FREE RESOURCE · EXAM READINESS SERIES

The Community Bank Access Review Checklist

A practical, examiner-ready framework for reviewing user access across every system your bank runs — core banking, online banking, Active Directory, and every ancillary application in between.

This checklist reflects the same core expectations found in FFIEC's guidance on Authentication and Access to Financial Institution Services and Systems: identify every user and system in scope, enforce least-privilege access, recertify on a repeatable schedule, and document the whole process well enough to hand to an examiner without reconstructing it from memory. Work through the eight sections in order the first time; after that, most institutions run sections 2-7 every review cycle.

1. Build Your System Inventory

Do this once, then revisit it whenever you add or retire a system.

- [ ] List every system that touches customer or financial data — core banking platform, online and mobile banking, Active Directory, loan origination, wire and ACH systems.
- [ ] Include ancillary, vendor-hosted, and legacy applications, not just the core platform.
- [ ] Note who owns each system and when it was last included in a review cycle.
- [ ] Flag any system added since the last review that hasn't yet been incorporated into the process.

2. Gather Access Data

- [ ] Export the current user list from every system in scope.
- [ ] Capture role or privilege level for each user where the system supports it.
- [ ] Record the export date for each source file.
- [ ] Cross-reference the combined list against HR's active employee roster.

3. Reconcile to a Single Roster

- [ ] Combine all exports into one master roster — one row per person, one column per system.
- [ ] Flag name or username mismatches across systems (e.g., legacy usernames vs. HR records).
- [ ] Identify anyone with access but no clear, current business justification.
- [ ] Identify terminated employees or offboarded vendors with access still active anywhere.

4. Certify with Department Heads

- [ ] Route each department's access listing to the appropriate manager for review.
- [ ] Require an explicit response for every user: confirm, revoke, or flag for follow-up.

- [ ] Retain the request and the response — email is acceptable if it's retrievable later.
- [ ] Set a firm deadline and track down non-responses before closing the cycle.

5. Remediate & Document Exceptions

- [ ] Assign an owner and due date to every flagged item.
- [ ] Confirm remediation actually occurred — don't accept "addressed" without evidence.
- [ ] Document the business reason for any exception that was knowingly accepted.

6. Assess Privileged & Third-Party Access

This is the category examiners most often probe first.

- [ ] Separately review all administrative or privileged accounts across every system.
- [ ] Confirm vendor and third-party access is included, not just employee accounts.
- [ ] Confirm service accounts (non-human accounts) are inventoried and reviewed.
- [ ] For credit unions: confirm CUSO, shared branching, and volunteer board access is included.

7. File the Record

- [ ] Compile exports, the reconciled roster, sign-offs, and remediation notes together.
- [ ] Label the package with the review date and the name of the process owner.
- [ ] Store it somewhere retrievable without reconstruction before the next exam.
- [ ] Set a calendar reminder for the next cycle — quarterly or semi-annually is standard.

Signs you've outgrown the manual process: reconciliation eats more than a day or two of staff time per cycle · several people touch the process without clear version control · you've had a near-miss with lingering terminated-employee access · you're adding systems faster than your process can absorb. None of these are a compliance failure on their own — they're signs the manual version is becoming a labor and risk problem worth addressing before an examiner raises it for you.

Want this automated? All Access IDM connects to your core banking platform, Active Directory, and every ancillary application to build this roster automatically and route certifications for you — no manual reconciliation required. Request a walkthrough at aaidm.com/demo.html or email hello@aaidm.com.