expectations and obtain input. The FedRAMP PMO is also available to provide feedback on your timeline.
- Prior to the kick-off, identify and provide additional Agency-specific requirements above the FedRAMP security control baseline (if applicable).

Best Practices During Planning:

- The authorization planning process should be a collaborative effort between the Agency, CSP, and 3PAO.
- Have regular and candid discussions with the FedRAMP PMO and the CSP throughout the authorization process to ensure that risk is understood.
- Engage the FedRAMP PMO (**info@fedramp.gov**) when needed to provide clarification on FedRAMP authorization process/procedures.

AT KICK-OFF

- The kick-off meeting is intended to review roles and responsibilities, key security items of note, project schedule, and future meeting cadence. A sample kick-off agenda is as follows:
- Understand roles and responsibilities of all project team members including Agency, CSP, and Third Party Assessment Organization (3PAO) personnel.
- Review project schedule and milestones and gain consensus from all parties.
- Ensure that all parties have access to FedRAMP's secure repository (OMB MAX) to obtain FedRAMP deliverables.
- Review network topology, interconnections, and system boundary diagram.
- If there are any additional Agency requirements, gaining consensus on those at this time is key, as well as any other Agency-specific security concerns.

Best Practices During Kick-Off:

- Ensure there is a clear understanding of roles and responsibilities for each stakeholder group.
- Commit to open communication and establish communication channels.

- If you need assistance with the kick-off, feel free to invite the FedRAMP PMO to help facilitate.
- At the end of the kick-off session, agree on the action plan moving forward and what the Agency reviewer will recommend to decision-makers.
- Require decision points and actions to be time bound with a date-certain outcome.

PACKAGE REVIEW

- Use FedRAMP's Agency Checklist to guide your review.
- Timely Agency feedback is critical to the overall project schedule. If the Agency reviewer has questions, discuss them with the CSP to understand the associated risk with the cloud. Maintain a regular cadence of meetings between the Agency, CSP, and 3PAO throughout the quality and risk review to address Agency questions and concerns in real time. This might include longer in-person working sessions to address specific areas of the system.
- Clearly define what will be "showstoppers" to the review process up front.
- Develop a method for tracking and updating your comments ahead of time, including how to theme similar comments and areas of focus.
- Clearly define deadlines by which each section of the authorization package should be reviewed.
- CSP and 3PAO remediation of the system based on reviewer comments can be iterative. Be strategic in your approach to remediating comments.
- Keep an open feedback loop with the CSP, 3PAO, and internal Agency stakeholder to capture lessons learned throughout the process to implement into your next Agency authorization.

POST ATO AND CONTINUOUS MONITORING:

- Note that Agencies are only issuing an ATO for their Agency's use of that cloud service. It is not a government-wide blanket risk acceptance. Other Agencies that are interested in authorizing the system will review the security deliverables and issue their own ATO through the reuse model.
- Ensure all ATOs are provided to **info@fedramp.gov**.
- The CSP will provide monthly continuous monitoring deliverables on FedRAMP's secure repository.
- It is incumbent upon each Agency to review materials and ensure they agree with any changes, deviation requests, scans, etc. and that the risk posture that they agreed to at the time of authorization remains consistent throughout the lifecycle of the system.

Best Practices Post ATO:

- Ask the CSP to conduct a monthly meeting to review continuous monitoring deliverables (a high-level report detailing transactions, scan, and POA&M) with all customers, and use this time to share any concerns or questions with the vendor.

COMMON TROUBLE AREAS THAT EXTEND TIMELINES

- **Accurate documentation** including the System Security Plan (SSP), attachments, and policies and procedures.
- **Accurate authorization** boundary that includes all system components that could come in contact with federal data.
- **E-authentication** level is appropriately selected.
- **Penetration testing** is completed in accordance with **FedRAMP guidance**