September/October 2012

Bank Notes

A timely information and idea statement

Consider new technologies for old banking problems - Part 2

By Dean Lemons

In the May/June issue of *Bank Notes*, Part 1 of this series discussed how emerging technologies can have special benefits for community banks. When careful analysis is done to find the right solution for a specific application, the new technologies can provide community banks with a competitive advantage. Implemented effectively, they can increase operational efficiencies and optimize the bank's internal processes and delivery of customer services. Other new technologies can serve to secure the integrity of systems and safeguard private information.

Yet despite their proven advantages, many community banks are not utilizing these solutions or are only partially using them. So given their critical role and often unexplored benefits in the community banking sector, *Bank Notes* is doing a two-part series on emerging technologies. In the May/June issue, we discussed the following four topics:

- Business intelligence
- Customer relationship management
- Social networking and social media
- Mobility and management

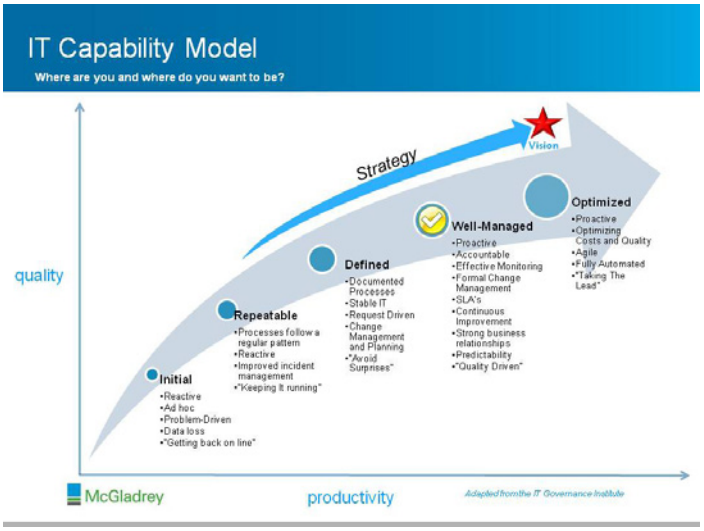
In this issue of *Bank Notes*, we'll be discussing the following four areas:

- Desktop virtualization
- Document management and process automation
- Data loss prevention
- Teller capture

The organizational reality check

First, let's review the basic analytical framework for evaluating new technologies. This was outlined in Part 1 of our series, but it's worth revisiting. The process starts with a technology investment analysis that examines your bank's information technology (IT) environment, business needs, current technologies and ownership issues. A methodical approach will help ensure that the investments are strategic and support your organization's business plan, as well as solve your existing systems' problems.

The IT capability model (pictured below) shows five different stages of maturity with respect to the management of systems and information – from initial (reactive and problem-driven) to repeatable (keep the status quo) to defined (stable with some controls) to well-managed (proactive and well-monitored) to optimized (mastery and leadership). If your bank is not in the latter two categories, then it's essential that you undertake an evaluation of your systems and processes and create a three to five year technology roadmap to help guide your investment decisions.



Identify relevant technologies

Once you have assessed your existing infrastructure and related processes, the next step is to identify technology improvement opportunities that would meet your current and anticipated business needs. Once completed, the technology plan will serve as a roadmap for future IT purchases. It is important to note that the technologies you identify today may not result in an investment this year or next – sometimes they are part of a longer-term plan that includes upgrades that will take place over a number of years. This means you should not expect to see immediate results. Over time, you'll see that purchase decisions line up with the business requirements plan, resulting in a reduction in the overall cost of technology ownership.

Now, let's turn to our four new solutions.

Consider new technologies, continued on page 3

LaPorte
CPAs & BUSINESS ADVISORS

An Independently Owned Member
McGladrey Alliance
McGladrey

Bank Notes

Basel III capital standard – What it means for community banks

By Sharon Griffin

As community banks struggle to compete in a sluggish economy, along comes Basel III, an international proposal for new capital standards that would increase capital requirements on all insured depository institutions and bank and thrift holding companies with assets over $500 million. Adopted by the Federal Reserve on June 7, 2012, the proposed rules are open for public comment through Oct. 22, 2012. The final rules will be phased in from 2013-2019, according to the roll-out schedule recommended by the Basel Committee on Banking Supervision, with the first phase going into effect on Jan. 1 of next year in the United States.

Basel III constitutes a fundamental redefinition of bank capital requirements. It adds a new capital component, common equity Tier 1 capital, and increases the minimum Tier 1 capital ratio requirement. Banks would be required to set aside capital over and above what has been set aside in the past. If capital levels fall below minimum requirements, a new capital conservation buffer framework would limit payments of retained earnings through capital distributions or discretionary executive pay.

Who is affected?

Beginning in 2013, all insured depository institutions and bank and thrift holding companies with assets of or over $500 million will be subject to increased capital requirements. The proposals would apply to all banking organizations currently subject to the minimum capital requirements, including national banks, state member banks, state nonmember banks, state and federal savings associations, certain top-tier bank holding companies domiciled in the United States and top-tier U.S.-based savings and loan holding companies.

Basel III is designed to ensure a consistent standard for quality of capital. Although its definition of capital is largely the same for small and large banks, the method used to measure the risk weighting of assets varies. Banks will have to track 13 categories of deductions and adjustments to capital and changes to risk weighted assets on a quarterly basis. The capital conservation buffer is intended to encourage banks to hold enough capital to reduce the probability of capital levels falling below minimum requirements in times of financial stress.

General proposals

The proposed changes will do the following:

- Revise the definition of capital to improve the ability of regulatory capital instruments to absorb losses
- Provide a multi-year transition period for the proposed requirements (expected to be from 2013-2019)
- Increase common equity capital requirements of 7 percent for common equity Tier 1 capital
- Phase out Trust Preferred as Tier 1 for all bank holding companies
- Establish higher capital requirements for high risk lending
- Remove references to credit ratings

Revised capital ratios

When fully phased-in, Basel III capital ratio requirements will be as follows:

- Tier 1 Leverage or Average Assets Ratio = 4 percent
- Common Equity or Risk-Weighted Assets Ratio = 7 percent *
- Tier 1 Leverage or Risk-Weighted Asset Ratio = 8.5 percent *
- Total Capital or Risk-Weighted Assets Ratio = 10.5 percent *
- Supplementary Leverage Ratio (Advanced Approach Investments Only) = 3 percent

  *Includes the 2.5 percent capital conservation buffer

Banks will have to demonstrate compliance with the three minimum capital requirements plus the capital conservation buffer. The complexity of Basel III's capital rules, with 13 deductions and adjustments to common equity and changes to risk weighting of assets, will affect the bank's ability to calculate, track and monitor ratios on a quarterly basis.

The costs of compliance

The timing of these proposed regulatory changes is, to put it mildly, not ideal for the community banking industry. It is occurring at a time when market conditions are lackluster, and full economic recovery has yet to be achieved. Many community banks are still grappling with anemic portfolios, a contracting deposit base and a decreasing revenue stream. Thus, at a time when many banks are still struggling, they are faced with the complex task of implementing new capital requirements. While some community banks are already in compliance with the new standards, others are not. For them, Basel III will force major revisions to capital plans and even require new sources of capital.

Some community banks could face significant compliance costs and administrative burdens. While larger community banks may be able to absorb these costs, small community banks with limited resources and expertise will have to hire additional resources to implement and monitor compliance going forward. The cost of complying with the new rules may put additional pressure on earnings, reduce net income and lead some community banks to seek out life preservers in the form of mergers or acquisitions.

To read more, go to: http://mcgladrey.com/Bank-Notes/Basel-III-capital-standard-What-it-means-for-community-banks

Payment Card Industry security standards: A primer for community banks

By Julie Perkins

Community banks often have difficulty understanding if they must comply with Payment Card Industry (PCI) security standards. Some may assume that PCI applies only to merchants and service providers. Banks that outsource credit and debit card processing also may be uncertain as to compliance requirements. Questions may further arise if the bank does not issue credit or debit cards at all.

Even if a community bank knows it must comply, understanding which guidelines are applicable to its institution can be challenging. Yet noncompliance could result in significant financial penalties and reputational damage to the community bank. Customer accounts could also be compromised.

To clarify this issue, this article will examine how PCI standards affect community banks, under what circumstances, and which standards should be followed in certain situations.

A short history lesson

To understand the purpose and scope of PCI standards, consider how the standards came to be. First of all, protection for card holder data has long been a hot topic in the financial services industry. The issue was highlighted by the 1999 passage of the Gramm–Leach–Bliley Act, which (among other things) stipulated that financial institutions must have a policy in place to protect information from security threats.

In the end, however, the PCI standards were developed not as a law or regulation, but as a private initiative by the payment card industry. The PCI Security Standards Council was launched in 2006 by the five global payment brands, Visa, Inc., MasterCard Worldwide, American Express, Discover Financial Services and JCB International; it was responsible for the development, management and education of the PCI standards. Shortly thereafter, the council introduced Payment Card Industry Data Security Standards (PCI DSS), a set of standards designed to ensure that merchants met minimum levels of security when they handled cardholder data. Later, the scope was broadened to include other entities.

PCI standards defined

The PCI standards are comprised of the following:

- Data Security Standard (PCI DSS) – The security standard for any organization that processes, stores or transmits cardholder data such as merchants and service providers
- Payment Application Data Security Standard (PA-DSS) – Security standard for the development of application software that processes, stores or transmits cardholder data
- PIN Transaction Security (PCI PTS) – Security standard for PIN entry devices such as credit card terminals
- Point-To-Point Encryption (PCI P2PE) – Security standard for the encryption of communications between two endpoints

PCI standards *do* apply to banks

Unbeknownst to some community banks, the above PCI standards *do* apply to them, as well as to merchants and service providers. The specific requirement is spelled out on page 5 of the PCI DSS, and it states that the standard "applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers and service providers, as well as all other entities that store, process or transmit cardholder data."

To read more, go to: http://mcgladrey.com/Bank-Notes/Payment-Card-Industry-security-standards-A-primer-for-community-banks

Consider new technologies, continued from page 1

Desktop virtualization

Virtualization is a software solution that enables multiple computers to run on the same hardware device, fully isolated from one another, as if they were running as separate computers. Most community banks begin the virtualization process with servers. It is important to realize that the server virtualization mindset focuses on CapEx reduction, whereas much of the value associated with desktop virtualization lies with OpEx reduction, which, as revealed below, is primarily associated with IT related operational and support efficiencies.

Virtualization is clearly catching on. According to "2012: Virtual desktops are all the rage" in NetworkWorld.com, Dec. 22, 2011, research firm, Gartner says that 40 percent of servers overall have been virtualized, but that is predicted to grow to 75 percent by 2015. Here are some ways that desktop virtualization improves operational efficiencies:

- Allows management of physical and virtual desktops from a single console
- Leads to higher availability, security and improved business continuity of desktops in the datacenter
- Extends the life of existing personal computer hardware
- Allows for the use of thin client hardware terminals
- Gives bank the ability to provide secure remote access to mobile users

Despite these benefits, desktop virtualization may not be the best fit for some banks. Whether it does or not depends on the type and mix of applications, total number of users and other factors. In fact, a number of community banks find that presentation virtualization, which many may recognize as Citrix Presentation Server or XenApp, is a better fit.

To read more, go to: http://mcgladrey.com/Bank-Notes/Consider-new-technologies-for-old-banking-problems-Part-2

Bank Notes

September/October 2012

Consider new technologies for old banking problems - Part 2

Basel III capital standard – What it means for community banks

Payment Card Industry security standards: A primer for community banks

111 Veterans Memorial Blvd., Suite 600
Metairie, LA 70005

Address Service Requested

For additional copies or change of address, contact LaPorte CPAs & Business Advisors. For more information, contact Leslie Paull, at (504) 835-5522 or e-mail her at lpaull@laporte.com. Visit our Web site at www.laporte.com.

Bank Notes

September/October 2012

Printed in U.S.A.