
On October 30, 2013, the Office of the Comptroller of the Currency (“OCC”) released OCC Bulletin 2013-29, “Third-Party Relationships,” highlighting the enhanced scrutiny to which national bank engagements of third-party service providers are now subject. The Bulletin notes the increasing significance and complexity of these relationships, and raises the concern that banks’ risk management processes may not be keeping pace with these developments. In particular, the OCC has identified deficiencies in banks’ risk management processes that include failure to properly assess and understand the risks and costs of third-party relationships, failure to perform adequate due diligence or ongoing monitoring, failure to assess a service provider’s risk management practices before entering into a contract, entering contracts that incentivize the service provider to take risks that increase revenue but that may be detrimental to the bank and its customers, and engaging in informal relationships without contracts. In light of these problems, as emphasized through recent agency enforcement actions, the Bulletin replaces OCC Bulletin 2001-47, “Third-Party Relationships: Risk Management Principles,” and OCC Advisory Letter 2000-9, “Third-Party Risk,” with increasingly detailed guidance and more stringent direction regarding banks’ ultimate responsibility for their vendors’ performance. National banks should revisit their policies, procedures and processes for evaluating, engaging and monitoring third-party service providers in light of this new articulation of the OCC’s supervisory expectations.

Overview of OCC Risk Management Expectations

The OCC makes clear that a national bank’s failure to have an effective risk management process that is “commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the bank may be an unsafe and unsound banking practice.” To develop an effective risk management process, a bank should formulate a strategy with respect to its third-party relationships and should manage risk throughout each relationship by performing appropriate due diligence, executing written contracts, engaging in ongoing monitoring, establishing contingency plans in the event of termination, delineating clear roles both within the bank and between the bank and its third-party service providers, maintaining appropriate documentation and reporting to senior management and the board of directors, and conducting independent reviews of the bank’s risk management processes. More rigorous risk management will be needed for “critical activities”—e.g., those activities that involve significant bank functions (such as payments, clearing, settlement and custody) or which could cause the bank significant risk, would require a significant commitment of resources, or would have a significant effect on customers or bank operations.

Life Cycle of a Third-Party Relationship

The Bulletin provides guidance and best practices governing each phase of a relationship: planning, due diligence, contract negotiation, ongoing monitoring, and termination. A few highlights are summarized below. In each area, the Bulletin differentiates to some extent between specific references that are expressed as a mandate through the use of
strong affirmative language and other somewhat softer “best practices” that are identified through reference to actions a bank should “consider” taking. While the latter language may give banks slightly greater leeway to deal with specific facts and circumstances, institutions should evaluate carefully any proposal to deviate from any of the standards suggested by the Bulletin, even if the standard is one that the OCC merely indicates that banks should “consider.”

**Planning.** A bank’s senior management should develop a management plan for its third-party relationships, particularly when critical activities are involved. This plan should account for, among other things, risks associated with the outsourced activity, the bank’s strategy, the complexity of the relationship, the cost of controlling risks, the nature and handling of customer interactions, implications for information security, specific laws applicable to the third-party activity, how the bank will monitor and assess compliance, and whether the relationship is consistent with the bank’s broader corporate policies.

**Due diligence.** Elaborating on the unremarkable concept that a bank should conduct due diligence on all prospective third-party-providers before making a selection and entering into a contract, the Bulletin goes on to indicate that a bank should not rely merely on previous experience with or knowledge of the provider. Even banks that have extensive direct and practical experience with a vendor, will now need to place that knowledge within the rubric of “an objective, in-depth assessment of the third party’s ability to perform the activity” safely and soundly and in compliance with law. As part of its diligence, a bank should ensure that, among other things, the third party has effective risk management and compliance programs, has the necessary licenses and expertise for the activity, is financially stable, and has a fee and incentive structure and subcontractor relationships that will not cause the vendor to take undue risks. A bank should also make sure that the third party conducts periodic background checks on its senior management and employees, as well as subcontractors with access to critical systems or confidential information.

**Contract Negotiation.** The Bulletin addresses a number of topics that are suggested or required for inclusion in third-party provider contracts. Institutions that fail to adequately address any of the listed contract topics are likely to be asked to justify the omission. For example, the Bulletin indicates that a third party should be required to promptly notify the bank of material issues and to retain records sufficient to enable the bank to monitor performance and legal compliance. The Bulletin emphasizes the need for audit rights in addition to other oversight provisions, including the direction to “[r]eserve the bank’s right to conduct its own audits of the third party’s activities or to engage an independent party to perform such audits.” This directive is certain to engender some difficult discussions with larger providers of common platforms used by dozens, even hundreds, of banks.

The contract should also address intellectual property rights and compliance with specific laws relevant to the relationship, and should provide for OCC supervision, as well as the right to terminate at OCC direction. National banks should carefully consider what indemnity provisions or limits on liability are appropriate for the specific relationship contemplated. The contract should address the extent to which the third party will be liable for the actions of its subcontractors, and the bank should reserve the right to terminate the contract if the third party’s subcontracting arrangements do not comply with the terms of the contract. The contract should not include burdensome upfront fees or other incentives that might lead to inappropriate risk taking. The Bulletin also indicates that third-party contracts should be approved by the bank’s board when critical activities are involved, a suggestion that may require process changes at many institutions, particularly if the Bulletin is read to require board approval of such agreements even if they are not otherwise material.

**Ongoing Monitoring.** A bank should dedicate sufficient staff to oversee and monitor third parties on an ongoing basis. In particular, a bank should assess a third party’s controls, its ability to meet service-level agreements and performance metrics, compliance, and trends in consumer complaint volume and resolution. National banks should receive regular reports from their third-party providers, and regular onsite visits may also be appropriate.

**Termination.** After a default or termination, a bank should have a contingency plan to transition functions in-house or to another provider. The contingency plan should cover capabilities, resources, and time frame for transition; risks associated with data retention and destruction, information system connections, and access control issues; how joint
intellectual property will be handled; and reputation risks if the termination results from the third party’s failure to meet expectations.

**Responsibilities of Bank Employees**

The Bulletin also recommends that a bank’s board of directors, senior management, and bank employees that directly manage third-party relationships focus on three key areas throughout the relationship.

**Oversight and accountability.** The bank should have clear roles for the board of directors, senior management and employees that directly manage third-party relationships.

- **Board:** ensure effective risk management processes are in place and review and approve relevant policies and processes, as well as contracts related to critical activities.
- **Senior management:** implement risk management processes; ensure appropriate monitoring, due diligence, and documentation of third-party relationships; hold accountable employees managing third-party relationships; and terminate agreements that no longer align with the bank’s strategies or where the vendor is not meeting expectations.
- **Employees:** conduct due diligence and ongoing monitoring of third parties, ensure compliance, address or escalate issues, keep third parties informed of bank operational issues, maintain appropriate documentation, and recommend termination where appropriate.

**Documentation and reporting.** A bank should retain documentation of its third-party risk management process and its arrangements with third parties. The bank should receive regular risk management and performance reports from third parties. Senior management should provide regular reports to the board on its ongoing monitoring and the results of independent reviews.

**Independent reviews.** A bank’s internal auditor, or an independent third party, should conduct reviews of the bank’s risk management processes. Among other things, these reviews should assess whether a third-party relationship is still aligned with the bank’s overall strategy, whether the bank’s processes adequately identify, monitor and report risks, whether the bank adequately responds to material issues like breaches or service disruptions, whether multiple disciplines are involved in risk management where needed (e.g., human resources, physical security, legal), whether there are clearly defined roles and responsibilities, whether there are any conflicts of interest in the selection and oversight of third-party relationships, and whether concentration risks are managed.

The Bulletin can be found [here](#).

If you have any questions regarding this update, please contact:

- **Bill Eckland**
  - weckland@sidley.com
  - 202.736.8267
- **David Teitelbaum**
  - dteitelbaum@sidley.com
  - 202.736.8683
- **Jim Huizinga**
  - jhuizinga@sidley.com
  - 202.736.8681
- **Joel Feinberg**
  - jfeinberg@sidley.com
  - 202.736.8473
- **John Van De Weert**
  - jvandeweert@sidley.com
  - 202.736.8094

**Sidley Banking and Financial Services Practice**

The Banking and Financial Services Practice group offers counseling, transaction and litigation services to domestic and non-U.S. financial institutions and their holding companies, as well as securities, insurance, finance, mortgage, and diversified companies that provide financial
services. We also represent all sectors of the payments industry, including payment networks and processors, money transmitters, and payors and payees in various systems. We represent financial services clients before the U.S. Department of the Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau and state regulatory agencies, as well as financial services regulators in other jurisdictions where we have offices. In addition, we represent clients before the United States Supreme Court, other federal courts and state courts.

To receive future copies of this and other Sidley updates via email, please sign up at www.sidley.com/subscribe