

COMMUNITY BANK IT & CYBERSECURITY CHECKLIST

Is your bank's technology
as secure, reliable, and compliant
as you think?

A practical self-assessment for
community bank leaders to identify
technology risks, strengthen security,
and ensure your bank can keep
serving your customers and community
with confidence.

**REDUCE RISK**

Identify potential vulnerabilities

**SUPPORT YOUR TEAM**

Keep employees productive
and confident

**STRENGTHEN COMPLIANCE**

Be better prepared for exams
and regulatory requirements

**PROTECT WHAT MATTERS**

Safeguard your customers,
your bank, and your community



Do You Know Who's Taking Care of Your Bank's Technology?

Community banks depend on technology to serve customers, protect sensitive information, keep employees productive, and operate reliably.

But you shouldn't have to become an IT expert to know whether the important things are being handled.

Use this checklist to start a conversation with your internal team and technology providers. You don't need to know every technical detail. What matters is knowing **who is responsible, what is being done, and whether you can verify it.**

1. IT Responsibility & Accountability

- ☐ We know exactly who is responsible for managing our bank's overall IT environment.
- ☐ Employees know whom to contact when they have a technology problem.
- ☐ Someone takes ownership of IT problems until they are resolved—even when another technology vendor is involved.
- ☐ We have a clear process for coordinating our IT provider, core provider, internet provider, software vendors, and other technology partners.
- ☐ Bank leadership receives understandable information about important IT issues, risks, and priorities.

Ask yourself:

If something significant happened tomorrow, would everyone know who owns the problem?

2. Cybersecurity

- ☐ We have documented cybersecurity policies and procedures appropriate for our bank.
- ☐ We know which systems, devices, applications, and accounts have access to sensitive information.
- ☐ Multi-factor authentication is being used where appropriate.
- ☐ Security updates and patches are being managed consistently.
- ☐ Endpoints and other applicable systems are actively protected and monitored.
- ☐ Administrative access is restricted and reviewed.
- ☐ We have a process for identifying and addressing security vulnerabilities.
- ☐ We regularly review whether former employees, vendors, or unused accounts still have access.

- ☐ Employees receive ongoing cybersecurity awareness training.
- ☐ We have a clear process for reporting suspicious emails, unusual activity, or potential security incidents.

Ask yourself:

If I were asked how we know these controls are working, could we produce evidence rather than simply saying, “Our IT company handles that”?

3. Backup, Recovery & Business Continuity

- ☐ Critical bank systems and data are backed up appropriately.
- ☐ Backups are protected from the same threats that could affect our primary systems.
- ☐ Someone monitors whether backups complete successfully.
- ☐ Backup restoration is tested rather than assumed to work.
- ☐ We know how quickly critical systems and information could reasonably be restored following an incident.
- ☐ Responsibilities during a technology disruption are documented.
- ☐ Our technology recovery plans align with the bank’s broader business continuity planning.
- ☐ Important technology vendors are accounted for in continuity and recovery planning.

Ask yourself:

When was the last time we proved that we could recover instead of simply confirming that a backup exists?

4. Technology Vendors

- ☐ We maintain an accurate list of important technology providers.
- ☐ We understand what each provider is responsible for—and what they are **not** responsible for.
- ☐ Technology-provider access to our environment is appropriately controlled.
- ☐ Someone coordinates vendors when a problem crosses multiple systems.
- ☐ Important technology-provider relationships and associated risks are periodically reviewed.
- ☐ We know whom to contact when a critical vendor experiences a problem.
- ☐ Important vendor documentation is organized and accessible when management needs it.

Ask yourself:

When two vendors disagree about whose problem something is, who takes responsibility for getting it resolved?

5. Employees & Access

- ☐ New employees receive only the technology access appropriate for their responsibilities.
- ☐ Access changes when an employee's role changes.
- ☐ Departing employees' access is removed promptly.
- ☐ Privileged or administrative accounts receive additional scrutiny.
- ☐ User access is periodically reviewed.
- ☐ Employees understand basic cybersecurity responsibilities.
- ☐ Employees have an easy way to get help when something looks suspicious.

Ask yourself:

Could we confidently explain who has access to sensitive systems and why they need it?

6. Monitoring & Maintenance

- ☐ Critical technology is proactively monitored rather than relying solely on employees to report problems.
- ☐ Security updates are applied through a defined process.
- ☐ Aging computers, servers, network equipment, and software are identified before they become emergencies.
- ☐ Technology issues and recurring problems are tracked.
- ☐ We have visibility into the overall health of our technology environment.
- ☐ Someone is looking ahead at technology needs instead of only fixing today's problems.

Ask yourself:

Is our IT strategy mostly preventative—or do we discover problems after employees are already affected?

7. Documentation & Preparedness

- ☐ Important IT systems and responsibilities are documented.

- ☐ Network and technology documentation is kept current.
- ☐ Hardware and software inventories are maintained.
- ☐ Important IT policies, procedures, reports, and supporting information can be located without a scramble.
- ☐ IT documentation isn't dependent on one employee or vendor having the information in their head.
- ☐ Management can obtain understandable answers to technology and cybersecurity questions.

Ask yourself:

What would happen if the person who knows the most about our technology suddenly wasn't available?

How Did Your Bank Do?

Mostly checked

That's encouraging—but don't assume checked means finished.

Ask your IT provider to **show you how they know** these areas are being handled. Good IT management should provide evidence, accountability, and understandable answers.

Several unanswered

An unanswered question doesn't automatically mean you have a problem.

It does mean you have something worth investigating.

Start by determining **who owns the responsibility and how the bank verifies that it's being handled.**

Many unanswered

It may be time for a more comprehensive conversation about how your bank manages technology.

You don't necessarily need to build an internal IT department. You may simply need a technology partner capable of taking greater ownership and giving leadership better visibility.

5 Questions to Ask Your IT Provider

1. **What are the three biggest technology or cybersecurity risks you believe our bank should address right now?**

2. **How are you verifying that our backups, security tools, updates, and monitoring are actually working?**
3. **When another technology vendor causes a problem, will you coordinate with them until the issue is resolved?**
4. **What documentation and reporting can you provide to help management understand our IT environment?**
5. **If you were sitting in my chair, what would you change about our technology over the next 12 months?**

A strong technology partner should be able to answer these questions clearly—without burying you in technical jargon.

You Don't Need to Become an IT Expert

You have a bank to lead.

Your job isn't to understand every firewall rule, security alert, backup job, or software update.

But you should be able to feel confident that the people responsible for your technology are **protecting it, monitoring it, documenting it, and taking ownership when something goes wrong.**

If this checklist uncovered questions you can't confidently answer, schedule a conversation with **EK Computer Inc.**

We'll talk about your bank, your current technology environment, and your concerns—and help you determine what deserves a closer look.

EK Computer Inc.

This checklist is intended as a general educational and discussion resource. It is not a comprehensive cybersecurity, regulatory, compliance, risk, or information-security assessment

and does not establish that a bank satisfies any particular regulatory requirement or security framework.