Technology both enables and presents risk to the financial services industry. This issue of FS Insights focuses on two current technology issues of importance to the industry.

**Reviewing Third Party Service Providers**

Motivated by such factors as the opportunity for cost reductions and economies of scale, and the desire to focus on core competencies, financial services companies of all types have been strong proponents of outsourcing. A paper issued earlier this year by the Joint Forum (which includes the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, and the International Association of Insurance Supervisors) recognizes not only the continued trend in the growth of outsourcing and offshoring (outsourcing beyond national borders) in the financial services industry, but also the increasing complexity of outsourcing arrangements whereby outsourcing services may be provided by a number of related and unrelated service providers, which may include both regulated and unregulated entities.

The offshoring phenomenon has added a new risk – country risk – to risks (e.g., strategic, compliance, operational, contractual, systemic, etc.) already associated with outsourcing. While country risk deals per se with the economic, political and social stability in a region, a broader view of country risk might also consider regulatory and business practices that may not align with those in the United States. Recently, it has been widely reported that the Office of the Comptroller of the Currency (OCC) has requested permission from the government of India to examine India-based subsidiaries of national banks that provide outsourcing services for their U.S. parent companies. This request coincides with media reports of security breaches in India including an undercover investigation by a British newspaper which suggested that an investigator was able to purchase personal information for 1,000 customers for the equivalent of five dollars. Even while Indian government approval is still pending, this development appears to be generating concern that the OCC might promulgate standards for Indian companies. The OCC is likely to contend that its actions are consistent with its mission to protect the safety and soundness of the national banking system, particularly since the OCC’s focus appears to be on subsidiaries of national banks.

The Joint Forum paper highlights the responsibilities of both regulators and financial institutions to ensure that outsourcing and offshoring arrangements are managed in a responsible way that does not leave financial institutions unduly exposed. The regulators in many developed nations have prescribed at least basic frameworks for conducting outsourcing arrangements. For U.S. financial institutions, the national approach is summarized in the chart that begins on page 2.

The key precept of effective management of third party service providers (TSPs) is that financial institutions must conduct comprehensive due diligence of their TSPs, both at inception of an outsourcing or offshoring arrangement and on an ongoing basis. The regulators, for their part, maintain the obligation to examine those TSPs that are regulated entities and, in certain cases, unregulated.

Conducting effective due diligence of a TSP may involve both off-site and on-site review.

In This Issue:

- Reviewing Third Party Service Providers
- Avoiding a Software Audit
Corporation (FDIC) provides practical advice on how both financial institutions and regulators can leverage publicly available information to aid in their reviews of TSPs. The specific information sources recommended by the FDIC include the following:

**Financial Data for Publicly Traded Companies**
- Annual reports – information about corporate strategy, potential risks, and financial condition
- SEC filings – detail on accounting methods and extraordinary events
- Mergent Online – standardized financial results from SEC filings, particularly 10-K Annual Reports and 8-K Current Reports
- Yahoo Finance – information on short interests and institutional holdings (http://finance.yahoo.com)

**Financial Analysis on Publicly Traded Companies**
- Thompson Analytics – brokerage house reports
- Moody's, Duff & Phelp's, Standard & Poor's – credit reports

Press Reports may be obtained through online searches of databases available through Factiva, American Banker, ProQuest, Business Source Elite, Lexis/Nexis, and Google. The Stanford Law School Class Action Clearinghouse provides information on class action lawsuits (http://securities.stanford.edu/info.html).

**Company Websites** often feature annual reports and press releases that provide information on acquisitions or changes in corporate structure, current management, location of headquarters and major facilities, product lines, how a company fits into the larger industry, and the results of any analyst conference calls.

**IT Consulting Firm Reports** are issued by firms such as Gartner, Tower Group, Forrester, and Celent that provide information about the current business environment and IT product quality.

These data sources, among other considerations, provide insight into changes in the TSP’s financial performance; the TSP’s strategy as reflected by such information as acquisitions and divestitures; geographic or product line expansion; or changes in management; legal or regulatory threats that may affect the TSP’s business viability; and market views on the TSP.

The FDIC uses this information to help develop its risk profile of a TSP and plan its examination strategy. Financial institutions can use the information similarly to support, in part, their risk assessments of TSPs and to determine what additional due diligence (which from the standpoint of a financial institution should always include, but not necessarily be limited to, an assessment of the TSP’s performance under the outsourcing arrangement as well as an evaluation of the TSP’s controls and regulatory compliance) is required to determine whether TSPs remain acceptable risks.

---

**United States - Securities Firms**

It is generally necessary for securities regulators not to object to the outsourcing of certain processes and procedures traditionally housed within securities firms before the outsourcing occurs. Rules 342, 346 and 382 of the New York Stock Exchange (of which most large firms are members) have been interpreted to preclude or limit outsourcing either entirely or only to regulated persons.

The Securities Exchange Act of 1934 generally prohibits any person or entity from engaging in the business of effecting transactions in securities for the account of others without first registering with the U.S. Securities and Exchange Commission. The phrase “engaging in the business of effecting transactions in securities for the account of others” has been broadly interpreted to include a myriad of activities.

---

**United States - Banks**

The Federal Financial Institutions Examination Council (FFIEC), the umbrella organization for the five U.S. financial institution regulatory agencies, has issued a series of guidelines and bulletins aimed at clarifying banks’ duties in managing risk in IT outsourcing relationships and at providing guidance to examiners. Recent updates specifically address information security risks in third-party relationships.

Current key U.S. bank regulatory guidance on outsourcing include:
- FDIC’s three technology bulletins entitled Effective Practices for Selecting a Service Provider; Tools to

---

2. Ibid.
Avoiding a Software Audit

Ask most financial services executives whether they are concerned about BSA audits and you’re likely to receive an earful about how difficult it is to comply with what appear to some to be ever-changing and ever-increasing regulatory expectations for AML compliance. But, there’s another BSA that should be receiving management attention, if it isn’t already.

According to Gartner (a leading IT researcher), 40 percent of midsize and large companies, including financial institutions, have the potential to be subject to external software audits in 2005.

Software audits determine whether or not an organization is software compliant. A company is considered to be software compliant if it legally acquired, configured, and is utilizing a genuine copy of copyrighted software in accordance to the terms and conditions of the software licenses purchased. Reasons for noncompliance include:

- Intentionally installing software that is not legally licensed or installing more copies than are licensed
- Employees installing illegal copies
- Asset records not accurately reflecting what is licensed or installed
- Inaccurate inventory records on the part of the software vendor
- Contract usage rights/definitions not clear

Software audits are primarily initiated through software enforcement agencies, such as the Business Software Alliance (BSA). The BSA is a profit-driven agency, which receives information/tips regarding companies’ lack of software compliance or illegal software activities via its hotline primarily from current or former employees. BSA members include Microsoft, Apple, Adobe and other software manufacturers, which typically provide the BSA with information regarding their clients. In addition to agencies such as the BSA, major software manufacturers maintain their own compliance enforcement teams. For example, manufacturers search for potential software violations based on the number of software licenses purchased as compared to the companies’ publicly disclosed number of employees, especially when software maintenance is renewed annually.

Risks to companies that are not software compliant include:

- Fines, new license fees and associated legal fees
- Time and resources required to deal with the software audit
- Damage to a company’s public image and brand

Manage Technology Providers’ Performance Risk: Service Level Agreements; and Techniques for Managing Multiple Service Providers (June 2001). FFIEC IT Handbook entitled “The Supervision of Technology Service Providers (TSP) Booklet” (May 2003), which outlines a risk-based supervision approach to the oversight and management of TSP relationships.

In mid-2004, US bank supervisors finalized an updated FFIEC IT Examination Handbook on Outsourcing Technology Services, which will provide guidance and examination procedures to assist examiners in identifying a financial institution’s risk management processes to establish, manage, and monitor technology outsourcing relationships.

United States - Insurance

Insurance companies are actively involved in the outsourcing of activities. State insurance supervisors have taken a number of approaches in addressing insurer outsourcing, including:

- Specific legal authority granted to the supervisor
- Examples of this include the laws on managing general agents and third-party administrators set forth in the National Association of Insurance Commissioners (NAIC) Managing General Agents Model Act, Third-Party Administrator Model Statute.
- Other outsourced activities are addressed in the on-site market conduct examination process where a company’s internal controls would be examined; including claims processing or investment management and violations addressed through the supervisor’s authority to prevent unfair claims settlement or unfair trade practices.

The NAIC Market Regulation and Consumer Affairs (D) Committee has created a Third-party Vendor Working Group to address further where current regulatory authority does not extend to certain areas in which insurance companies use third-party service providers. The Group expects to produce recommendations for incorporation into the NAIC’s Market Conduct Examiners Handbook.
According to the International Association of IT Asset Managers (IAITAM), settlements are approximately $30,000 per title infringed. Late last year, the BSA announced more than $2.2 million in settlements with 25 companies nationwide, which equates to $80,000 per company. These numbers do not reflect the cost, which can be considerable, of lost business or productivity that results from allocating resources to deal with the software audit process.

For example, on a recent project handled by the Protiviti IT Asset Management team, a major insurance company in the Northeast had paid between $400,000 and $500,000 in software non-compliance costs per year for three years. The total cost includes fines, non-compliant software licenses and maintenance costs, self-audits, software true-up costs and the time expended to deal with all of this.

Once the company was on the BSA’s annual radar screen, it found it difficult to maintain compliance costs without instituting an enterprise IT asset management program, which it completed last year.

Many companies are aware of the risks of software audits and tend to overbuy software to protect themselves. While this may be one way to mitigate risk, it is not cost effective and a more reasoned approach involves the development and maintenance of a software compliance program that includes the following:

- Maintaining solid proof of purchase evidence
- Reviewing software contracts and orders for all licenses against invoices
- Tracking name changes of software products and versions
- Verifying purchase history and inventory
- Validating copyrighted products
- Knowing the terms and conditions of vendor contracts
- Ensuring the terms and conditions are mutually beneficial
- Instituting an automated enterprise life cycle IT asset management (ITAM) program

Findings of a 2004 study commissioned by the BSA of 300 individuals who work in financial services suggest that software compliance programs are highly effective in preventing and reporting software piracy. An automated enterprise ITAM program is the best strategy to ensure software compliance and provide the necessary information for a BSA audit.

---