argentum IT

VETERAN-OWNED MANAGED IT & CYBERSECURITY

FREE RESOURCE



FOR BANK LEADERSHIP & COMPLIANCE OFFICERS

FFIEC IT Exam Readiness Checklist

for Community Banks

36 plain-English checkpoints across the five areas examiners scrutinize most — access management, patch management, vendor & third-party risk, incident response & business continuity, and the documentation an examiner will ask to see. No jargon. Just a straight read on where you stand.

5	36	2011
EXAM FOCUS AREAS	CHECKPOINTS	FOUNDED, LOUISVILLE KY

Argentum IT, LLC is a veteran-owned managed IT and cybersecurity provider serving compliance-heavy institutions across Kentucky and Southern Indiana — including community banks preparing for FDIC, FFIEC, and NCUA IT examinations.

WHAT'S INSIDE

1. Access Management
2. Patch Management
3. Vendor & Third-Party Risk
4. Incident Response & Business Continuity
5. Documentation an Examiner Will Ask to See
+ A 3-tier self-score so you know exactly where you stand

This checklist is an educational resource and does not constitute legal, regulatory, or examination advice. Consult your compliance officer, legal counsel, or regulator for guidance specific to your institution.

How to use this checklist: These 36 checkpoints mirror the areas FFIEC examiners consistently focus on for community banks. Work through each section with your IT lead or managed services provider and check off only what you can actually prove today. Turn to the last slide to score yourself.

1 Access Management

Who can get in, and why

Examiners want proof that access is intentional, not accidental. Weak or stale access controls remain one of the most commonly cited findings in community bank IT exams.

- ☐ **Written access control policy** exists and has been reviewed within the past 12 months.
- ☐ User access is granted based on job role (least privilege) — not by default, convenience, or "that's how it's always been."
- ☐ A documented process removes access immediately when someone is terminated or changes roles — same day, not "when someone gets to it."
- ☐ **Multi-factor authentication (MFA)** is required for email, remote access, and every administrator-level account.
- ☐ The list of employees with administrator-level access is documented, kept as small as possible, and reviewed at least quarterly.
- ☐ Logs of who accessed sensitive systems, and when, are collected and actually reviewed — not just retained.
- ☐ Vendor and third-party remote access is individually approved, logged, and reviewed — not left standing indefinitely.

2 Patch Management

Closing known holes before someone else finds them

Most breaches don't exploit a mystery vulnerability — they exploit a known one that was never patched. Examiners will ask how fast you close gaps, not just whether you eventually do.

- ☐ A written patch management policy defines how quickly critical vulnerabilities must be patched, with separate timeframes for critical vs. routine updates.
- ☐ A current, accurate inventory exists of every server, workstation, and piece of software in your environment — including branch locations.
- ☐ Patches are tested before they're pushed to production systems, not applied blind.
- ☐ You can produce a report showing patch compliance across all systems — including branch and remote devices — on request.
- ☐ Any hardware or software that is end-of-life or no longer supported by the manufacturer is identified, with a documented remediation plan.
- ☐ Patch management records are retained and organized well enough to hand to an examiner without a scramble.

3 Vendor & Third-Party Risk

The area examiners scrutinize hardest

Since the 2023 interagency guidance on third-party relationship risk management, examiners expect banks to actively manage vendor risk for the life of the relationship — not sign a contract and move on.

- ☐ A current inventory of every technology vendor exists, with each vendor assigned a risk tier based on the data or systems it touches.
- ☐ Every critical vendor went through documented due diligence before being onboarded — not a handshake and a signature.
- ☐ Vendor contracts include the provisions examiners look for: right-to-audit, breach notification timelines, data ownership/return, and subcontractor (fourth-party) disclosure.
- ☐ Critical vendors are reassessed on a defined schedule — annually at minimum — not just once at signing.
- ☐ Current SOC 2 reports, cyber insurance certificates, or other independent assurance are collected and reviewed annually for critical vendors.
- ☐ Vendor and third-party risk is reported to the board or a board committee on a regular, defined schedule.
- ☐ A documented contingency plan exists for what happens if a critical vendor fails, is breached, or needs to be replaced.

4 Incident Response & Business Continuity

What happens when, not if

A plan that has never been tested is a guess, not a plan. Examiners increasingly ask for evidence of testing — not just a binder on a shelf.

- ☐ A written, board-approved incident response plan exists specifically for cyber events — not just a generic disaster plan.
- ☐ That plan has been tested with a tabletop exercise in the past 12 months, with the results documented.
- ☐ The plan defines exactly who notifies whom, and on what timeline, if a breach occurs — including regulatory notification deadlines.
- ☐ Backups are documented with a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- ☐ A full backup restoration has actually been tested in the past 12 months — not just confirmed as “completed” in a log.
- ☐ The Business Continuity Plan is reviewed and updated at least annually, and after any major change to operations or technology.
- ☐ Cyber insurance coverage has been reviewed against your actual environment and controls — not renewed on autopilot.

5 Documentation an Examiner Will Ask to See

Could you produce each of these within 24 hours?

Good controls that can't be documented and produced quickly look, to an examiner, exactly like no controls at all. Be honest about what you could hand over today.

- ☐ Written Information Security Program (WISP), board-approved within the past 12 months.
- ☐ Technology / cyber-specific risk assessment, updated within the past 12 months.
- ☐ Vendor inventory and due diligence files for every critical vendor.
- ☐ Incident response plan, plus evidence of the most recent test.
- ☐ Business Continuity Plan, plus evidence of the most recent test.
- ☐ Patch management policy, plus a recent patch compliance report.
- ☐ Access control policy, plus the most recent user access review.
- ☐ Board or committee minutes showing IT / cybersecurity oversight and reporting.
- ☐ Most recent independent audit, assessment, or penetration test results, plus a remediation tracking log.

How Ready Are You?

Count your checkmarks out of 36, and find your range below.

30–36	**Exam-Ready** You're in strong shape. Close the last few gaps and walk into your next exam with confidence.
18–29	**Gaps Worth Closing** You have real progress — and real gaps. These are exactly the kind of items examiners cite as findings.
Under 18	**High-Risk Before Your Next Exam** These aren't minor process gaps — they're the areas examiners cite first.

Not Sure How You'd Score? That's Exactly What a Discovery Call Is For.

In 15 minutes, we'll give you a clear, no-jargon read on where your bank stands against FFIEC, GLBA, and vendor risk expectations — and what it would take to close any gaps before your next exam.

Schedule Your Free 15-Minute Discovery Call →

Argentum IT (502) 473-9330 or Info@ArgentumIT.com

01
We Speak Examiner, Not Just IT

Our assessments and documentation map directly to FFIEC, GLBA, and NIST — not generic "best practices" language.

02
Vendor Risk, Actually Managed

We track and document the third-party risk piece most MSPs ignore — the area examiners scrutinize hardest.

03
Veteran-Owned, Compliance-First

We built our practice around regulated industries from day one in Louisville, Kentucky.