Introduction

The banking industry has often been a proving ground for the application of evolving technologies. The volume of transactions, the amount of associated data, and the need for efficiency and accuracy make banks and other financial institutions ideally suited to prove that new technologies are ready for primetime. However, the fundamental need in the banking industry to effectively manage risk creates a dilemma for banks as they seek to implement new technology. In the past, banks and financial institutions took comfort in the inherent risk management of mainframe technology, which allowed for centralized security and tighter controls. However, the growing capabilities of desktop hardware and software, and expanding network bandwidth have removed the security blanket of mainframe-based computing. More and more of the responsibility for capturing, storing and processing transaction and customer data has been migrated away from central systems and data centers into the hands of branches and regional operating centers, and, with the growth of self-service via the internet, telephone, or through ATMs and POS terminals, into the hands of the customer.

These changes have allowed banks to increase efficiency and to better meet customer demand for ease of use and greater flexibility. Furthermore, this evolution has somewhat leveled the playing field as access to any financial institution, regardless of size or location, is only a few Internet clicks away. However, banks now face the challenge of meeting increasing demands from regulators and from the market for controls on financial and customer data that meet or exceed what existed in the day of the mainframe. Increased reliance on distributed processing and on public and private network capabilities multiplies the potential points of failure that banks must protect against and provides increased opportunities for hackers and fraudsters to gain access to bank systems and information. Recent events, including the impact of 9/11 on financial centers in New York and the rapid growth of identity fraud have highlighted the need for improved recovery capabilities and controls. However, the propagation of wireless services and capabilities clearly driven by the demand for flexibility and open access to financial services will only grow.

Increased regulatory oversight and scrutiny only highlight the complexity of managing banks especially in today's distributed processing environment. Corporate excesses over the last decade led to the 2002 passage of Sarbanes-Oxley, requiring increased controls over financial reporting. In the financial industry, a new regulatory focus on operational risk, privacy, and the role banks can play in shutting down the flow of capital to terrorists and other criminal organizations has placed an increased burden on banks to effectively manage and control their networks and the data that they process. These competing demands from the public and regulators for increasing access and flexibility, greater controls, and improved recovery capabilities mandate a rethinking of how banks manage their networks, test their systems and procedures, and plan for business continuity in the case of a disaster. Management of the network, testing of critical processes, and disaster recovery processes, which may have been viewed as separate and distinct functions in the past, are becoming increasingly interdependent, and are likely to continue to converge and overlap as new regulations take effect.

Background

Section 404 of Sarbanes-Oxley requires that companies clearly define management responsibility for establishing an adequate internal control structure and procedures for financial reporting. The annual report must include an internal assessment of the adequacy of the control structure and procedures. Likewise, the external auditor must attest to management’s assessment of the controls and procedures. The requirements of Section 404 have already led to countless hours of effort in every industry to ensure that the appropriate controls are in place for calendar year filers at the end of 2004. But given the
number and complexity of financial transactions handled by financial institutions, and the amount of regulatory oversight of the financial industry, the impact of Sarbanes-Oxley has been particularly far-reaching for banks. The challenge of compliance is complicated even further for banks as mergers and consolidations continue. The large and expanding footprint of many financial institutions, with regional operations and the associated distributed technology components, often inherited from acquired institutions, creates a fragmented environment that makes creating the required unified view at the top even more difficult. While the accuracy and quality of financial data has always been vital to the day-to-day operations of any financial institution, Sarbanes Oxley demands a level of transparency in these processes that has not been required until now.

As the industry enters its first cycle of annual reporting with initial compliance efforts complete, the next challenge will be to ensure that the appropriate structure and procedures are in place to maintain compliance on an ongoing basis. Achieving initial compliance has been far more difficult, time-consuming, and costly than anticipated when the legislation was first enacted. The initial compliance date has been delayed twice since 2002. In a survey of its members, Financial Executives International found that, for companies with revenue in excess of $5 billion, the cost of first year compliance averaged $4.7 million, including 35,000 person-hours (approximately 20 FTE years) of internal effort. In the scramble to achieve compliance, it is certain that many organizations were forced to implement one-off solutions that will be difficult and costly to repeat every year. As many as half of the companies subject to the requirements of Sarbanes-Oxley are expected to retool their control structures in the next one to two years to build a more efficient, repeatable process.

**Information Technology and Network Implications**

As the means to store, secure, analyze, and report on financial data, corporate information technology infrastructure is a critical component of successful compliance with Sarbanes-Oxley. Particularly as the work of compliance transitions from project status to an ongoing process, the need to tailor the infrastructure to support efficient, repeatable processes that integrate the controls and assurance required by Sarbanes-Oxley into the day-to-day operations of financial organizations will be a key driver of success. And as is so often the case, successful integration will be accomplished through the enhancement of corporate systems, infrastructure, and the codification of processes used to manage and test them.

The first step in this process will be establishing a comprehensive inventory of key financial data and of the systems, applications, and methods used to gather, process, and store these data. In addition to the ability to ensure the accuracy of financial reports, the control environment must also provide assurance that material, non-public information is secure and is not selectively available to any outside parties prior to the formal public release of such information. As such, the data inventory should include information necessary to distinguish not only whether the data are key to financial reporting, but the level of security required to ensure timely disclosure. It will also be critical to identify the source of the data, establish the system of record for each piece of key information, and define what other systems and processes access, update, and copy the information. While an inventory may have been created already as part of the initial compliance effort, it is critical to ensure that the inventory is robust enough to accommodate evolving data and reporting requirements.

With a dynamic inventory system in place to identify key financial data and material non-public information, the classification information can now be leveraged to support ongoing compliance. As financial institutions grow and evolve over time, reporting mechanisms will need to adapt to changes. Change management processes should now require a review of the inventory information to determine whether a change involves any data, systems, or processes that are critical to financial reporting. If this is detected, additional due diligence will be required prior to implementation of the change to ensure that the integrity of the financial report process and any associated controls are not adversely affected. Depending on the nature and scope of the changes, and their potential impact on key financial data, this due diligence may include regression testing of the financial reporting process and security of material non-public information.

**The Distributed Processing Environment**

Given the size and complexity of the information technology infrastructure of today’s financial institutions, the change control procedures discussed above are necessary, but may not be sufficient to ensure that seemingly innocuous changes do not adversely affect key financial data. The advancing capability of desktop hardware, software, and end users continues to lead to more distributed processing and to development of business critical technology solutions that are not controlled by central information technology resources. Any user with a spreadsheet program, desktop database software, or a webpage may be creating, gathering, replicating, or modifying data that are critical to the financial reporting process.

Several steps must be taken to prevent errors from entering into the reporting process and the control
environment. First, every one must be educated on the scope and impact of the new regulations, and on how to learn more if they believe that their work may have an effect on financial reporting. In particular, this training and education should include instruction on how to access inventory information to determine whether inputs to or outputs from an end-user process are classified as key financial data or material nonpublic information. Second, sound network access controls based on inventory classification must be implemented and enforced. When end-users request access to data classified as key to financial reporting, compliance resources can review the reason for the request, and how the data will be used to assess any risks to financial reporting or disclosure.

**Testing and Validation**

As indicated above, changes to processes that affect financial reporting are inevitable. The steps suggested so far represent a proactive approach in the effort to identify compliance risk from any potential changes prior to implementation. However, relying on education and compliance with new controls and procedures will not prevent all changes that might adversely affect financial reporting, from slipping through. To address this risk and satisfy the executives and external auditors who are certifying reports, experts are also recommending a regular schedule of regression testing and monitoring to avoid a surprise at reporting time. This testing and monitoring should be carried out on a regular schedule outside of testing related to any specific change, and would serve as a key input into the executive signoff and external auditor attestation.

The need for so much testing raises another question. As any one involved in system testing and quality assurance will tell you, one of the greatest challenges to effective testing is creating and maintaining a representative test environment. The test environment must reasonably approximate the environment in which the production process will run. Any variations between the test and the production environment can raise questions about how applicable the test results will be in the real (production) world. These concerns must constantly be balanced against the time, effort, and expense associated with maintaining a true mirror of production. Furthermore, as the scope of the process to be tested grows, the complexity and the resources required to create and maintain the test environment grow with it.

For just this reason, creating and maintaining an environment for Sarbanes-Oxley compliance testing at a financial institution is particularly challenging in the distributed processing world. Simply put the vast majority of operational systems at banks and other financial institutions process monetary transactions that ultimately feed into the financial reporting processes covered by Sarbanes-Oxley. While the regulations do include disclaimers for materiality of the potential impact on the company’s overall financial reports, where that line can be drawn is not clearly defined at this point, and will most likely evolve over time. As a result, even a moderately risk-averse approach to testing dictates that the large majority of a bank’s operational systems and network components be considered in scope for Sarbanes-Oxley testing.

**Controlling the network and establishing a test environment without breaking the bank**

As financial institutions begin to ponder the question of how to maintain and demonstrate ongoing compliance with Sarbanes-Oxley, options may seem somewhat limited on how to control the network and create the testing environment. However, by rethinking current processes for network support, testing, and recovery, new opportunities may present themselves. For banks willing to outsource support and maintenance of their networks and information technology infrastructure, many of the processes should already be in place to ensure the security and control of the production environment as part of the outsourcing relationship.

To ensure efficient use of an outsourced network, a central point of contact is generally used to approve and prioritize requests for additions or changes to the network. This central point of contact may be in supply chain management or in a relationship management group in information technology. While this group may not have considered controls related to Sarbanes-Oxley in the past, it will be more efficient to leverage this gatekeeper process that is already in place to assess the compliance risk of infrastructure changes, than to create a separate checkpoint. In fact, this built in feature of an outsourced production environment may provide the additional business benefit necessary for some banks that have considered outsourcing in the past, but have not been able to justify making the switch yet. By leveraging the vendor process to enforce the appropriate controls, banks can share a portion of the fixed costs of enforcing the new regulatory controls with the outsourcing vendor's other clients, thereby reducing the overall cost of their compliance program.

Even for financial institutions that have no intention of outsourcing their production environment, disaster recovery and business continuity hot-site providers may offer the most economical solution to create a standing test environment for compliance testing. To offer an effective recovery option, these vendors must already have the capability and capacity to substantially replicate the institution’s production environment. Furthermore, these providers are accustomed to organizing and scheduling their resources for periodic testing of their...
client’s recovery plans. Sarbanes-Oxley compliance testing will likely be more frequent than the current annual or semi-annual disaster recovery tests and may demand increased capacity from these vendors. However, since it will generate a revenue stream and workload that is more consistent and predictable than the risk-based disaster recovery business, the opportunity also represents a win for the vendors, allowing them to better utilize idle bandwidth and justify investments in additional capacity with a steadier stream of offsetting revenue.

As with the outsourcing of the production environment, the participating financial institutions can limit their internal investments in additional testing capacity, share part of the fixed costs of compliance testing with other clients, and may be able to negotiate favorable rates for compliance testing by bundling it with disaster recovery vendors. In fact, once the test environment and disaster recovery are combined through a single provider, some institutions that have not even considered outsourcing support of the production network may want to reconsider based on further discounts and other benefits of an all-in-one solution.

This integrated approach to controlling and managing the network, testing regulatory compliance, and ensuring recovery capabilities is not necessarily common practice today, and may require some rethinking of vendor relationships. Providers that specialize in one or the other of these services may not have the resources or desire to expand their offerings. To the extent that bundling of these services can yield savings and greater effectiveness in testing, controls, and recovery, banks may need to search out vendors that can provide a comprehensive solution.

**Other compliance considerations**

While Sarbanes-Oxley is the most pressing driver of the current focus on controls and risk management within banks, work done in support of Sarbanes-Oxley may be leveraged to support and enhance compliance with other recent and upcoming regulatory changes. By expanding the scope of the Sarbanes-Oxley data inventory to include the inventory and classification of sensitive customer data and credit information, banks may be able to build more efficient processes and controls to satisfy FACTA, Anti-Money-Laundering, and Patriot Act requirements and have substantial infrastructure in place to support any potential regulatory changes that may arise from recent, high-profile incidents of identify theft from third party data consolidators.

Likewise, with BASEL II expanding the focus of international oversight to include operational risk, the changes made in support of Sarbanes-Oxley will strengthen overall operational risk management. In addition to being able to certify the quality of their financial reports, banks will be able to demonstrate a better understanding of their key data, improved controls on their production network, enhanced testing capabilities and stronger, more robust relationships with their infrastructure and disaster recovery providers.

**Conclusion**

The evolution of technology in the financial industry, recent headlines, and changes in the regulatory environment have created a perfect storm for banks as they seek to grow their business, become more efficient, and respond to increasing market demands for flexibility. Technology and network capabilities have dictated that banks move from a central to a distributed processing model. Meanwhile, events such as Y2K, 9/11, and corporate scandals have mandated the need for effective risk management and disaster recovery capabilities. In response to these events, new regulations and greater scrutiny dictate a need for greater transparency and the ability to demonstrate the effectiveness of internal controls.

A great deal of time, effort, and expense has been dedicated over the last two years to satisfying the new regulatory requirements, particularly of Sarbanes-Oxley. With initial compliance efforts largely complete, banks must now figure out how to live with these new regulations going forward. While satisfying regulatory requirements is often viewed as a cost of doing business, a more holistic approach to these new regulations offers banks an opportunity to consolidate functions, increase efficiency, and save money while complying with the common sense spirit of the new requirements.

In a world of resource constraints, items such as comprehensive data inventories, enhanced network controls, and more robust test infrastructures have remained the stuff of information technology strategy and vision. While the benefits have always been intuitively appealing, they are difficult to quantify. As a result, when combined with the complexity, cost, and effort to create these features and capabilities, few organizations have demonstrated the will to move them from vision to implementation. These new regulatory requirements have created a now urgent need for investing in these changes. Banks that approach these changes judiciously and with more than compliance in mind, can reap additional, significant bottom-line business benefits. Providers of test and production network outsourcing and disaster recovery services will be well-positioned to help in this effort by preparing to offer a comprehensive suite of these services in response.
Cheryl Yaeger is President of BenchMark Consulting International. She has extensive experience in the financial services industry with the delivery of large integrated change initiatives such as bank mergers and consolidations, technology integration activities and strategic alignment evaluation and adjustment.

Paul McNamara is a consultant at BenchMark Consulting International with more than 18 years of financial services experience. He specializes in retail, lending, operations, information technology, project management, and associated business process design and implementation.

BenchMark Consulting International has specialized in improving the financial services industry since 1988. The company is a management consulting firm that improves the profitability of its financial services clients through the delivery of management decision making information and change management services to realize the benefits of business process changes. BenchMark Consulting International’s expertise is in the measuring, designing and managing of operational processes.

The firm has worked with 36 of the top 50 (in asset size) commercial banks, all 14 automobile captive finance corporations, several of the largest consumer finance corporations and many regional banks throughout the United States. Internationally, BenchMark Consulting International has worked with the five largest Canadian commercial banks, more than 40 European organizations in 11 different countries, in addition to financial institutions in Latin America, Asia and Australia.

The company is a wholly owned subsidiary of Fidelity Information Services, Inc., with clients in more than 50 countries and territories, providing application software, information processing management, outsourcing services and professional IT consulting to the financial services and mortgage industries. BenchMark has dual headquarters in Atlanta, GA and Munich, Germany. For more information please go to www.benchmarkinternational.com