COMPLIANCE CHECKLIST

FedRAMP compliance checklist

Federal Risk and Authorization Management Program

Jurisdiction: Cloud service providers serving US federal agencies

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who FedRAMP applies to

Cloud service providers (CSPs) offering services to US federal agencies. FedRAMP authorization is required for any cloud product agencies acquire under FISMA.

FedRAMP checklist

STEP 1

- [ ] Determine FedRAMP impact level (Low, Moderate, High) based on the highest-impact agency data - note the FedRAMP 20x initiative is moving toward updated authorization classes.

STEP 2

- [ ] Secure an agency sponsor (Agency Authorization is now the single pathway - the JAB Provisional ATO route was discontinued by FedRAMP in August 2024).

STEP 3

- [ ] Engage an accredited Third-Party Assessment Organization (3PAO).

STEP 4

- [ ] Build the FedRAMP package: System Security Plan (SSP), policies, procedures.

STEP 5

- [ ] Run the 3PAO assessment and address findings.

STEP 6

- [ ] Submit the Security Assessment Plan (SAP), Security Assessment Report (SAR), and POA&M.

STEP 7

- [ ] PMO and authorizing official review; address review comments.

STEP 8

- [ ] Receive the agency Authority to Operate (ATO).

STEP 9

- [ ] Maintain continuous monitoring (ConMon): monthly scans, annual assessments, ongoing POA&M.

STEP 10

- [ ] Re-authorize on the standard cadence or upon significant change.

FAQ

Is there still a JAB / Provisional ATO path?

No. GSA announced the dissolution of the Joint Authorization Board in May 2024 (replaced by the FedRAMP Board), and FedRAMP discontinued the JAB Provisional ATO authorization path in August 2024. There is now a single Agency Authorization pathway - a sponsoring federal agency reviews the assessment package and grants the ATO. CSPs that previously held a JAB P-ATO retain those authorizations until they expire or transition. The program is also moving toward FedRAMP 20x, which updates the authorization model further.

What is FedRAMP Ready vs Authorized?

FedRAMP Ready is a designation a CSP earns by completing a Readiness Assessment Report (RAR) with a 3PAO; it indicates the CSP is likely ready to pursue an authorization. Authorized means a sponsoring federal agency has granted the ATO and the CSP appears in the FedRAMP Marketplace.

How much does FedRAMP cost?

Costs are highly variable: 3PAO assessment fees, internal control implementation, ongoing ConMon. Typical first-time FedRAMP Moderate authorizations are quoted at $250K-$2M total, with annual ConMon adding $100K-$500K depending on system complexity. High baseline is significantly more.

Is StateRAMP related to FedRAMP?

StateRAMP is a separate non-profit programme modelled on FedRAMP for US state and local governments. A FedRAMP authorization usually satisfies StateRAMP requirements via reciprocity, but each state retains the right to add requirements.

Source: https://ba-copilot.com/compliance/fedramp-compliance-checklist. Tick each item as it is completed and add the named owner.