

FedRAMP High IAL3 Readiness Checklist

When teams preparing for a FedRAMP High (Class D) assessment struggle with IAL3, the usual cause is evidence fragmented across systems, owners and formats. Use this checklist to package a defensible record for your independent assessor before the audit window opens.

What NIST IAL3 requires

“IAL3 identity proofing SHALL only be delivered as on-site attended. The proofing agent MAY be co-located with the applicant or attend the identity proofing session via a CSP-controlled kiosk or device.” SP 800-63A-4 §4.3.1

“For identity proofing at IAL3, the CSP SHALL collect: One piece of FAIR evidence and one piece of STRONG evidence, Two pieces of STRONG evidence, or One piece of SUPERIOR evidence.” §4.3.2

“The CSP SHALL collect and retain a biometric sample from the applicant during the identity proofing process” §4.3.3

“The CSP SHALL distribute or enroll the subscriber’s initial authenticator during an on-site attended interaction with a proofing agent.” §4.3.10

Source: NIST SP 800-63A-4, pages.nist.gov/800-63-4/sp800-63a/ial/

What assessors expect to see

- A clear control narrative linking identity proofing events to account provisioning and authenticator binding.
- Evidence that the same person proofed is the same person receiving privileged access.
- Documented exception handling, re-verification triggers and account recovery safeguards.
- Repeatable operating procedures backed by records from day-to-day operation.

Evidence checklist

1. Policy and governance

- ☐ Identity proofing policy defining populations, assurance targets and ownership.
- ☐ Role matrix (Security, IAM, HR, Compliance) with approval boundaries.
- ☐ Exception policy including approval authority and expiration windows.
- ☐ Retention and disposal policy for identity evidence and associated metadata.

4. Operational controls

- ☐ Runbooks for failed checks, suspected impersonation and stale identity records.
- ☐ Ticket samples proving that exceptions are tracked to closure.
- ☐ Periodic access recertification outputs for privileged users.
- ☐ Evidence quality reviews showing each control has been tested.

2. Enrollment and proofing workflow

- ☐ Documented attended proofing process for IAL3 candidates.
- ☐ Evidence capture specification (identity documents, biometrics, session context).
- ☐ Proof that verification artifacts are tamper-resistant and time-bound.
- ☐ Chain-of-custody documentation for any hardware-assisted flow.

3. Authenticator binding and access lifecycle

- ☐ Procedure showing how IAL3 identity is bound to an AAL3-capable authenticator.
- ☐ Provisioning logs with user, role, approver and timestamp lineage.
- ☐ Recovery flow controls to prevent help-desk bypass of high-assurance identity.
- ☐ Revocation and re-issue records for lost, stolen or compromised authenticators.

5. Re-verification and continuous assurance

- ☐ Trigger policy for re-verification (role change, recovery, high-risk events).
- ☐ Sample events showing successful trigger, review and decision outcomes.
- ☐ Metrics for verification completion time, failure rates and exception volume.
- ☐ Documented linkage between risk signals and identity step-up actions.

Map your evidence to NIST's IAL3 conformance criteria

NIST's conformance criteria for SP 800-63A-4 list IAL3-1 to IAL3-24. Group your evidence the same way so your assessor can test it criterion by criterion.

Group	NIST criteria	Evidence to have ready
Setting and proofing type	IAL3-1, IAL3-7, IAL3-11	Where each session took place (an approved private location), that it was on-site attended, and who attended.
Attended session and recording	IAL3-12 to IAL3-17	Agent attendance on live high-resolution video, the recording notice and consent, and the recording retention schedule.
Controlled devices	IAL3-18 to IAL3-21	The kit or kiosk allow-list, who controls each device between sessions, and inspection and chain-of-custody records.
Evidence and verification	IAL3-2 to IAL3-6, IAL3-8 to IAL3-10	The evidence collected, its validation against the issuer, and the biometric comparison result.
Notification and authenticator	IAL3-22 to IAL3-24	The notice of proofing sent to a validated address, and the authenticator enrolled during the session.

Trust Swiftly's full control-by-control IAL3 conformance mapping is available under NDA.

Common evidence gaps to close now

- **Control text without operating proof:** policy language with no evidence of day-to-day execution.

- **Disconnected systems:** proofing logs, IAM records and ticketing data do not share a common identifier.
- **Weak recovery controls:** account recovery paths downgrade assurance unintentionally.
- **No exception lifecycle:** exceptions are approved but never reviewed for closure or renewal.

Package evidence for review speed

- Create one evidence index per control family with owner, source system and last validation date.
- Attach one representative “happy path” and one “exception path” artifact set for each high-risk workflow.
- Normalize export formats and naming conventions before your pre-assessment review.
- Assign a single evidence coordinator to eliminate duplicate or conflicting submissions.

Need help mapping this to your program? Talk to an IAL3 specialist at trustswiftly.com/contact-us. More buyer resources: trustswiftly.com/resources.