Cross-border outsourcing and risk management for banks[1]

Hugh C. Kelly
Senior Advisor for Global Banking,
Office of the Comptroller of the Currency

Daniel E. Nolle
Senior Financial Economist,
Office of the Comptroller of the Currency

Abstract

U.S. banks are increasingly outsourcing an expanding range of their operations to third-party service providers. Recent industry estimates show that outsourcing by U.S. banks accounts for almost 20 percent of their information technology services spending. Importantly, the prospect of considerable cost savings and access to scarce information processing and development resources has led a growing number of banks to consider making greater use of foreign-based service providers – that is, of engaging in 'cross-border outsourcing'. Notwithstanding the potential cost savings that can result from outsourcing offshore, banks face significant risk management challenges from these activities. Some of these challenges are unique to cross-border outsourcing while others, associated with risk management for domestic service providers, may take on added significance for cross-border outsourcing.

Managing the risks associated with cross-border outsourcing is extremely important, especially in the case of the banking industry where problems can take on systemic significance and can affect confidential customer or bank records. In consequence, the Office of the Comptroller of the Currency has published risk management guidelines for banks engaging in cross-border outsourcing. This article summarizes that guidance, placing the discussion in the context of the recent rapid growth in outsourcing. Among the most important risk management challenges to assess and address are: 1) the strategic fit that cross-border outsourcing will provide for a bank's overall operations; 2) country risk, which includes social, economic, and political instability; 3) legal and compliance risks related to the potential applicability of foreign jurisdictional laws to the outsourced activities; and 4) operational risks related to security and confidentiality of bank and customer information.

1 The opinions expressed in this article are those of the authors alone, and do not necessarily represent those of the Office of the Comptroller of the Currency or the U.S. Treasury Department. The authors thank Jim Devlin, Jeff Gillespie, Virginia Hagan, Carter Messick, Nancy Wentzler, and Cliff Wilke for insightful comments.

Cross-border outsourcing and risk management for banks

U.S. banks are increasingly outsourcing an expanding range of their operations to third-party service providers. Recent industry estimates show that outsourcing by U.S. banks accounts for almost 20 percent of their information technology services spending, while industry projections estimate nearly a 40 percent increase in such outsourcing by 2005. Importantly, the prospect of considerable cost savings and access to scarce information processing and development resources has led a growing number of banks to consider making greater use of foreign-based service providers – that is, of engaging in 'cross-border outsourcing'.

Notwithstanding the potential cost savings that can result from outsourcing offshore, banks face significant risk management challenges from these activities. Some of these challenges are unique to cross-border outsourcing while others, associated with risk management for domestic service providers, may take on added significance for cross-border outsourcing. Among the most important risk management challenges are the following:

- Assessing the strategic fit that cross-border outsourcing will provide for a bank's overall operations, a process which includes conducting appropriate due diligence and risk assessment before deciding to contract with an overseas service provider.
- Assessing country risk, which includes social, economic, and political instability.
- Assessing legal and compliance risks related to the potential applicability of foreign jurisdictional laws to the outsourced activities.
- Assessing operational risks related to security and confidentiality of bank and customer information.
- Monitoring and oversight of vendor performance.

In addition, particularly since September 11th, the increased threat of terrorism has heightened the importance of ensuring that business continuity planning and disaster recovery capabilities are addressed during the outsourcing agreement, with an eye toward the possibility that the need for an unplanned termination of the agreement could arise.

Bulletin 2002-16, published by the Office of the Comptroller of the Currency (OCC) in May 2002, provides specific risk management guidelines for national banks engaging in cross-border outsourcing.[2] This article summarizes that guidance, placing the discussion in the context of the recent rapid growth in outsourcing.

The article is organized as follows. The next section sketches the magnitude and recent growth of outsourcing of information services, focusing in particular on cross-border outsourcing. This look at the outsourcing 'landscape' includes a brief discussion of the characteristics of cross-border outsourcing that have made it an increasingly attractive alternative for a growing number of firms, including in particular financial services firms. The following section begins with the observation that along with the benefits come risks. Managing the risks associated with cross-border outsourcing is extremely important, especially in the case of the banking industry where problems can take on systemic significance and can affect confidential customer or bank records. In consequence, the final section summarizes recent risk management guidance issued by the OCC for national banks to apply to their cross-border outsourcing plans and activities.

Cross-border outsourcing landscape

Outsourcing of information-related services is not new. Indeed, many industries have been outsourcing some or much of their information technology (IT) services – e.g. customer software development, application maintenance, and IT package implementation – since at least the start of the technology boom of the 1990s.[3] Nor is the use of foreign-based third party vendors new. However, outsourcing - including cross-border outsourcing - has seen significant growth recently, as firms facing stiffer competition in an increasingly globalized economy look to control costs and obtain expertise. The nature of IT services that are being outsourced has also changed recently, as firms have increased their outsourcing of IT 'business processes' – e.g., loan and deposit processing, payroll processing, mortgage servicing, and customer interaction services such as call centers. Some of these business processes are

2 The Office of the Comptroller of the Currency charters, regulates, and examines national banks.

3 PwC Consulting, 'Riding the Offshoring Wave,' PricewaterhouseCoopers (2002).

regarded as higher value-added 'strategic' activities as compared to traditionally outsourced 'commoditized' services.[4]

In addition, while historically financial services outsourcing was generally limited to a single service provider for a given functionality, in recent years banks' outsourcing relationships have increased in scale and complexity as a direct result of advances in information technology and the emergence of electronic banking. Many outsourced services, particularly in the area of electronic banking, are 'sub-contracted' to additional third party service providers and/or conducted in a foreign country. Further, as electronic banking services have become more technologically advanced and have grown in strategic importance, certain online functional applications, such as electronic bill presentment/payment and account aggregation services, are dependent on a small number of specialized third-party vendors and service providers.[5]

Outsourcing

To illustrate both the extent and growth of IT and business processes outsourcing, Table 1 compares estimates and projections from several recent studies for the U.S. and worldwide. The top half of the table compares estimates of the current or recent levels of outsourcing (domestic and foreign-based). The bottom half shows growth projections for outsourcing. For example, an International Data Corporation (IDC) study estimated that IT outsourcing by U.S. firms in 2001 was U.S.$29.04 billion, with the banking industry's U.S.$5.7 billion accounting for 20 percent of that amount - the largest single industry share. Further, the U.S.$5.7 billion spent by U.S. banks in 2001 on outsourcing represents 19 percent of U.S. banks' total IT spending.[6] TowerGroup has estimated worldwide IT outsourcing for 2003 at U.S.$120 billion, a figure that accounts for over one-third of the estimated U.S.$340 billion in total IT spending worldwide.[7] Further, Gartner estimated a similar level of outsourcing worldwide for business processes, at U.S.$123.6 billion in 2001.

The studies are in rough agreement about likely substantial growth in outsourcing. Gartner projects a 44 percent increase in business processes outsourcing between 2001 and 2005. IDC's and TowerGroup's projections for the growth of IT outsourcing by U.S. firms over the 2001-2005 period are similar, with the former projecting a 53 percent increase and the latter a 61 percent increase. IDC also expects rapid growth for IT outsourcing by U.S. banks from 2001 through 2005.

Cross-border outsourcing

Clearly, outsourcing of information services is substantial and set to expand greatly. What about an important subset of outsourcing – outsourcing to foreign-based vendors? While data is currently hard to come by, Table 2 gives some idea of the fact that cross-border outsourcing has become quite substantial. The data are from a PriceWaterhouseCoopers study that approaches the subject via the phenomenon of 'offshoring.'[8] Offshoring includes both the use of foreign-based facilities owned by a firm for production processes formerly done 'onshore' in the home country (i.e., production that is not outsourced),[9] as well as the use of foreign-based third-party vendors – i.e., cross-border outsourcing.

4 See, e.g., Schroeder, Michael, 'More Financial Jobs Go Offshore,' The Wall Street Journal (May 1, 2003); PwC Consulting, 'Riding the Offshoring Wave,' PricewaterhouseCoopers (2002); 'Back office to the world' (May 3, 2001), The Economist.

5 Electronic Banking Group, Basel Committee on Banking Supervision, 'Risk Management Principles for Electronic Banking' (May 2001).

6 Celent Communications estimates that U.S. banks spent $32.8 billion on IT in 2001, and TowerGroup estimates IT spending by banks was $26.5 billion. The average of these two estimates is $29.7 billion; $5.7 billion is 19.2 percent of this (average) total IT spending by U.S. banks. For the Celent and TowerGroup estimates of IT spending totals see Rountree, David, 'Technology Spending Persists in Downturn,' Bank Technology News, Vol. 15, No. 3 (March 2002).

7 Sisk, M., 'Outsourcing Goes On-Demand,' Bank Technology News, Vol. 16, No. 2 (February 2003).

8 PwC Consulting, 'Riding the Offshoring Wave,' Price Waterhouse and Coopers (2002). This approach is typical of recent accounts in the press and in industry studies that focus initially on the location of production, and subsequently distinguish between 'captive' foreign-based production facilities owned by firms, and the use of foreign-based vendors. See also PwC Consulting, 'Offshore Resourcing: Once Adventurous, Now Essential for Financial Services Firms,' PricewaterhouseCoopers (2002); 'The Rush to Send Back-Office Business Overseas,' http://knowledge.wharton.upenn.edu; and 'Raising the Bar On Offshore IT for Insurance,' Celent Communications press release, May 23 2003.

9 Some industry observers have begun to refer to this aspect of offshoring as 'insourcing.' See for example Patel, Divya Verma, 'Banks benefit from insourcing,' The Asian Banker, June 19, 2003.

TABLE 1. LEVEL AND GROWTH OF INFORMATION SERVICES OUTSOURCING
(estimates and projections)

Study	Time Period	Region	Outsourced Operations	Estimates/ Projections
Level of Outsourcing				
International Data Corporation (IDC)[1]	2001	United States	Information Technology (IT) – All industries	$29.04b
IDC[1]	2001	United States	IT - Banking	$5.70b
IDC[1]	2005	United States	IT – All industries	$44.34b
IDC[1]	2005	United States	IT - Banking	$8.83b
TowerGroup[2]	2003	Worldwide	IT – All industries	$120.00b
Gartner[3]	2001	Worldwide	Business processes – All industries	$123.60b
Gartner[3]	2005	Worldwide	Business processes – All industries	$178.50b
Growth of Outsourcing				
Gartner[3]	2001-2005	Worldwide	Business processes – All industries	44% increase in business processes outsourcing
IDC[1]	2001-2005	United States	IT - All industries	53% increase in IT outsourcing
TowerGroup[3]	2001-2005	United States	IT – All industries	61% increase in IT outsourcing
IDC[1]	2001-2005	United States	IT - Banking	39% increase in banking IT outsourcing

Sources: Office of the Comptroller of the Currency using various industry sources, as follows:
1 Hallerman, D., 2002, 'Bank IT Outsourcing: A Trend without a Direction,' eMarketer.com, October 8
2 Sisk, M., 2002, 'Outsourcing Goes On-Demand,' Bank Technology News, 16:2
3 Rountree, D., 2002, 'Technology Spending Persists in Downturn,' Bank Technology News, 15:3

As illustrated in Table 2, the majority of the 51 large North American and European firms (the majority of which are financial services companies) surveyed by PwC have moved some of their IT (69%) and business processes (56%) activities to foreign locations. Consistent with recent accounts of offshoring, India dominates as the foreign location of choice, primarily because of its relatively large pool of well-educated, English-speaking workers.[10, 11] For the clear majority of companies 'offshoring' some of their production, 87 percent, have done so by using foreign-based service providers for IT activities. In addition, the majority of the companies offshoring their business processes do so via cross-border outsourcing. Finally, on average, companies engaged in cross-border outsourcing use more than one vendor, both for IT and business processes activities; the maximum number of foreign-based vendors used by a company is 10 for IT activities and 5 for business processes activities.

10 See also, e.g., Schroeder, M., 2003, 'More Financial Jobs Go Offshore,' The Wall Street Journal, May 1; and The Economist, 'Back office to the world' (May 3, 2001).

11 Note that the flow of outsourcing is not exclusively from developed countries to developing countries. For example, recently the Bank of New York announced it will provide third-party settlement services to Banco do Brazil, and EDS (a U.S.-headquartered vendor) recently signed a six-year IT outsourcing deal with Banque Hervet, a French subsidiary of HSBC Holdings. See, respectively, The Asian Banker, 'Banco do Brazil signs CLS deal have done so by using foreign-based service providers for IT activities. In addition, the majority of the companies offshoring their business processes do so via cross-border outsourcing. Finally, on average, companies engaged in cross-border outsourcing use more than one vendor, both for IT and business processes activities; the maximum number of foreign-based vendors used by a company is 10 for IT activities and 5 for business processes activities.

TABLE 2. 'OFFSHORING' AND CROSS-BORDER OUTSOURCING OF INFORMATION TECHNOLOGY AND BUSINESS PROCESSES

Characteristic	Operations	
	Information Technology	Business Processes
Offshoring: Percent of 51 large companies locating significant operations offshore	69%	56%
Location: Offshoring companies locating operations in:		
■ India	86%	57%
■ Philippines	7%	17%
■ Ireland	5%	16%
■ Other	2%	10%
Cross-Border Outsourcing: Offshoring companies using foreign-based 3rd party vendors	87%	51%
Average number of cross-border vendors per company	3	2
Maximum number of cross-border vendors by a single company	10	5

Memorandum: Total U.S. financial services jobs moving to offshore outsourcing (2003-2008) projected at 500,000 (8% of industry total) by A.T. Kearney.
Source: Office of the Comptroller of the Currency using information from 'Riding the Offshoring Wave,' PwC Consulting, PriceWaterhouseCoopers (2002), and Schroeder, M., 2003, 'More Financial Jobs Go Offshore,' The Wall Street Journal, May 1

Notes:
- Fifty-one companies (43 North American, 8 European) with offshore outsourcing experience surveyed by PwC Consulting.
- Twenty-three of the surveyed companies were financial services firms.
- 'Offshoring' refers to the practice of a company moving work from its home country to a foreign location, either by establishing its own operations or by outsourcing.
- Outsourcing refers to the use of 3rd party vendors for the provision of work formerly done by the company itself.
- Cross-border outsourcing refers to the use of a 3rd party vendor located in a foreign country.
- Business processing includes functions such as back office processing, finance and accounting work, and operation of call centers.

The degree to which companies rely on cross-border outsourcing is likely to increase because there are substantial perceived benefits. Table 3 summarizes key benefits and their estimated magnitudes. The first four rows in Table 3 focus on cost reductions from cross-border outsourcing. Relative to using U.S. vendors, the Wharton and Gartner studies estimate cross-border outsourcing cost savings of 20 to 50 percent for activities such as call center operation and loan servicing. A Celent study estimates cross-border outsourcing has resulted in cost savings of 30 percent for insurance companies, relative to retaining selected activities in-house.

TABLE 3. ESTIMATED BENEFITS OF CROSS-BORDER OUTSOURCING

Study	Benefit	Estimate
Wharton[1]	Cost reductions – business processes	20% - 40% vs. home-country (U.S.) vendors
Gartner[2]	Cost reductions - call centers	30% - 40% vs. home-country (U.S.) vendors
Wharton[3]	Cost reductions - loan servicing	20% - 50% vs. home-country (U.S.) vendors
Celent[4]	Cost reductions – IT for North American insurance companies	30% vs. in-house
Wharton[5]	Reduced worker attrition	12% - 35% in India vs. 70% - 120% in U.S.
Forrester Research[6]	Quality improvement – IT: 'Value for the money'	88% of 145 surveyed financial service firms responded that off shore vendors ranked 'somewhat better' to 'much better' than analogous U.S. vendors.
Forrester Research[6]	Quality improvement – IT: 'Quality of deliverables'	71% of 145 surveyed financial service firms responded that offshore vendors ranked 'somewhat better' to 'much better' than analogous U.S. vendors.
Forrester Research[6]	Quality improvement – IT: 'On-time delivery'	67% of 145 surveyed financial service firms responded that off shore vendors ranked 'somewhat better' to 'much better' than analogous U.S. vendors.
Forrester Research[6]	Quality improvement – IT: 'Having the right skills'	65% of 145 surveyed financial service firms responded that off shore vendors ranked 'somewhat better' to 'much better' than analogous U.S. vendors.

Sources: Office of the Comptroller of the Currency using various industry sources, as follows:

1 'The Rush to Send Back-Office Business Overseas,' http://knowledge.wharton.upenn.edu.
2 'The Case For, and Against, Shifting Back-office Operations Overseas,' http://knowledge.wharton.upenn.edu.
3 'Case Study: Inside the Progeon-Greenpoint Mortgage Transaction,' http://knowledge.wharton.upenn.edu.
4 'Raising The Bar On Offshore IT For Insurance,' Celent Communications press release (May 23, 2003).
5 'Business Processes Are Moving from the West to Other Parts of the World,' http://knowledge.wharton.upenn.edu.
6 Breitkopf, D., and Kingson J.A., 'E-Strategists Humbler, But No Less Ambitious,' American Banker (May 8, 2003).

Table 3 includes estimates of other benefits as well. Workers in many countries providing cross-border outsourcing find jobs in the outsourcing industry relatively more attractive than do U.S. workers. Hence, attrition can be substantially lower at foreign-based vendors, as indicated by the wide gap between attrition rates for Indian versus U.S. outsource workers displayed in Table 3. Furthermore, in a growing number of countries the educational and skill levels of workers employed by vendors are high compared to workers attracted to similar jobs in developed countries.[12] As a result, many companies are finding that the quality of service provided by offshore outsourcers is superior to the quality they have experienced

using home country vendors. Table 3 summarizes the results of a Forrester Research study that includes the percentage of surveyed U.S. firms responding that they perceived quality improvements in work done by offshore vendors relative to U.S.-based vendors. For example, 71 percent of the U.S. firms found the 'quality of deliverables' from foreign-based vendors to be superior to that of U.S. outsourcers.

Risk management for banks engaging in cross-border outsourcing

Use of foreign-based third-party service providers is substantial, and there is an emerging consensus that it is set to grow substantially in light of the cost and other benefits companies have reported experiencing. The story is not all one-sided of course, because the benefits are accompanied by risks that must be managed. In an effort to help banks balance their risk-reward decisions about cross-border outsourcing, the OCC recently published guidance on identifying and managing cross-border outsourcing risks. This section summarizes OCC Banking Bulletin 2002-16, Bank Use of Foreign-Based Third-Party Service Providers, issued in May 2002.[13]

In its bulletin, the OCC notes that a national bank's use of third-party service providers located outside the U.S. is generally permissible,[14] and may offer cost-effective means of processing data and transactions and of providing expertise in processing, marketing, and technology-related functions. However, it also cautions that relative to dealing with U.S.-based vendors, cross-border outsourcing can raise unique risk issues that require additional risk management oversight efforts. The bulletin places particular emphasis on the management of key aspects of strategic risk, country risk, and legal (compliance) risk. In addition, OCC Bulletin 2002-16 stresses the need for banks to establish adequate monitoring and oversight processes before entering into a contract with a foreign-based third-party service provider. Finally, the bulletin addresses the need for a national bank to establish cross-border outsourcing relationships in a way that does not diminish the ability of the OCC to access, in a timely manner, data or information needed to effectively supervise the bank's operations. OCC Bulletin 2002-16 sets forth the following risk considerations for banks contemplating cross-border outsourcing:[15]

Strategic risk

The board of directors and senior management are responsible for understanding the special risks associated with the bank's outsourcing relationships with foreign-based service providers and ensuring that effective risk management practices are in place. A first step is a risk assessment and due diligence process undertaken before a national bank enters into a contract with a foreign-based service provider.[16] The due diligence process should include an evaluation of the foreign-based service provider's ability - operationally, financially, and legally - to meet the bank's servicing needs given the foreign jurisdiction's

12 The attrition and skill-level stories are likely more complex than this 'attractiveness of outsourcing jobs' scenario implies, however. In general, the mid-to-late 1990s 'dot.com' boom opened opportunities for IT workers in the U.S. and other developed countries, many of whom moved from relatively mature IT industries – including some traditional aspects of outsourcing - to new, higher paying IT jobs. Subsequently, the 'dot.bomb' shakeout of the early twenty-first century has added to IT industry attrition rates, including once again, some outsourcing sectors. Nevertheless, the U.S. and other developed countries still offer greater mobility to IT workers than most developing countries, and hence attrition rates are bound to be different for some sectors. The authors are grateful to Carter Messick for this insight.

A labor market issue gaining increasing attention is the impact of offshoring, including cross-border outsourcing, on home country workers. For example, five states in the U.S. have pending legislation aimed at keeping jobs currently being lost to offshoring. The bills include measures blocking firms from using foreign workers on state contracts, and requiring foreign-based call center workers to identify their location to customers. See Schroeder, M., 2003, 'States Fight Exodus of Jobs,' The Wall Street Journal, June 3.

13 Bulletin 2002-16 on cross-border outsourcing supplements OCC Bulletin 2001-47, Third-Party Relationships: Risk Management Principles (November 2001). Also relevant are OCC Advisory Letter 2000–12, FFIEC Guidance on Risk Management of Outsourced Technology Services (November 2000), and OCC Bulletin 2001–8, Guidelines Establishing Standards for Safeguarding Customer Information (February 2001). The term 'foreign-based third-party service providers' refers to third parties whose servicing operations are located in a foreign country and subject to the law and jurisdiction of that country. Accordingly, this definition would not include a U.S.-based subsidiary of a foreign firm because its servicing operations are subject to U.S. laws. It would include U.S. service providers to the extent their actual servicing operations are located in or outsourced to (e.g., subcontracted to) entities domiciled in a foreign country and subject to the law and jurisdiction of that country. Also, Bulletin 2002-16 applies to international branches of U.S. national banks that use third-party providers domiciled in the same foreign country or in another foreign country.

14 Subject to economic and trade sanctions of the Office of Foreign Assets Control (OFAC) of the U.S. Treasury. The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, organizations sponsoring terrorism, and international narcotics traffickers based on U.S. foreign policy and national security goals. For more information, refer to the OFAC Website at http://www.treas.gov/ofac/

15 Note that, in a knock-on sense, failure to manage these risks can result in public recognition of substandard performance by a vendor, a possibility that raises reputational risk for a bank. The authors thank Cliff Wilke for this insight.

laws, regulatory requirements, local business practices, accounting standards, and legal environment. The due diligence should also consider the parties' respective responsibilities in the event of any regulatory changes in the U.S. or the foreign country that could impede the ability of the bank or service provider to fulfill the contract. Without an effective risk assessment process, outsourcing to foreign-based service providers may be inconsistent with the bank's strategic plans, may introduce unforeseen risks that are difficult to manage, or may be too costly.

Country risk

In outsourcing to a foreign-based service provider, a bank may be exposed to country risk, which is the possibility that economic, social, and political conditions and events in a foreign country might adversely affect the bank. Such conditions and events could prevent the foreign-based service provider from carrying out the terms of its agreement with the bank. To manage country risk, a bank must closely monitor foreign government policies and political, social, economic, and legal conditions in countries where it has a contractual relationship with a service provider. The bank's risk assessment process should take into consideration relevant country risk factors and establish sound procedures for dealing with country risk problems, including having appropriate contingency plans and exit strategies.[17]

Legal (compliance) risk

A bank's use of a foreign-based service provider must not inhibit its ability to comply with all applicable U.S. laws and regulations. These include requirements concerning accessibility and retention of records, such as the Bank Secrecy Act, the national sanctions and embargo programs of U.S. Treasury's Office of Foreign Assets Control (OFAC), and other relevant U.S. consumer protection laws and regulations. National banks that use a foreign-based service provider should consider how foreign data privacy laws or regulatory requirements may interact with U.S. privacy laws and regulations and how any possible conflicts can be managed.[18]

Three legal risk issues warrant particular attention:

- **Contracts** - Contracts between the national bank and a foreign-based service provider should take into account business requirements and key factors identified during the bank's risk assessment and due diligence processes. In particular, bank management should consider inserting contract provisions that will protect the privacy of customers and the confidentiality of bank records given U.S. law and the foreign jurisdiction's legal environment and regulatory requirements.[19] In addition, contracts with third-party service providers should contain a provision indicating the provider agrees that the services it performs for a national bank are subject to OCC examination.[20]

- **Choice of law** - Before entering into an agreement or contract with a foreign-based service provider, national banks should carefully consider which country's laws they wish to control the relationship and then insert choice of law and jurisdictional covenants that provide for resolution of all disputes between the parties under the laws of a specific jurisdiction.

  Contracts that include choice of law and jurisdictional covenants will help to ensure continuity of service, to maintain access to data, and to protect non-public customer information. Such contracts and covenants, however, can be subject to interpretation of foreign courts relying on local laws. These local laws may differ substantially from U.S. laws in how they apply and enforce choice of law covenants, what they require of banks, and how they protect bank customers. Therefore, as part of its due diligence process, before a bank enters into a proposed contract with a foreign-based service provider it should obtain a legal review from someone experienced in that country's laws regarding the enforceability of all aspects of the subject contract and any other legal ramifications.

16 OCC Bulletin 2001–47 and OCC Advisory Letter 2000–12 identify factors that banks should consider when performing due diligence on potential third-party service providers.

17 The Comptroller's Handbook 'Country Risk Management' (October 2001), and the Interagency Statement on Sound Risk Management Practices for Country Risk (March 2002) describe the elements of an effective country risk management process.

18 Banks should be aware that some foreign jurisdictions may have data privacy laws or directives that apply to information transferred from the United States to that foreign jurisdiction over the Internet or to information collected within the foreign jurisdiction using automated or other equipment in that jurisdiction.

19 OCC Bulletin 2001–47 provides additional guidance on factors that national banks should consider when entering into a binding contract.

20 12 USC 1867(c) sets forth OCC's authority to examine third-party service providers.

- **Confidentiality of information** - Bank management should ensure that any contract with a foreign-based third-party service provider prohibits the service provider from disclosing or using bank data or information for any purpose other than to carry out the contracted services. The contract should state that all information shared by the bank with the foreign-based third-party service provider, regardless of how the service provider processes, stores, copies, or otherwise reproduces it, remains solely the property of the bank. Also, any sharing of non-public customer-related information from U.S. offices with a foreign-based third-party service provider must comply with the OCC's privacy regulation, including requisite disclosures to and agreements with customers who would be affected by the bank's relationship with that provider.[21] Further, contracts between a national bank and a foreign-based service provider must include a provision requiring the service provider to implement security measures that are designed to safeguard customer information.[22]

Monitoring and oversight

As with domestic outsourcing arrangements, national banks should implement an effective oversight program to monitor the foreign-based service provider's ongoing financial condition and performance.[23] In addition, the bank must determine that the service provider maintains adequate physical and data security controls, transaction procedures, business resumption and continuity planning and testing, contingency arrangements, insurance coverage, and compliance with applicable laws and regulations.

Bank management should ensure that it has sufficient expertise to perform the oversight function. As part of this function, the bank should evaluate independent audit reports prepared by the service provider's audit staff, external audits and reviews (for example, SAS 70 reviews[24]), and internal reports provided by the bank's own auditors.[25] Banks must be aware of, and prepared to effectively deal with, obstacles that geographic distance and language and cultural differences may pose.

Access to information

Bank access to information - Critical data or other information related to services provided by a foreign-based third-party service provider to a national bank must be readily available at the bank's U.S. office(s).[26] Such information should include copies of contracts, due diligence, and oversight and audit reports. In addition, the bank should have an appropriate contingency plan to ensure continued access to critical information and service continuity and resumption in the event of unexpected disruptions or restrictions in service resulting from transaction, financial, or country risk developments.

Regulator access to information - A national bank's use of a foreign-based third-party service provider and the location of critical data and processes outside U.S. territory must not compromise the OCC's ability to examine the bank's operations. Accordingly, the OCC expects a national bank to establish such a relationship in a way that does not diminish the OCC's access to data or information needed to supervise the bank.

For this reason, a national bank should not outsource any of its information or transaction processing to third-party service providers that are located in jurisdictions where the OCC's full and complete access to data or other information may be impeded by legal, regulatory, or administrative restrictions unless copies of all critical records also are maintained at the bank's U.S. offices. Further, copies of the results of the bank's due diligence efforts and regular risk management oversight, performance and audit reports on the foreign-based third-party service provider, as well as all policies, procedures, and other

21 See OCC Bulletin OCC 2000–21, 'Privacy Rules and Regulations' (June 20, 2000); and 12 CFR Part 40, 'Privacy of Consumer Financial Information,' which was published in the Federal Register on June 1, 2000 at 65 FR 35162.

22 See section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801(b), and the 'Interagency Guidelines Establishing Standards for Safeguarding Customer Information' contained in 12 CFR Part 30, appendix B. Also note that a bank should not share any non-public OCC information, such as an examination report, with a foreign-based service provider except with express OCC approval. Such non-public OCC information remains the OCC's property, and the bank should take all required measures to protect the information's confidentiality.

23 OCC Bulletin 2001–47 and OCC Advisory Letter 2000–12 provide additional guidance regarding oversight of third-party relationships.

24 AICPA Statement of Auditing Standards 70, 'Reports of Processing of Transactions by Service Organizations,' known as SAS 70 Reports, are one form of external review. Type II SAS 70 reports review the service provider's policies and procedures and provide tests of actual controls against policies and procedures.

25 Based upon the bank's own risk assessment, the bank should monitor its service providers to confirm that they adequately safeguard bank customer information. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers. See 12 CFR 30, appendix B, III.D.3.

26 In instances where the national bank's foreign branches have outsourced local operations or services cross-border to third-party service providers domiciled in another foreign country, copies of such records can be maintained at the bank's foreign branch office.

important documentation relating to the bank's relationship with the service provider, should be maintained in English for review by examiners at the bank's office(s).

OCC supervisory approach

As outlined in Bulletin 2002-16, the OCC's supervisory approach to cross-border outsourcing emphasizes the responsibility of the serviced national bank to conduct adequate due diligence, manage risks appropriately, comply with applicable laws, and ensure access to critical information with respect to the services being provided by a foreign-based third party. Examination focus is placed on the results of the bank's due diligence, risk assessment, and ongoing oversight program as well as the internal and/or external audits arranged by the service provider or the bank. If any of these risk management processes are found deficient, then the OCC will require the bank to take the necessary steps to strengthen risk management controls or terminate the outsourcing relationship.

If circumstances warrant, the OCC may examine a national bank's outsourcing arrangement with a foreign-based service provider. If the provider is a regulated entity, then the OCC may arrange through the appropriate foreign supervisor(s) to obtain information related to the services provided to the bank and, if significant risk issues emerge, to examine those services.

Conclusion

Both outsourcing – whether to domestic vendors or foreign vendors operating in the domestic market – and cross-border outsourcing have seen significant growth recently, as firms facing stiffer competition in an increasingly globalized economy look to control costs and obtain expertise. As with outsourcing relationships with domestic third-party service providers, a national bank's board of directors and management are responsible for ensuring that the bank effectively oversees any relationships with foreign-based third-party service providers. Before a bank contracts for the services of such a provider, it should properly assess the associated risks and carry out appropriate due diligence, including careful consideration of contract matters and choice of law and forum provisions. Additionally, the bank should have sufficient policies, practices, expertise, and access to critical information to enable it to oversee the risks of the outsourcing relationship, including ensuring compliance with U.S. and foreign laws.