Managing Third Party Relationships: New Regulatory Guidance for Banks

Jan 14 2014

Posted By: William E. Taibl & Brion T. Winters

Practice Area: Banking and Commercial Finance

The use of third-party relationships has allowed financial institutions to outsource key functions such as tax, legal, audit, information technology and loan servicing (among others). This allocation of banking functions can generate cost savings, increase efficiencies, refocus internal operations and can allow a financial institution to offer new products or services and access new markets. The outsourcing of banking functions can also expose financial institutions to certain risks, including operational, reputational, strategic, and compliance/legal risks.

In response to the increased desire of financial institutions to leverage their finite resources by taking advantage of third-party relationships, the Office of the Comptroller of the Currency and the Federal Reserve Board have released guidance for managing risks associated with the use of third-parties. This Commercial Law Update summarizes the guidance published by the OCC on October 30, 2013 (the "**OCC Guidance**") and the Fed on December 5, 2013 (the "**Fed Guidance**"). Board members, senior management and compliance officers should be aware of how this guidance affects their institution's current outsourcing processes because a failure to implement effective risk management processes in connection with third-party relationships ***may constitute an unsafe and unsound banking practice***.

As of the date of this *Update*, the Federal Deposit Insurance Corporation has not indicated whether it plans to issue new third-party risk management guidance, nor has there been any indication that interagency guidance on this topic is forthcoming. State-chartered non-member banks and savings associations should continue to rely on existing FDIC guidance, including the Financial Institution Letter entitled "Guidance for Managing Third-Party Risk" dated June 6, 2008 (FIL-44-2008), although familiarity with the concepts introduced in the OCC Guidance and the Fed Guidance may be beneficial as you review your third-party risk management processes.

OCC Guidance
The OCC Guidance provides detailed direction to national banks and federal savings associations with regard to assessing and managing the risks related to the use of "third-party relationships," which include any business arrangements between the institution and another entity, whether by contract or otherwise, but generally do not include a financial institution's relationship with its customers.

The general principle underlying the OCC Guidance is that national banks and federal savings associations should "adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships." The OCC Guidance provides financial institutions with flexibility to tailor risk management processes to each financial institution's own risk profile, rather than imposing a one size fits all approach on all financial institutions under the OCC's purview. Nevertheless, the OCC Guidance notes that effective third-party risk management processes should include the following elements throughout the entire relationship:

- **Planning**: develop plans that outline the financial institution's strategy for managing risks inherent in the relationship;
- **Due Diligence and Third-Party Selection**: conduct due diligence commensurate with the level of risk and complexity of the relationship prior to establishing such relationship and consider the third-party's strategies and goals, legal and regulatory compliance, financial condition, business expertise and reputation, information security and reliance on subcontractors;
- **Contract Negotiation**: negotiate written contracts that clearly specify the parties' rights and responsibilities;
- **Ongoing Monitoring**: perform ongoing monitoring throughout the duration of the relationship;
- **Termination**: create contingency plans for terminating the relationship;
- **Documentation and Reporting**: develop proper documentation and reporting processes;
- **Oversight and Accountability**: ensure that the board and senior management of the financial institution are effectively managing the relationship; and
- **Independent Reviews**: perform independent reviews of the financial institution's risk management processes.

The OCC Guidance references heightened requirements on certain "critical activities" (*i.e.*, activities involving significant functions of a financial institution such as payment, clearing, settlement, custody and information technology) that require more comprehensive and rigorous oversight and management. The OCC states that critical activities will impose greater oversight responsibility on a financial institution's senior management and board of directors to ensure that such activities are performed in a safe and sound manner and in compliance with applicable law. The escalated responsibilities of the board and senior management include:

- board approval of initial plans to manage the relationship;
- a more active role in the due diligence process by senior management and the board;
- ongoing monitoring and review of existing relationships;
- board approval of contracts that involve critical activities; and
- independent reviews of risk management processes conducted periodically with appropriate actions taken in response to any adverse results.

The OCC Guidance replaces and enhances prior guidance (namely, Bulletin 2001-47 and OCC Advisory Letter 2000-9) which was less detailed and did not include the heightened requirements applicable to outsourcing "critical activities."

Fed Guidance

The Fed Guidance applies to state member banks, bank and savings and loan holding companies (including their nonbank subsidiaries) and U.S. operations of foreign banking organizations. The Fed Guidance outlines standards for implementing risk management programs regarding a financial institution's use of "service providers" to perform operational functions. The use of the term "service providers" in the Fed Guidance is broadly defined to include all entities (whether bank or non-bank, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign) that have entered into a contractual relationship with a financial institution to provide business functions or activities. Regarding these service provider programs, the Fed Guidance lists the following "core elements" of an effective risk management program:

- **Risk Assessments**: determine whether to outsource, the cost implications and the ability to provide appropriate oversight and management;
- **Due Diligence and Selection of Service Providers**: review business background, reputation and strategy, financial performance/condition and internal controls;
- **Contract Provisions and Considerations**: document terms in written contracts that are reviewed by legal counsel prior to execution and cover, among other things, scope, cost, audit rights, monitoring of performance standards, confidentiality and security of information, indemnification, default and limits on liability;
- **Oversight and Monitoring of Service Providers**: establish performance metrics and ensure that personnel with oversight and management responsibilities have proper expertise and stature to manage the relationship, and structure the process to be risk-focused with more frequent assessments and monitoring for higher risk service providers;
- **Incentive Compensation Review**: review and approve the service provider's compensation structure to determine whether it encourages unnecessary risk-taking; and
- **Business Continuity and Contingency Plans**: prepare contingency plans focusing on critical services and consider alternative arrangements in response to performance failures.

The Fed Guidance states that an appropriate risk management program should be focused on risk (namely, activities that: (a) have a substantial impact on an institution's financial condition, (b) are critical to the institution's ongoing operations, (c) involve sensitive customer information or new bank products or services, or (d) pose material compliance risk) and provide oversight and controls commensurate with the level of risk.

Unlike the OCC Guidance, the Fed Guidance explicitly provides that the depth and formality of a risk management program will depend on the "criticality, complexity, and number of material activities being outsourced." Accordingly, if a smaller financial institution, such as a community bank, outsources a small number of critical activities to reputable service providers – notwithstanding that such critical activities may implicate material risks – the risk management program may be simpler and require less compliance elements and considerations. The Fed's pragmatic approach appears to offer greater flexibility to smaller financial institutions (like community banks) that outsource critical banking activities.
