A Simplified Checklist for FedRAMP

Are you REALLY ready for FedRAMP?
Chat with a FedRAMP consultant and/or 3PAO to get a sense of the considerable cost, commitment, and ongoing operational impact of FedRAMP. Gain Management buy-in early.

Do you need support (a consulting firm) to pursue FedRAMP?
Determine if you have in-house NIST/FISMA/FedRAMP expertise that is readily available to work near exclusively on FedRAMP for 3- 6 months. If not, engage a consulting firm to do some of the heavy lifting.

What Security Categorization?
Determine whether your data mandates a Low, Moderate, or High categorization. Consider going higher for marketing reasons; but understand the cost, schedule, and complexity implications of the decision.

Agency? GSA/JAB? (eventually both?)
If you initiated the effort, it's likely a GSA ATO you're pursing, else your considering an Agency ATO. There may be cost/marketing benefits to each approach. Seek 3PAO and consulting firm guidance.

Do you need a dedicated FedRAMP environment?
If you already have a SOC2/ISO-27001 certified environment it may be beneficial to maintain a dedicated FedRAMP environment due to the relatively stringent and prescriptive controls mandated by NIST 800-53.

Engage a 3PAO
You will need a 3PAO to perform the required testing. Early engagement can be advantageous as a good 3PAO's input can be beneficial. *(occasionally the Agency is the 3PAO)*

Generate the Required Documentation
This sounds simpler than it is. Generating 800+ pages of documentation requires an extensive amount of decision making to optimize the design & operation of the controls. Remember; you need to do what you document in order to get, and remain, authorized.

Perform the Dance
FedRAMP is a choreographed exercise involving you, the3PAO and GSA/Agency with phased document preparation, submission, review, feedback, & updates. Unfortunately, it's more a waltz than jitterbug.

Entertain the 3PAO (and hopefully ace the test)
A strong relationship between you, the consulting firm and the 3PAO will allow you to shape and optimize the System Test Plan the 3PAO prepares, tests against, and submits the results of to the GSA/Agency.

Final Touch-Ups
Generate Plans of Actions & Milestones (POAM's) and update any required documentation based on testing and final feedback. Submit concluding paperwork, and raise a glass!

PivotPoint SECURITY