

# NetGain<sup>+</sup>

## TECHNOLOGIES

### CASE STUDY:

COMMUNITY BANKS FALLING  
SHORT ON ANNUAL IT AUDIT



---

## CASE STUDY: Community Banks Falling Short on Annual IT Audit

### Contents

03 Profile

04 Challenge

05 Solution

06 Results

---

# Profile

Community banks undergo a series of audits and examinations. In addition to the financial statement audit that evaluates the organization's adherence to standard accounting practices, banks must schedule a periodic information technology (IT) audit. The IT audit evaluates the design and effectiveness of the bank's internal controls—including security practices, efficiency protocols, development processes, and IT oversight.

The American Bankers' Association advises that putting internal controls into place is necessary but is insufficient without additional security measures. Community banks must have qualified personnel who are responsible for the IT environment: installing and setting up the controls appropriately; formulating and enforcing plans to deal with security breaches; and enacting new strategies to prevent future IT violations or infringements.

The IT audit allows independent and unbiased observers to review and assess a bank's information systems. The auditor will examine information systems, their inputs, outputs, and processing. The IT audit will evaluate the systems meant to guard the bank's data and the organization's ability to protect its information assets. During the IT audit, a bank also should be able to document its internal controls—availability, security and confidentiality, and integrity—including its ability to transmit information securely to authorized parties.

Ultimately, the goal of the required IT audit is to minimize risk for the bank's customers and vendors and to ensure compliance prior to the FDIC examination.

Community banks face real repercussions for poor examination results. The FDIC and FFIEC may limit a poorly performing bank's ability to function. Continued failure to address insufficient information technology may put accreditation at risk. Additionally, the FDIC may actually forbid banks from acquisitions and investments while operating under poor examination results.



To comply with banking regulations, community banks must undergo periodic IT audits.



The FDIC may actually forbid banks from acquisitions and investments while operating under poor examination results.

## Challenge

Two community banks recently sought counsel from NetGain Technologies to improve their IT audit outcomes.

### “Bank A” anticipated a poor IT Examination

“Bank A” was facing several challenges in proactively managing its technology environment. The bank’s existing information technology resources included an IT director and a technical support staff member. Support issues and a lack of technical expertise within the bank’s existing IT department caused project delays and missed deadlines.

When the FDIC announced that Bank A would be scheduled in six weeks for a long-overdue IT examination, the bank’s leaders knew they had a short window to make some necessary changes. They were aware that many projects had been languishing on the IT department’s “to do” list, including projects that, if left incomplete, would translate to a negative result on the examination. The situation was made more dire when the bank’s IT director unexpectedly tendered resignation to seek another career path.

### “Bank B” needed to recover from a negative audit

“Bank B” had recently dismissed its only IT staffer after receiving negative results from an IT audit. Then an unexpected ice storm forced the bank to work from an alternate operating site, in compliance with its documented disaster recovery plan. Technology at the alternate site failed to function as originally designed, keeping the bank from continuing its operations until days after the initial storm hit. In addition to bruising the bank’s reputation within the community, the snafu resulted in two financial damages: loss of revenue during the downtime, and fines imposed on it for being unable to meet its regulatory requirements.

While employees were suffering from a lack of confidence prevalent throughout the bank’s internal culture, Bank B’s executives expected an audit in the next six months and were concerned about the instability, insecurity, and lack of support for the bank’s technology.



---

# Solution

The two banks were facing vastly different circumstances, but both needed an IT solution customized to unique challenges. Seeking a long-term solution to avoid repeating their situations, both banks chose to join a managed IT services program.

## “Bank A” chose a trusted advisor

“Bank A” had previously contracted NetGain Technologies to install hardware. Its leaders were aware of NetGain Technologies’ all-inclusive IT support and managed services solution, Technology OneSource, and decided that it was a perfect time to make the switch to managed services.

NetGain Technologies came onsite to interview key personnel, collect necessary support information, and prioritize outstanding projects. NetGain’s team of business consultants and engineers provided short- and long-term roadmaps that prioritized business continuity first, a positive audit result second, and long-term stability and efficiency rounding out the plan.

Under a Technology OneSource contract, engineers patched and upgraded Bank A’s unsupported and insecure operating systems. They reviewed existing disaster recovery and business continuity plans, and revised protocols to reflect the client’s capabilities. Hardware and software reconfigurations corrected the bank’s backup failures and disaster recovery issues. NetGain Technologies became fully engrained in the company culture, and was a critical part of Bank A’s team drive for success.

## “Bank B” researched its managed service options

After researching local managed service providers, “Bank B” entered into a Technology OneSource relationship to begin the process of addressing its list of concerns.

NetGain Technologies’ engineers performed a complete operations and technical assessment, a routine part of new Technology OneSource initiatives. Beginning with a full and complete review of the client’s technology posture, from Bank B’s internet service provider down to the mission-critical applications on end-users’ workstations, the NetGain team acquired a comprehensive understanding of



Both banks needed an audit-friendly IT solution customized to their unique challenges.

### CASE STUDY:

#### Community Bank IT Audits

NETGAIN TECHNOLOGIES // 05

Bank B's business objectives and the best-practices misalignments that pose a risk to those objectives. NetGain Technologies provided a list of recommendations, prioritized based on specific risks to the client's unique organization, and further separated those recommendations that would be implemented at no additional cost to the client, as part of the new Technology OneSource agreement.



“Looking back, I have no doubt that we would have never made it through this transition without NetGain.” – *President of Bank A.*

---

## Results

Initially, community banks often switch to a managed IT services program to resolve a specific problem. Members of Technology OneSource find that the program allows them to focus their time and resources to banking, rather than “putting out fires” or attempting to keep ahead of evolving IT compliance requirements. Because both banks in this study opted to join Technology OneSource, their results are ongoing—but summarized below are the resolutions to their initial challenges.

### “Bank A” aced the audit, resumed growth mode

The FDIC examiners performed their audit as expected, and NetGain Technologies met with the examiners at Bank A's request. NetGain's team was able to provide the information the examiners needed to complete their assessment, as well as to instill confidence that the client was clearly in control of proactively and responsibly managing its technology.

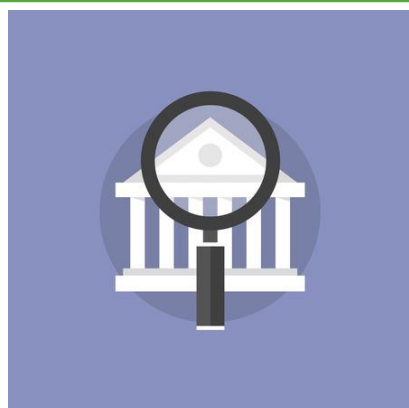
Preliminary audit results identified a few operational and technical action items that Bank A was able to correct easily prior to the final, positive report results. Through its partnership with NetGain Technologies, Bank A was able to meet its goals of ensuring a positive audit result, providing continuity of support as the organization underwent growth, and filling the role of the bank's departed IT director.

### FDIC praises “Bank B” for audit turnaround

Bank B's board decided that its existing business risks were unacceptable, and chose to engage NetGain Technologies' fixed-fee proposal to remediate the issues discovered. NetGain Technologies confirmed the new

proposed architecture with the client's software and hardware manufacturers to ensure compatibility, then created a phased approach for project implementation. One afternoon around three weeks after the project initiation, the president of Bank B stepped into the bank's Operations manager's office to express his concern that he'd noticed nothing taking place. He requested a deadline for beginning the migration of a specific mission-critical application—and was thrilled to learn that the migration had already taken place, three days prior, with no visible impact to the organization's operation.

Since implementing Technology OneSource, Bank B has completed an FDIC examination and an internal audit, both with positive results. Technology OneSource engineers have conducted live disaster recovery tests that provided proof-of-concept for the bank's entire technology infrastructure, and has an assigned team that meets quarterly with the bank's leadership to review current technology changes and strategic planning initiatives.



Bank B is “lightyears ahead of where they were during the previous examination.” – *FDIC examiner.*



2031 Georgetown Road  
Lexington, KY 40511

 844-77-SMART

 [SMART@NetGainIT.com](mailto:SMART@NetGainIT.com)

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

#### CASE STUDY:

Community Bank IT Audits

NETGAIN TECHNOLOGIES // 07

