

# Technology Outsourcing: A Community Bank Perspective

***Eric Robbins and  
Joe Van Walleghem***

Eric Robbins and Joe Van Walleghem are economists in the Division of Supervision and Risk Management of the Federal Reserve Bank of Kansas City. The article has benefited greatly from the comments of Ken Boldt and David Au. The views expressed in this article are those of the authors and do not necessarily reflect those of the Federal Reserve Bank of Kansas City or the Federal Reserve System.

## INTRODUCTION

As the technology used by financial institutions has become increasingly sophisticated and interconnected, management of risks associated with this technology has become more challenging. Risks to the availability of processing systems to support customer transactions, business continuity, and the integrity and security of customer account information, and risks related to outsourcing technology services have received heightened attention in the industry and from regulators. The events of September 11 and widely publicized reports of identity theft and other information system vulnerabilities have highlighted these concerns and point to the necessity for rigorous controls to protect the integrity and continuity of technology used in the industry. For many institutions, outsourcing is an attractive way to gain access to technology and the resources and expertise needed to manage the risks that come with it. However, institutions that rely on technology outsourcing face the additional challenge of ensuring that these risks are appropriately addressed by external technology service providers.

Management of risks related to outsourcing of technology services is particularly relevant for community banks, most of which rely on third-party vendors for essential technology services like core processing.<sup>1</sup> Community banks often turn to outsourcing because they do not have the scale of operations to effectively develop and maintain complex systems. Third-party technology service

providers serve this need by giving banks an alternative to developing the processes in-house.

Outsourcing technology services does not reduce or eliminate the financial institution's responsibility for ensuring that the fundamental risks associated with information technology and the business lines that use it are effectively addressed. The transfer of day-to-day control over essential processes to a third-party vendor means that some risks will be realized in a different manner than if the activities were performed under the direct control of the institution. The control framework for outsourced technology services has received heightened attention in the industry and has become a key factor in the regulatory examination process for institutions that outsource critical processes.

The purpose of this article is to provide information about the evolving bank technology service provider industry and how it could affect community banks' risk management practices. The first section describes the bank technology service provider industry and the trends and economic fundamentals that govern the prospects of firms in the market. The article details consolidation trends in the bank technology service industry and profiles the largest bank information technology firms as well as regional firms and software vendors. The article then describes the extent that community banks rely on third-party vendors for bank technology processing and factors that affect the choice of vendor. The final section reviews information on outsourcing risk management practices and standards.

## **STRUCTURE OF THE TECHNOLOGY SERVICE PROVIDER INDUSTRY**

A bank in the process of selecting a technology service provider can gain perspective on the available choices by considering the selection of products and vendors, their market strategies and competitive relationships to one another, and the fundamentals driving those strategies. All of these factors comprise the structure of the industry.

The federal banking agencies, through the Federal Financial Institutions Examination Council (FFIEC), have identified approximately 150 firms that provide significant information technology services to commercial banks and thrifts.<sup>2</sup> Of the technology service providers identified by the agencies, approximately 90 are providing core processing services or software. These companies range from Fortune 500 firms with a national market presence to small privately owned companies. Included in the total number of firms are specialists in banking technology services and firms that are diversified in other sectors of technology or financial services. Some of the firms provide the whole range of applications used by banks, including core processing software, check imaging, electronic banking, asset-liability modeling, payments processing, point-of-sale (POS) and ATM processing, teller and lender packages, and customer relationship management software, as well as processing of mortgages, credit cards, insurance, and a host of other applications. Other firms specialize in a single product or product suite.

The bank technology service provider industry is in a transition phase being brought about by changing economic fundamentals in banking and in information technology.<sup>3</sup> Consolidation among the bank technology service providers has been ongoing for a number of years, but the process seems to be accelerating with new mergers and acquisitions a frequent occurrence.<sup>4</sup> Among the reasons is slowing revenue growth related to consolidation in the banking industry.

Consolidation in the banking industry is reducing the field of potential bank customers for the technology service providers. The aggregate number of banks has declined by nearly 50 percent since peaking 20 years ago. Although the technology needs of banks in the aggregate have grown rapidly, industry consolidation has shifted industry assets to the largest banking organizations that rely less on outside technology service providers than do smaller banks. This consolidation has been especially pronounced among the top-tier banking

organizations.<sup>5</sup> During the last 10 years, the proportion of commercial banking industry assets held by the 10 largest banking organizations has increased to above 50 percent.

The shape of the consolidation that is taking place among the bank technology service providers furnishes insight into the fundamentals and future direction of the market. Market extension, vertical integration, and adjacent market mergers describe some of the consolidation strategies being followed. The mergers promote efficiencies by increasing revenues over which to spread fixed research and development and other costs. This factor is likely becoming more important as the complexity of technology services increases along with the expertise required in providing them. One theme that is evident from the consolidation pattern relates to efforts by the large bank processors to serve many of the financial services markets being affected by financial convergence such as insurance, securities, and investment management. The broadened scope provides opportunities for cross-selling and product integration. Greater standardization and the need for common platforms also may have contributed to consolidation along with the need for greater reliability and backup capabilities.

To look at trends and structure of the bank technology service provider industry, we divided the industry into three segments for discussion purposes. The first segment profiles the largest publicly traded companies that provide core processing services. These firms are well represented in most geographic markets for bank processors, and the experience of these companies provides an overview of the consolidation patterns and business strategies in the industry. A second segment includes significant regional technology service providers. The third segment reviewed covers independent software companies—comprising firms that are known for turnkey<sup>6</sup> or service-center processing software but are not subsidiaries of the larger companies. In most markets, banks selecting

technology service providers can choose from among the largest providers along with the smaller regional companies and software vendors.

## National Technology Service Providers

The largest providers of core processing services for regional and community banks include five companies: Fiserv, Brown Deer, Wis.; Metavante, Brookfield, Wis.; Fidelity National Financial, Jacksonville, Fla.; BISYS Group, New York, N.Y.; and Jack Henry and Associates, Monett, Mo.<sup>7</sup> The strategies these companies follow are indicative of the competitive changes that are taking place in the financial services and information technology industries.

In different ways, these companies have evolved through the realignment process that has transformed the technology service provider sector over the past 20 years. As financial institutions increase the number of services they offer their customers, technology service providers respond with enabling products. Fiserv, Fidelity National Financial, BISYS, and Metavante have all diversified their product lines in order to support banks and other financial services companies that are offering services related to insurance, investment management, and securities. Many of the major technology service providers, as well as some regional providers, either currently offer or are adding complementary services related to item processing and check imaging. These areas have received increased attention following the enactment of the Check Clearing for the 21st Century Act (Check 21).<sup>8</sup> Following are brief descriptions of each of the top five technology service providers.

Fiserv was formed in a management buyout of First Data Processing in Milwaukee, Wis., and Sunshine State Systems in Tampa, Fla., in 1984. Initial acquisitions were from banks that were exiting the core processing business. Since its formation, Fiserv has made more than 100

acquisitions, including 33 core processing companies. Fiserv's customer base is broadly diversified across the financial services sector and includes banks, mortgage companies, broker-dealers, retirement plan administrators, insurance companies, health care companies, and trust companies. Fiserv also works as a broker-dealer for banks that offer nondeposit investment products.

The recent emergence of Fidelity National Financial as one of the largest bank processors is indicative of the rapidity of the realignments that are impacting bank technology service providers. Fidelity National Financial, the country's largest title insurance company, entered the bank technology business by acquiring Alltel Information Services in April 2003. Fidelity has extended its market share through a series of acquisitions that have included Aurum Technology from EDS in February 2004 and InterCept in September 2004.<sup>9</sup> Both Aurum Technology and InterCept have significant community bank customer portfolios. Fidelity's strategic acquisitions in the bank core processing sector allow it to leverage its position in the financial services sector, which is based in title insurance and mortgage processing for a large number of domestic and international customers.

The BISYS Group, Inc. was formed as a leveraged buyout of Automatic Data Processing's (ADP) data processing business in 1989. BISYS began as a technology service provider for community banks and has diversified as a technology outsourcer for all segments of the financial services industry. BISYS' business lines also include services for mutual funds and other investment firms, retirement services, and insurance distribution. Its strategy is to provide technology services that will allow clients in banking, insurance, and investments to capitalize on convergence in the financial sector.

Among the five largest bank technology service providers, Metavante is the only provider owned by a banking company. A subsidiary of Marshall and Ilsley Corporation, a bank holding company, Metavante offers core account processing to financial

institutions and is a deposit system outsourcer for larger banks. In May 2004, Metavante acquired Kirchman Corporation. Kirchman is the developer of Kirchman Bankway, a core processing turnkey application that is used primarily by the community banking market. The Kirchman acquisition made Metavante a significant supplier of turnkey software for the community bank market. This is a good example of a bank technology service provider's attempt to develop business relationships with all sizes of banking institutions.

Jack Henry and Associates is the most prominent example of an independent core processing company that grew up servicing community banks in the former unit banking states, which were concentrated in the Midwest. Until recently, many of these states limited banks to one or two locations, resulting in a banking structure with large numbers of small independent banks reliant on third-party technology service vendors. Jack Henry provides ancillary products to its core processing customers, such as ATM network software, imaging, customer relationship management solutions, Internet banking solutions, and other services. Stepping outside its traditional role as a processor, Jack Henry recently acquired Banc Insurance Services (BIS). BIS assists financial institutions in forming insurance agencies but does not provide insurance processing services. Compared with other major technology service providers, Jack Henry concentrates primarily on services for banks and credit unions.

Table 1 provides summary information on the top five processing companies. This information includes their business segments and corresponding revenues, acquisitions related to core processing, and core processing software products. The bank technology service providers are not ranked because segment revenues disclosed in the firms' financial reports are not directly comparable. However, Fiserv, Metavante, Fidelity, BISYS, and Jack Henry are generally acknowledged to be the most prominent providers of core processing services to community banks.

Table I

## Characteristics of Top Five Core Processing Technology Service Providers

Revenue	Business Segments	Processing Acquisitions	Software
<b>Fiserv Incorporated (year-ending December 31, 2003)</b>			
\$ 1,974MM	<ul style="list-style-type: none"> <li>Financial institution outsourcing, systems and services</li> <li>Health plan management services</li> <li>Securities processing and trust services</li> <li>Other services: plastic card and document services</li> </ul>	EDS Credit Union Group, 2003 Precision Computer Systems, 2003 NCR Bank Processing Operations, 2001 Central Service Corporation, 1997 FIS Group, 1997 Information Technology, Inc. (ITI), 1995 Financial Institutions Outsourcing, 1993 San Antonio Inc., 1984 First Data Processing, 1984 Sunshine State Systems, 1984	CBS CustomerFile ITI Premier II Precision BAIS Precision VISION
\$399MM			
\$224MM			
\$102MM			
<b>Fidelity National Financial (year-ending December 31, 2003)</b>			
\$5,986MM	<ul style="list-style-type: none"> <li>Title insurance and escrow</li> <li>Financial institution processing and outsourcing</li> <li>Real estate information services</li> <li>Specialty insurance</li> <li>Corporate and other services</li> </ul>	InterCept, September 2004 Kordoba GmbH & Co., 2004 Aurum Technology, 2004 Customized Database Systems, 2004 Sanchez Computer Associates, 2004 ALLTEL Information Services, 2003	Horizon BancPac BancLine Miser Sanchez Profile
\$853MM			
\$560MM			
\$135MM			
\$181MM			
<b>Marshall &amp; Ilsley Corporation (parent company of Metavante, year-ending December 31, 2003)</b>			
\$1,370MM	<ul style="list-style-type: none"> <li>Banking</li> <li>Data services (Metavante)</li> </ul>	Kirchman Corporation, 2004 NYCE, 2004 Advanced Financial Solutions, Inc., 2004	Metavante Kirchman Bankway
\$662MM			
<b>BISYS (fiscal year-ending June 30, 2004)</b>			
\$562MM	<ul style="list-style-type: none"> <li>Investment services</li> <li>Insurance and education services</li> <li>Information services</li> </ul>	Capital Synergies Inc., 2003 First Northern Financial Resources, 2002 Harrison James Group, 2002 Boston Institutional Group, 2001 Automatic Data Processing (ADP), 1989	TotalCS (TCBS) TotalPlus
\$255MM			
\$220MM			
<b>Jack Henry and Associates (fiscal year-ending June 30, 2004)</b>			
\$382MM	<ul style="list-style-type: none"> <li>Bank systems and services</li> <li>Credit union systems and services</li> </ul>	Credit Union Solutions, Inc., 2003 BankData Systems, 2000 Symitar Systems, Inc., 2000 BancTec, 1999	Banker II CIF 20/20 Core Director Liberty Silverlake System
\$85MM			

Sources: Company web sites, annual reports for periods indicated

## Regional Service Providers

Every region is served by several independent and bank-affiliated technology service providers that compete with the national firms. Several of the regional technology service providers are owned by one or more banks or bank holding companies. Examples of bank-owned service providers are Data Center Inc. (DCI), Hutchinson, Kan., and McCoy Myers, Amarillo, Texas. Most of these vendors provide services to a limited regional or multi-state area. In recent years, many of the regional companies have been targets of mergers and acquisitions and have become divisions of the large information technology firms. Others have expanded through acquisitions or have been involved in peer-to-peer mergers.<sup>10</sup> Table 2 provides information on significant regional service providers.

## Software Companies

Fiserv, Metavante, Jack Henry, Fidelity National Financial, and BISYS have acquired many of the largest core processing software companies in recent years. Prominent software companies that have been acquisition targets include ALLTEL (2003), Aurum Technologies

(2004), Sanchez Computer Associates (2004), Kirchman Corporation (2004), InterCept (2004), Precision Computer Systems (2003), and Information Technology, Inc. (1995). Although the field of independent core processing software companies is narrowing, there continue to be several well-known independents. The independent software providers are listed in Table 3. These companies offer ancillary software products that are integrated with their core processing software or build systems to accommodate integration with software products purchased from other vendors. While these companies generally concentrate on in-house software solutions, some also offer offsite data processing.

## TECHNOLOGY OUTSOURCING IN COMMUNITY BANKS

For the majority of community banks, and many regional banks, software and services provided by third-party vendors form the backbone of the automation used in core processing. Community banks tend to rely on third-

Table 2

### Regional Bank Service Corporations and Independent Data Processors

Company Name	Services
BMA Management Support Corp. Salt Lake City, Utah	Markets its BankRite core processing software for in-house or service bureau outsourcing use.
Computer Services Inc., (CSI) Paducah, Ky.	Provides core processing to banks in 18 states. Significant outsourced core processing provider in Illinois, Indiana, Kentucky, Nebraska, and West Virginia.
COCC Avon, Conn.	Remarkets Open Solutions' TCBS software to banks in the Northeast and Mid-Atlantic.
Data Center Inc., (DCI) Hutchinson, Kan.	Provides data processing to banks in the Midwest and Southwest with processing sites in nine states.
Intrieve Inc. Cincinnati, Ohio	Provides core and item processing, electronic banking products to financial institutions in the Midwest.
I-Tech Corporation Billings, Mont.	I-Tech provides core processing for banks in the Northwest using ITI Premier software.
McCoy Myers Amarillo, Texas	Markets its own Meridian software to banks in the Southwest, predominantly Texas.
Rurbanc Data Services, Inc. (RDSI) Defiance, Ohio	Remarkets ITI Premier software to banks in the Midwest.

Sources: Company web sites and news releases

Table 3

### Independent Core Processing Software Providers

Company Name	Services
Open Solutions Glastonbury, Conn.	Software (The Complete Banking Solution—TCBS) is offered as an in-house/turnkey solution or outsourced through Open Solutions' service bureaus or its partners, BISYS and COCC.
Harland Financial Solutions Atlanta, Ga.	Harland acquired Concentrix in 2000. Harland now offers core processing software to banks and credit unions under the names of SPARAK, BankServ, CuServ, and ULTRADATA.
Nicola Banking Systems Chickasha, Okla.	Nicola markets its own core processing software as well as ancillary products for in-house use.
Modern Banking Systems Ralston, Neb.	Interstate Business Equipment markets the Modern Banking Systems software for in-house core processing.

Sources: Company web sites and news releases

party vendors because they often lack the resources required to support an internal team of technology experts to develop and customize software and hardware systems. This mode of operation is not likely to change. As the technology used by financial institutions has become more complex, and management of the risks has become more challenging, meeting technology requirements with internal resources has become less practical for community banks, and they are likely to continue to rely on external technology service providers.

Community banks generally either outsource processing or process in-house using a server-based or a turnkey processing system. Outsourcing involves transmitting data pertaining to transactions that occur during the day for processing to an offsite service center operated by a vendor using either a batch or an online entry process. Larger banks using an in-house core processing system may use vendor software but often use internal resources to design and configure the system. What factors influence a community bank's choice between in-house processing versus outsourced processing? What factors influence whether a community bank purchases technology services from a national, regional, or specialized service provider? This section discusses several factors that may have some bearing on the decision-making process.

### In-House/Turnkey and Outsourced Processing

Among community banks utilizing technology service providers, there is no clear cut preference between the turnkey processing option and outsourcing to an offsite service center. The 2004 Survey of Community Banks in the Tenth Federal Reserve District asked community banks to identify the technology service provider they use for a variety of bank processes.<sup>11</sup> Of those responding, 46 percent said their deposit and general ledger processing is done in-house with vendor-provided software, compared with 54 percent whose deposit and general ledger processing is outsourced (see Table 4). State member bank examination data support this finding. According to the most recent examination data for 174 state member banks in the Tenth District, the split between in-house and outsourced core processing is fairly even.

Table 4

### Percent of Banks Choosing In-House/Turnkey or Outsourced Core Processing

	Choices for Core Processing	
	In-house/Turnkey (Percent)	Outsourced (Percent)
2004 Tenth District Community Bank Survey	46	54
Tenth District State Member Bank Examination Data	49	51

A variety of factors may influence the method of bank technology processing that is chosen by each individual bank. An analysis of Tenth District community banks seems to indicate that smaller community banks favor in-house turnkey processing systems as opposed to outsourced processing systems. The average asset size of 86 state member banks in the Tenth District that utilize in-house turnkey systems is \$109 million, compared with the average asset size of \$160 million for 87 state member banks that outsource their core processing. One reason small banks may choose in-house turnkey processing is the ability to purchase a processing system at a fixed cost that can be spread out over an extended period.

### **Technology Service Provider Alternatives**

The characteristics of each individual bank may also influence its choice of technology service provider. One of the factors that could influence this choice is whether the technology service provider's business continuity and information security policies mesh with those of the financial institution. In addition, community banks may consider whether the technology services they require are available from a single source. Many of the regional service providers offer ancillary products related to Internet banking, item processing, document imaging, and other banking products. The largest technology service provider companies tend to offer not only bank core processing solutions and ancillary products but also products related to insurance, trust, disaster recovery, and investment services. Based on information from the 2004 Survey of Community Banks in the Tenth Federal Reserve District, most of the national service providers, along with several regional processors and software companies, serve community banks in the region.

## **MANAGING TECHNOLOGY OUTSOURCING RISK**

As outsourcing relationships have become more pervasive, management of outsourced technology relationships has received heightened attention within the financial services industry and from regulators. Management of risks in outsourcing relationships is based on the premise that outsourcing business processes does not transfer responsibility for addressing the risks associated with the activities or the technology that is used in the processes. The transfer of day-to-day control over outsourced processes to a third-party vendor means that operational risks will be realized in a different manner than if the activities were performed in-house.

The inherent risks of technology applications in financial institutions have always required rigorous controls to address risks related to the security, availability and integrity of technology systems and resources, and customer privacy. Outsourcing complicates management and control of these risks because the bank is separated from the day-to-day management and physical control over the processes. Even so, financial institutions must craft an outsourcing framework that incorporates mechanisms to permit them to monitor and control risks related to the outsourced processes. The federal regulatory agencies,<sup>12</sup> individually and through the FFIEC,<sup>13</sup> have issued guidance that identifies key risk management and examination considerations for control of risks associated with outsourcing.

The FFIEC guidance addresses four key elements that should be incorporated in a risk management framework for technology outsourcing:

- Risk Assessment
- Service Provider Selection
- Contract Provisions and Review
- Ongoing Service Provider Monitoring

Financial institutions should assess the risk associated with specific technology service providers

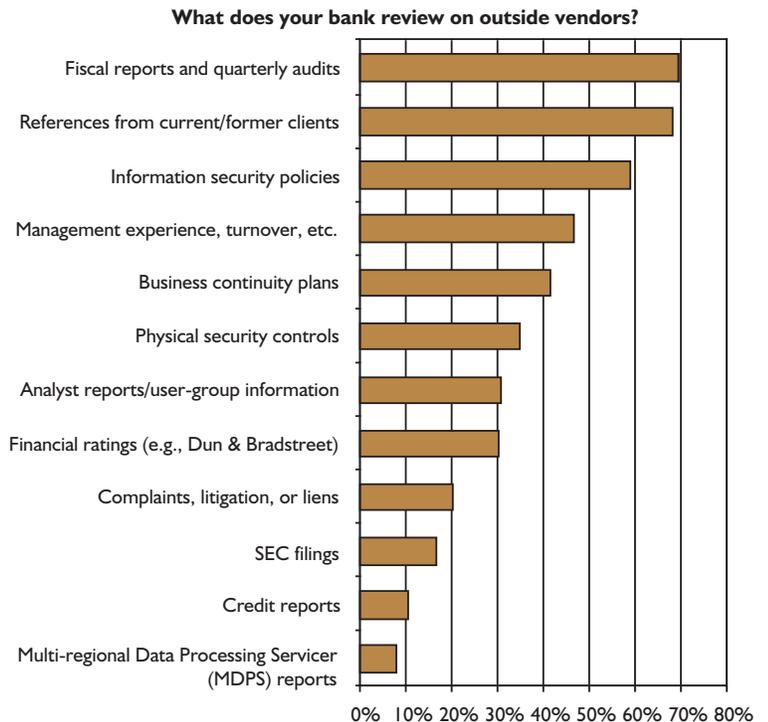
and services. These risks can include operations risk related to a technology service provider's poor performance and the associated impact on the bank's reputation, competitiveness, financial soundness, or ability to comply with regulatory requirements. The risk assessment should also identify the necessary controls for managing outsourcing relationships.

The selection of a technology service provider that supports the institution's overall requirements and foreseeable needs over a multi-year period is the first step toward addressing the financial and operational risks involved in outsourcing. During the time that an outsourcing arrangement is likely to be in place, important changes can occur that may affect the suitability of the technology chosen or the viability of the service provider. Evaluating technologies and service providers is complicated by the rapid changes taking place in the economics of the industry. Among these changes are the industry consolidation and realignment and emerging developments previously discussed.

Financial institutions should also consider whether the provider's proposals meet the needs of the institution in the near term as well as the future strategic direction of the bank. The due diligence process should include an evaluation of the contract provisions, including service-level agreements and monitoring tools. Once an outsourcing arrangement has been established, the financial institution must be able to monitor each service provider's controls, condition and performance, and have the ability to take steps necessary to correct any deficiencies that may arise. In addition, banks should determine whether the information security, business continuity, and customer information security policies of their vendors meet the expectations of the bank. Additional information regarding business continuity planning, standards for protecting customer information and information security is provided in Box A—References for Managing Technology Risk. Financial institutions should consider each of these issues in relation to the use of technology service providers.

Chart 1

### Community Bank Oversight of Technology Service Providers



The 2004 Survey of Community Banks in the Tenth Federal Reserve District asked respondents to identify their actions taken to review outside vendors. Chart 1 above shows the responses to these questions. Most frequently, respondents review financial reports and audits, references, and information security policies.

Business continuity plans, information security policies, and independent audits<sup>14</sup> of technology service providers are important sources of information that should be used as part of an ongoing monitoring program. High percentages of survey respondents indicated they address these areas with vendors. Nearly 60 percent of survey respondents indicated that they review vendors' information security policies, and 40 percent of respondents said that they review the business continuity plans of their outside vendors. The importance of these risks is highlighted by recent

events and escalating concerns about issues pertaining to business continuity and identity theft. In response, regulators have increased scrutiny of business continuity planning and customer information security policies and procedures.

Oversight and monitoring of technology service providers is also supported by the regulatory examination reports that are available to the provider's customers. An overview of the information technology examination program and rating system for both banks and technology service providers is provided in Box B—Information Technology Examination Programs. Although the banking agencies do not have licensing authority over technology service providers to the banking industry, the services provided by significant vendors are subject to regular examination and regulation by the bank supervisory agencies. Under the Bank Service Corporation Act, the federal financial regulatory agencies are empowered to examine companies that provide services to financial institutions for which they have oversight responsibility.<sup>15</sup> Approximately 150 third-party technology service providers are included in the examination and supervision programs of the federal banking agencies. The goal of the examination program is to identify risks associated with technology vendors that could adversely affect serviced institutions. Examiners evaluate the effectiveness of controls over data integrity, information security and confidentiality, service availability, and financial stability of the service provider. Copies of the examination reports are made available to each service provider's bank and thrift clients by their regulatory agency.

## CONCLUSION

Many community banks rely on third-party service providers to meet their processing needs—either through outsourcing or by purchasing turnkey systems. Third-party service providers can help financial institutions control overhead and promote efficiency by providing access to advanced technologies not available in-house while

permitting the institution to focus on its core business. As the information technology industry has matured, virtually the entire financial services industry has implemented automated processes to perform core processing functions as well as a host of ancillary tasks. Even though many processes are well-established, technologies and business processes continue to evolve as new ways are developed to process and deliver financial services.

Managing relationships with technology service providers remains a challenge even for the most sophisticated institutions. The technology service provider industry is undergoing rapid change, including industry consolidation and realignment. Consolidation is changing the line-up of vendors serving the market and the ongoing viability of processing systems, some of which may be discontinued or combined with other systems as a result of mergers and acquisitions between vendors. Given the reliance of banks on technology service providers, financial institutions should monitor and evaluate the potential impact of these changes on their vendor relationships.

As the community bank survey responses indicate, the primary focus of third-party vendor management for many banks has been to ensure that the vendor is in stable financial condition and will provide a viable product that is available with minimal down time. Recent events have highlighted the importance of risk management practices addressing business continuity and the security of customer information. As the industry has evolved, so have standards and practices for technology risk management. One key to effective technology risk management is to have a structured outsourcing management process that addresses the full range of risks associated with the outsourced tasks. The fundamental elements that comprise effective controls over technology outsourcing have become relatively standardized and are incorporated in regulatory guidance. Financial institutions of all sizes can benefit by measuring their internal processes against these established standards.

## References for Managing Technology Risk

### Business Continuity Planning

A number of events, including attacks against the U.S. financial system, power outages, and hurricanes, validate the importance of business continuity planning. In March 2003, the Federal Financial Institutions Examination Council (FFIEC) published its updated Business Continuity Planning handbook ([http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus\\_continuity\\_plan.pdf](http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf)). The regulators stress that planning for business continuity should not be confined to resumption of the technology function, but resumption of critical business processes on an enterprise-wide basis. Financial institutions should consider the interdependencies that exist between themselves and service providers. Service providers in this context include not only the vendors that provide technology processing, but also telecommunications and power providers. (The Financial Services Roundtable and BITS recently published the “BITS Guide to Business-Critical Telecommunications Services,” November 2004). Examiners will evaluate whether the institution’s business continuity plan addresses critical outsourced services and how its technology service providers’ business continuity plans are incorporated into those of the financial institution.

### Customer Information Security Guidelines—Protecting Customer Information

In 2001, the federal bank regulatory agencies issued guidance regarding the protection of customer information. (Interagency Guidelines Establishing Standards for Safeguarding Customer Information and

Rescission of Year 2000 Standards for Safety and Soundness, 12 CFR part 208, app. D-2, and part 225, app. F; Final Rule). The Standards for Safeguarding Customer Information require financial institutions to: develop a written information security program; perform a risk assessment of information security threats and the effectiveness of institutional policies to control risk; complete an annual report on the bank’s compliance with these guidelines to the board of directors; and exercise appropriate due diligence in selecting service providers including ensuring that contracts require the service provider to implement appropriate measures to protect customer information. Financial institutions should monitor, evaluate, and adjust their information security program in response to a number of factors, including the changing business environment and outsourcing arrangements.

### Information Security

The federal regulatory agencies outlined their expectations regarding an effective process for securing customer information in the above noted guidance. The FFIEC Information Security Handbook provides additional recommendations regarding processes related to: conducting a risk assessment, developing an information security strategy, implementing security controls and security testing programs, and developing monitoring programs ([http://www.ffiec.gov/ffiecinfobase/html\\_pages/it\\_01.html#infosec](http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec)). As noted earlier, outsourcing of information technology processes introduces an added level of risk that must be taken into account when developing, implementing, and managing an information security program.

## Box B

### Information Technology Examination Programs

The federal bank and thrift examination agencies assess information technology risks for financial institutions through examinations of bank IT functions. Examination ratings follow the Uniform Rating System for Information Technology (URSIT) system, which was originally adopted in 1978 and revised in 1999.<sup>16</sup> The rating framework is based on the CoBIT<sup>17</sup> model and includes four IT risk management components (the “AMDS components”). The four components are: (1) audit, (2) management, (3) development and acquisition, and (4) support and delivery. The table below provides a summary of the factors used for each element in the URSIT system.

Examination priorities and scheduling for technology service provider reviews are based on a variety of factors.

To determine examination priorities, each vendor is assigned a risk category based on a number of factors, including: type of service provided (business line risk); size of client base; prior examination results; quality of oversight, including audit reviews; whether technology used is new and untested or stable; and reported problems by clients. A technology service provider with a large client base or providing a critical service<sup>18</sup> or that presents other risk factors will be assigned an “A” priority in the program. “A” priority service providers are examined on a 24-month cycle. Average risk or “B” priority service providers are examined at least every 36 months, and low risk or “C” priority service providers are examined infrequently.

### Description of URSIT Rating System Component Rating Factors

#### URSIT Components

Excerpted from FFIEC Uniform Rating System for Information Technology, January 13, 1999.

Component Category	Rating	Rating Factors
<b>Audit</b>	1 to 5	Audit function assessment of exposure to risks and quality of internal controls associated with acquisition, implementation, and use of IT. Audit practices should address IT risk exposures throughout the institution and its service providers. Audit independence, level of oversight by board and management, adequacy of audit methodology and scope, follow-up, and reporting.
<b>Management</b>	1 to 5	Management effectiveness in addressing IT risks related to strategic planning, quality assurance, project management, risk assessment, infrastructure, third-party vendor contracts, regulatory and legal compliance.
<b>Development and Acquisition</b>	1 to 5	Management’s ability to identify, acquire, install, and maintain appropriate information technology, including software and hardware solutions that meet the needs of the organization. Management should have in place effective business processes for implementing any kind of change to hardware or software used, including purchase of hardware or software, development or programming, or purchases from vendors.
<b>Support and Delivery</b>	1 to 5	Addresses the ability of the organization to provide technology services in a secure environment and includes such factors as the condition of IT operations and their reliability, security, and integrity, which could affect quality of the information delivery system. Practices should ensure the continuity of operations and the reliability and availability of data. The scope of the rating extends to operational risks throughout the organization and service providers.
<b>Composite</b>	1 to 5	The composite risk rating is derived by making a qualitative summarization of the four component ratings.

## ENDNOTES

- <sup>1</sup> Core processing refers to the processing of deposit and loan data, customer information files, and general ledger processing.
- <sup>2</sup> The FFIEC is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The participating agencies identify technology service providers as part of the examination process.
- <sup>3</sup> See Bertil E. Chappuis, Kevin A. Frick, and Paul J. Roche, “High-Tech Mergers Take Shape,” *The McKinsey Quarterly*, 2004, number 1.
- <sup>4</sup> See Wade Will, “Processors Consolidate: 3 Vendors Snap up 4,” *American Banker*, April 22, 2004.
- <sup>5</sup> The recent merger of J.P. Morgan Chase and Bank One is an example of a merger with repercussions for technology service providers. In December 2002, J.P. Morgan Chase had announced a seven-year \$5 billion outsourcing agreement with IBM, which was described as one of the largest technology outsourcing contracts (in any industry) on record. As a result of the merger, the IBM outsourcing contract was cancelled, as the combined entity is converting to the in-house approach favored by Bank One and most other large (Top 50) banking organizations. (See Gretchen Morgensen, “I.B.M. Shrugs Off Loss of a Service Contract It Once Flaunted,” *The New York Times*, September 16, 2004.) BISYS, a specialized financial services technology company, is also losing business as a result of the merger. BISYS was the servicer for the large mutual funds managed by both J.P. Morgan and Bank One. The merged entity decided that the combined processing of both banks’ mutual funds is on a scale that will be cost effective to bring in-house.
- <sup>6</sup> Server-based and turnkey systems are systems and hardware set up to perform core processing for banks on an in-house basis. The term “turnkey” refers to the fact that these systems generally require minimal programming or setup by the technical staff for the customer.
- <sup>7</sup> Metavante is a subsidiary of Marshall & Ilsley Corporation, Milwaukee, Wis.
- <sup>8</sup> For a further discussion of trends in the payments processing industry, see Richard J. Sullivan, “The Supervisory Framework Surrounding Nonbank Participation in the U.S. Retail Payments System: An Overview,” working paper, Payments System Research Department, Federal Reserve Bank of Kansas City, 2004, <http://www.kansascityfed.org/FRFS/PSR/home.htm>.
- <sup>9</sup> Steven Bills, “One Deal On, One Deal Off; Fidelity National to Buy InterCept, Delay Spinoff,” *American Banker*, September 10, 2004.
- <sup>10</sup> For example, CSI of Paducah, Kentucky, recently acquired two data processing companies, expanding its market to 10 additional states and 300 additional bank customers.
- <sup>11</sup> The 2004 Community Bank Survey, as described in “The 2004 Survey of Community Banks in the Tenth District” was distributed in February 2004 to all commercial banks in the Tenth Federal Reserve District with year-end 2003 assets less than \$1 billion, approximately 1,300 banks. We received 341 responses to the survey, equaling a response rate of 27 percent.
- <sup>12</sup> Board of Governors of the Federal Reserve System, Supervision and Regulation Letter SR 00-4, “Outsourcing of Information and Transaction Processing,” February 29, 2000, <http://www.federalreserve.gov/boarddocs/SRLETTERS/2000/SR0004.HTM>.
- <sup>13</sup> Federal Financial Institutions Examination Council, “Outsourcing Technology Services,” FFIEC IT Examination Handbook, June 2004, <http://www.ffiec.gov/ffiecinfobase/index.html>.
- <sup>14</sup> In addition to standard financial statement audits, audits designed specifically to look at controls and processes of service providers are generally available. Statement of Auditing Standards (SAS) number 70, “Service Organizations,” sets forth standards for independent audit reviews over a service provider’s processes and controls. Most technology service providers make SAS 70 reviews available to client institutions.
- <sup>15</sup> 12 USC 1867 (c) (1) and 12 USC 1464 (d) (7).
- <sup>16</sup> “Supervision of Technology Service Providers,” *FFIEC IT Examination Handbook*, March 2003.
- <sup>17</sup> The Information Systems Audit and Control Association (ISACA), organized in 1969, developed information systems audit and control standards including a framework of “Control Objectives for Information Technology” (the “CoBIT” framework).
- <sup>18</sup> Critical services include: asset management processing, clearing and settlement services, core bank processing, corporate electronic banking/cash management, disaster recovery services, and wholesale payment.