WILMERHALE

OCC Releases New Guidance on Third-Party Risk Management

2013-10-31

The Office of the Comptroller of the Currency (the "OCC") issued on October 30, 2013 updated guidance (OCC Bulletin 2013-29) on managing the risks presented by vendor and other third-party relationships. The activities of customer-facing bank vendors have given rise to recent enforcement actions addressing safety and soundness, consumer protection and other compliance risks, and the OCC's new bulletin makes clear that third-party risk management continues to be a supervisory concern. The new bulletin restates many of the OCC's expectations already described in existing guidance,[1] but it also highlights certain "critical activities" that merit enhanced risk measures and places some new emphasis on three steps in the risk management life cycle: contingency planning; the documentation of third-party risk management activities; and the responsibilities of the board of directors and senior management.

Continued Regulatory Scrutiny

The OCC's new bulletin expresses the OCC's concern that risk management practices are not keeping pace with the growing risk and complexity of third-party relationships. It reiterates that a bank's failure to implement an effective third-party risk management program might constitute an unsafe and unsound banking practice that could prompt a downgrade in a bank's CAMELS management rating or lead to an enforcement action. These statements, together with the recent enforcement activity in this area, suggest that third-party risk management will remain an enforcement priority going forward.

Critical Activities

The bulletin does not establish a uniform set of requirements that are generally applicable to all service providers or all banks. Instead the OCC expects that a bank's risk management practices will be commensurate with the risk and complexity of the bank's third-party relationships. The OCC does seem to go one step further than the existing guidance by highlighting certain third-party relationships that involve "critical activities." According to the OCC, these critical activities include significant bank functions (e.g., payments, clearing, settlements or custody), significant shared

services (e.g., information technology) and other activities that:

- could cause significant customer impacts;
- could cause the bank to face significant operational, compliance, reputational or other risks if the third party fails to perform as promised;
- require a significant investment to implement the third-party relationship; or
- could have a major impact on the bank's operations if the bank must find an alternate third party or bring the services in-house.

With respect to these critical service providers, the OCC expects that the bank will:

- conduct more extensive due diligence of the service provider;
- provide summaries of those due diligence findings to the board of directors;
- ensure that the board of directors reviews and approves the proposed contract with the service provider;
- engage in comprehensive monitoring of the service provider's performance and financial condition, including in some cases by appointing a senior officer responsible for that oversight;
- ensure that the board of directors reviews the results of management's ongoing monitoring; and
- periodically arrange independent testing of the bank's risk controls.

Risk Management Life Cycle

The OCC's prior guidance described a risk management process that requires, for each third-party relationship: a risk assessment to identify the bank's needs and requirements; appropriate due diligence to select the service provider; negotiation of an appropriate contract with the selected service provider; and ongoing monitoring of the service provider's performance and financial condition.

The OCC's new bulletin incorporates these risk management practices and also identifies several other practices that should be a part of the "risk management life cycle," including:

- contingency planning for the termination of the service provider relationship;
- documentation and reporting measures designed to facilitate appropriate service provider oversight; and
- specified roles and responsibilities of the board of directors and senior management for overseeing each service provider relationship.

  These practices were generally described in the OCC's prior guidance, but by identifying them as separate aspects of the risk management life cycle, the OCC's bulletin underscores their importance.

One notable new emphasis is on contingency planning. While prior OCC guidance made clear that service provider contracts should include appropriate post-termination transition services provisions, the OCC now specifically requires planning for the eventual end of a third-party

relationship. In some cases, that planning should include the development of an exit strategy in the event that the bank must terminate the contract early based on the service provider's performance failures or financial condition. This planning should also ensure that the bank has the timing and resources required to transition the services in-house or to a new service provider.

The OCC's new guidance also stresses the importance of banks documenting their third-party risk management activities. These documentation practices should require the retention of due diligence reports, the internal and third-party reports obtained in connection with service provider monitoring and also the reports delivered to senior management or the board of directors.

Consistent with the OCC's continued focus on governance, the OCC also highlights the roles and responsibilities of the board of directors and senior management in managing third-party risks. In particular, the OCC expects that the board of directors will, at least with respect to each critical service provider, review summaries of the due diligence findings and review and approve the proposed contract.

Other Notable OCC Expectations

In addition to the OCC's emphasis on these aspects of the risk management life cycle, the OCC has reiterated, and in some respects expanded upon, its existing expectations. For instance, the OCC's new bulletin provides that:

- The risk assessment and planning process should consider the risks inherent in transitioning the services to a new service provider following the termination of the relationship.
- Due diligence reviews should include reviews of audited financial statements and, in some cases, an analysis of the service provider's financial condition that is as comprehensive as the analysis the bank would conduct before extending credit.
- For customer-facing service providers, due diligence should include reference checks with external organizations such as industry associations, the Better Business Bureau, the Federal Trade Commission and state regulators.
- Service provider contracts should appropriately restrict subcontracting, include performance measures that do not incentivize undesirable outcomes (e.g., adverse effects on bank customers) and require appropriate reporting on customer complaints and material developments affecting the service provider.
- Service provider contracts should address compliance with applicable law and specify appropriate indemnification and other remedies for the service provider's compliance issues.
- Monitoring of each service provider should adapt over time to changes in the service provider's risk profile and, for customer-facing service providers, should extend to the volume, nature and trends of customer complaints.

---

[1] The OCC's new bulletin replaces OCC Bulletin 2001-47 and OCC Advisory Letter 2000-9. It is

intended to supplement the Federal Financial Institutions Examination Council's guidance on outsourcing technology services. The OCC does not refer to the CFPB's 2012 bulletin on oversight of service providers (CFPB Bulletin 2012-03), but the new OCC requirements generally are consistent with the CFPB's expectations.

Authors

Russell J. Bruemmer

RETIRED PARTNER

+1 202 663 6000

Franca Harris Gutierrez

PARTNER

Chair, Financial Institutions Practice

Co-Chair, Securities and Financial Regulation Practice

franca.gutierrez@wilmerhale.com

+1 202 663 6557