

Vendor Management: New Guidance Pressures Institutions to Improve Outsourcing Practices

FDIC, OCC Focus on Risk Assessment, Management of Third-Party Relationships

Linda McGlasson, Managing Editor

June 17, 2008

A financial institution can outsource a service, but it cannot cede responsibility for the potential risks to itself and its customers.

This is the message from banking regulatory agencies to member institutions, hammered home by recent bulletins from the Federal Deposit Insurance Corporation (FDIC) ([FDIC Guidance for Managing Third-Party Risk](#)) and Office of the Comptroller of the Currency (OCC) ([OCC Bulletin Released on Application Security for OCC-Regulated Banks](#)), which combined oversee roughly three-quarters of U.S. banks. Their guidance comes on the heels of the National Credit Union Administration's earlier announcement ([Vendor Management and Strategic Planning: How to Tackle the Key Examination Issues of 2008](#)) that **vendor management is a top examination topic** for U.S. credit unions in 2008.



The increased agency focus on managing third-party risk has been on the radar for some time, say industry information security leaders - particularly on the heels of the TJX data breach ([TJX, MasterCard Agree on \\$24 Million Settlement](#)), which revealed the risks and responsibilities of critical customer data in third-party hands. Selection, contract structuring and ongoing management of third-party service providers are the consistent themes from the agencies. **The most frequently used term: "Due diligence."**

"If you do the due diligence and you have good, thoughtful people working on this, along with the appropriate level of legal review, the better off you will be in the long run," says Steve Fritts, Associate Director of Risk Management Policy at the FDIC.

FDIC's Guidance

Recognizing the scale and complexity of institutions' third-party relationships, the FDIC on June 6 issued guidance outlining the potential risks of third-party relationships, as well as risk management principles that may be applied to mitigate the potential threats.

The FDIC guidance, which details the lifecycle of the vendor management process, is something the agency has been working on for more than two years, Fritts says. The guidance is seen as being especially important for the smaller community banks that employ 50 or fewer employees. "They still offer a wide variety of services and rely very heavily on vendors," Fritts says, but they also frequently have relationship managers wearing a variety of different hats within the organization.

Examiners already assess a bank's third-party relationships as a component of the bank examination process. The new guidance emphasizes the need for a basic, common sense approach to due diligence, legal contract management and the operational management of those contracts.

The FDIC also is emphasizing that an **institution's board of directors and senior management** are ultimately responsible for managing third-party activities.

Earlier guidance on vendor management focused more on the IT operations, but the latest statement takes a broader approach, and banks can apply it from a business decision-making and process perspective, Fritts says. "We looked to bring it all together and make it as comprehensive as possible for a bank."

Reputational Risk, Business Continuity

Coupled with the OCC's recent statement about the potential risks of application security, whether in-house or outsourced, the FDIC's latest guidance shows that regulators are paying keen attention to their institutions' most critical third-party relationships - and the institutions must do the same, industry analysts say.

David Schneier, Director of Professional Services at Icons Inc., a Princeton, N.J.-based banking/security consultancy, says he sees a wide range of vendor management activities and programs among his firm's financial institution clients.

"Some of our clients have extensive, well-thought out programs that do an excellent job of identifying and measuring the associated risk factors," he says. Others have remarkably informal approaches that are little better than a hand-shake agreement, with an underlying signed contract. The majority, Schneier says, are "somewhere in the middle" where the institution has some method of assessing a vendor's risk through reviewing its financial soundness, checking contact references, or obtaining SAS 70 reports. Unfortunately, these institutions aren't very good at continually monitoring critical risk factors once they are actively doing business, Schneier says.

Recently, Schneier encountered an institution with a strong vendor management program in place, yet a significant business process had been contracted to a new vendor and the bank's entire process had been bypassed. This was due in large part to the functional business owner "believing they were empowered to make decisions independently without having to ask for anyone's approval," Schneier says. His conclusion: Even with strong controls in place, without proper support from senior management, the best-designed controls are rendered ineffective.

Regulators do not expect bank management to spend an excessive amount of time poring over their relationships with the postal meter company, Fritts says, but rather "Focus on core processes and the bank's major business enterprises that depend on third-party services."

One area that needs special attention, Fritts says, is reputational risk - i.e. when outside loan service agreements or mortgage brokers represent the bank and run afoul. "Some of those relationships have resulted in loss of reputation by a bank that had not completely vetted a vendor," Fritts says.

When entering into third-party relationships, institutions must think through the possible range of situations they might face together, Fritts says. When Hurricane Katrina hit New Orleans, for instance, many of the affected institutions had to revise their planning, backup and vendor support relationships. Many New Orleans-based banks that had arranged to move IT data center operations to the Houston area had to scramble for new options when the hurricane turned and headed toward Houston. "They had to find somewhere else to relocate to, and they had to do this on the fly," Fritts says.

The clear message being sent to banking institutions by their regulators: Vendor management is too critical to be done "on the fly."

[Close Window](#)

BankInfoSecurity.com is your source for bank information security news, regulations, and education.