COMPLIANCE CHECKLIST

NIST RMF compliance checklist

NIST Risk Management Framework (SP 800-37 Rev 2)

Jurisdiction: US federal information systems and the contractors that build them

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who NIST RMF applies to

US federal agencies and contractors that build, operate, or host federal information systems. The broader NIST CSF and SP 800-171 also apply outside government (especially for DoD contractors and critical-infrastructure operators).

NIST RMF checklist

STEP 1

- [ ] Prepare: establish the risk-management context - roles, risk tolerance, common controls, and continuous-monitoring strategy (added as Step 1 in SP 800-37 Rev 2).

STEP 2

- [ ] Identify and define the information system boundary.

STEP 3

- [ ] Categorize the system using FIPS 199 (Low / Moderate / High for confidentiality, integrity, availability).

STEP 4

- [ ] Select the baseline controls from NIST SP 800-53 Rev 5 matched to the FIPS 199 categorisation.

STEP 5

- [ ] Tailor and supplement the baseline based on system-specific risk.

STEP 6

- [ ] Implement controls and document them in the System Security Plan (SSP).

STEP 7

- [ ] Assess control implementation per NIST SP 800-53A using an independent assessor.

STEP 8

- [ ] Develop a Plan of Action and Milestones (POA&M) for any residual findings.

STEP 9

- [ ] Authorizing official reviews the authorization package and makes the ATO decision.

STEP 10

- [ ] Operate under the ATO and run continuous monitoring on the configured cadence.

STEP 11

- [ ] Re-authorize at the boundary of significant change or the end of the authorization term.

FAQ

What is the difference between the NIST RMF and the NIST CSF?

The RMF (SP 800-37 Rev 2) is a seven-step process (Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor) for managing risk to federal information systems and supports the ATO process. The Cybersecurity Framework (CSF 2.0, released February 2024) is an outcome-oriented framework with six functions - Govern (added in 2.0), Identify, Protect, Detect, Respond, Recover - used widely outside government. The RMF is a "how to authorise an information system" process; the CSF is a "how to organise cybersecurity outcomes" framework.

How does NIST SP 800-171 fit in?

SP 800-171 is the protection requirements for Controlled Unclassified Information (CUI) in non-federal systems. It's the substrate of CMMC Level 2. SP 800-53 (federal systems) and SP 800-171 (non-federal CUI custodians) cover related but distinct populations.

How long does an ATO take?

A first-time ATO typically takes 12-18 months from boundary definition through authorization. Subsequent ATOs are shorter if the baseline and SSP roll forward and continuous monitoring evidence is intact.

What is the FedRAMP relationship to NIST?

FedRAMP is the implementation of NIST SP 800-53 controls for cloud service providers serving the US federal government. A FedRAMP authorization satisfies the federal agency's responsibility under FISMA for cloud-based information systems.

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