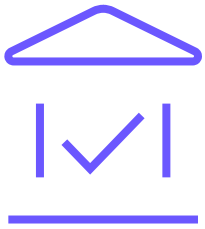

Your Credit Union MFA Documentation Checklist

The FFIEC's 2021 guidance on Authentication and Access concludes that single-factor authentication is no longer adequate for high-risk transactions and high-risk users. NCUA's Information Security Examination assesses access control and vendor risk directly. This checklist helps you get the documentation in order before an examiner asks for it.

Note: This checklist covers member-facing authentication. Your exam will also assess workforce and admin access, which should be treated as a separate exercise.

Step 1

Inventory every system where a member authenticates

Map every channel a member uses to prove who they are: online banking and mobile app, call center and IVR, branch and ATM/ITM, account recovery flows, and anything a service provider hosts on your behalf.

Do not forget: wire and ACH origination screens, card management portals, and any self-service flow that resets a credential.

- [ ] Authentication channel inventory complete

Step 2

Record the current authentication method per channel

For each channel, record what's actually in place: SMS OTP, KBA, app-based push or TOTP, passkeys, or nothing beyond a password.

Pay attention to where the method changes between channels. A passkey at web login that drops to security questions on a phone call is the gap, not two separate answers. An example is laid out below

- [ ] Authentication method documented for every channel

Step 3

Define high-risk transactions and high-risk members

The FFIEC guidance rules out single-factor authentication for high-risk transactions and high-risk members, and leaves your risk assessment to define both. Document your definitions:

- High-risk transactions: wire and ACH origination, account ownership changes, credential and contact-detail changes, large-value transfers
- High-risk members: levated transaction limits, business accounts, any segment with prior account-takeover attempts
- Standard risk:balance inquiries and low-risk self-service

The guidance doesn't define these terms. Your examiner will ask how you did.

- [ ] High-risk transactions and members defined and documented

Step 4

Document your rationale for keeping SMS OTP anywhere it remains

If any high-risk channel still relies on SMS OTP, document why, what compensating controls are in place, and your migration path. NIST SP 800-63B-4 classifies SMS as a restricted authenticator. Keeping it means four things: offer members at least one non-SMS alternative, tell them the risks, cover it in your risk assessment, and hold a migration plan. NIST binds federal agencies, not credit unions, but it defines the direction examiners look toward.

- [ ] SMS rationale, non-SMS alternative, and migration path on file

Step 5

Move high-risk access toward phishing-resistant authentication

Passkeys (FIDO2/WebAuthn) and hardware security keys are bound to the legitimate domain and can't be phished, intercepted, or replayed. Authentication layers that support these methods can be added on top of existing digital banking platforms without requiring a full replacement.

Priority targets: wire and ACH origination, credential changes, and any channel that was the entry point for a prior incident.

- [ ] Adaptive step-up rules defined for clinical and patient-facing workflows

Step 6

Document who controls the authentication decision

If a core or digital banking vendor sits between you and the login screen, document whether upgrading authentication is within your control or requires a vendor roadmap commitment. This determines whether Step 5 is a project you can start now, or a vendor conversation you need to start now.

- [ ] Authentication ownership documented: Internal control vs. vendor dependency

Step 7

Start the vendor risk conversation now

ISE examines vendor risk directly, and the FFIEC guidance extends authentication risk to third parties. If a vendor controls or influences your authentication method, your vendor risk file needs to reflect that dependency and your plan for any gap it creates.

Vendor reviews and procurement take months. Don't wait for an exam finding to start them.

- [ ] Vendor risk assessment reflects authentication dependencies

Step 8

Build the audit trail as you go

Monitoring and logging are core to the FFIEC's view of an authentication program. Capture from day one: who authenticated, with which method, on which channel, and what happened on any step-up or high-risk event.

Reconstructing this evidence after the fact is far harder than logging it as it happens.

- [ ] Authentication event logging active on priority channels

There's no final rule here to start a countdown. The FFIEC guidance is already in effect, and your next ISE exam is the checkpoint.

Read the full breakdown of why NIST restricted SMS OTP: →

Ready to talk through what exam-ready authentication looks like for your credit union? →