November 2013

Regulatory brief

A publication of PwC's financial services regulatory practice

Managing third-party relationships: It's complicated

Overview

On October 30, 2013, the Office of the Comptroller of the Currency ("OCC") issued Bulletin 2013-29, "Third-Party Relationships." The Bulletin's enhanced guidance and new requirements address the growing volume and complexity of operational interconnectedness with third parties. Effective immediately, it applies to OCC-regulated entities, i.e., national banks and federal savings associations ("banks").

The Bulletin builds on previous OCC issuances in four major ways. First, the Bulletin enhances prior risk management standards. As important examples, it addresses the risk of third-parties' reliance on subcontractors (i.e., fourth-parties to the bank), and it adds resilience as an element of managing third-party risk (see **Appendix I** for detail of these new requirements, including those for fourth-party risk).

Second, the Bulletin expands the covered range of "third-party relationships" beyond those addressed in prior OCC issuances. As a result, no third-party relationship remains categorically out of the Bulletin's bounds.

Third, the Bulletin introduces the concept of third-party relationships that involve "critical activities."[1] It sets the expectation that banks will have more comprehensive and rigorous due diligence, management, and oversight of such relationships, including a substantial increase in board involvement (see **Appendix II** for detail of the board's expected role).

Finally, the Bulletin explicitly establishes the overarching standard that a bank "should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships." This signals that the OCC will take a holistic approach to assessing banks' risk management (in addition to applying specific standards) that will require banks to maintain a robust analytical process to identify, measure, monitor, and control the risks associated with third-party relationships. To underline the importance of meeting the overarching standard, the OCC warns that failure to adopt appropriate processes may be "an unsafe and unsound banking practice" resulting in matters requiring attention ("MRAs"), enforcement actions, or an adverse impact on CAMELS ratings.[2]

---

[1] Critical activities include significant bank functions such as payments, clearing, settlements, custody; significant shared services such as information technology; and other activities that involve significant inherent risk.

[2] The CAMELS rating is an overall assessment of a bank based on six individual ratings; the word CAMELS is an acronym for the following: capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk.

pwc

These changes reflect the OCC's lessons-learned from supervising banks' management of third-party risks during the years since the OCC's prior issuances. They also appear to reflect lessons from recovery and resolution planning ("RRP"). For example, RRP revealed that the range of interdependencies that could expose banks to risk is broader than had been addressed in prior OCC issuances. That lesson appears to be reflected in the Bulletin's broader definition of third-party relationships. Similarly, RRP revealed that resilience is an important element of risk management, and the Bulletin specifies consideration of a third-party's resilience as a required part of due diligence.[3]

We believe that the Bulletin's most immediate impact will be to increase the costs of outsourcing functions to third-parties (by increasing the required initial investment and operating costs of risk management systems that meet the new standards). The Bulletin will also likely lead to changes in banks' business models, including some consolidation of third-party vendors and repatriation of outsourced activities. These changes will require increased management attention in the short-run, but will also present a strategic opportunity to improve banks' organizational capabilities, operational resilience, profitability, and ultimately their competitive advantage.

The most successful organizations will be the ones that work to fully meet the enhanced regulatory standards in a way that also enables them to meet their business objectives. The Bulletin provides guidance on the former, but the latter will depend on banks' strategic judgment and creativity, and a healthy dialogue with the regulator.

This **Financial Services Regulatory Brief** provides key background information followed by our view of the Bulletin's most significant highlights: (a) enhancing prior standards, (b) broadening the definition of third-party relationship, (c) establishing higher standards for third-party relationships involving "critical activities," including an increase in board involvement, and (d) signalling the OCC's holistic approach to assessing risk management. We also suggest how banks can adapt to the new third-party risk management requirements.

[3] Recovery and resolution planning requires banks to identify and develop plans to ensure the resilience of material operational interconnections and interdependencies – particularly those that support critical operations – and to enable banks to be sold or wound-down in a timely and orderly manner.

Background

Bulletin 2013-29 rescinds two prior OCC issuances: Bulletin 2001-47 ("Third-Party Relationships: Risk Management Principles") and Advisory Letter 2000-9 ("Third-Party Risk"). Banks should apply the new Bulletin in conjunction with other OCC and interagency issuances on third-party relationships and on other areas of risk management (listed in the Bulletin's Appendix B).

The Bulletin responds to the OCC's concerns about the damage that can be done when banks fail to adequately manage the risks of third-party relationships[4] and its concern that the quality of risk management over third-party relationships has not kept pace with the evolving complexity of those relationships. Notably, the OCC elected to address its views by issuing guidance to help improve the quality of banks' risk management, rather than by curtailing the use of third parties or otherwise attempting to slow the pace of change.

The Bulletin also appears to incorporate information responsive to congressional inquiries on the appropriateness of using independent third-parties to conduct Independent Foreclosure Reviews.[5] The Bulletin explicitly applies to the "use of independent consultants" and documents the baseline requirements that apply to the use of independent third-parties (e.g., standards for selection including due diligence and contractual requirements, and on-going relationships).[6]

[4] The Bulletin lists the following examples of risk-management failures related to third-party relationships: (a) failure to properly assess and understand the risks and direct and indirect costs involved in relationships, (b) failure to perform adequate up front due diligence and on-going monitoring of relationships, (c) entering into contracts without assessing the adequacy of a third party's risk management practices, (d) entering into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers (in order to maximize the third party's revenues), and (e) engaging in relationships without contracts in place.

[5] The Independent Foreclosure Reviews were required under consent orders that the OCC issued in April 2011, in conjunction with the Board of Governors of the Federal Reserve System ("Fed") and the former Office of Thrift Supervision, against 14 major mortgage servicers for unsafe and unsound practices in residential mortgage servicing and foreclosure processing. The Fed subsequently issued similar consent orders against two additional major mortgage servicers.

[6] Separately, in OCC Bulletin 2013-33, issued November 12, 2013, the OCC supplements those baseline requirements by documenting the specific standards the OCC will apply to the use and review of independent consultants in enforcement actions.

What are the key changes?

The OCC builds on prior standards

The Bulletin expands both the breadth and level of detail of the standards for managing the risks associated with third-party relationships, and organizes these new standards around five phases of the third-party relationship "life cycle": planning, due diligence and third-party selection, contract negotiation, on-going monitoring, and termination.

At a high-level, the Bulletin specifies requirements for an effective risk management process across the relationship life cycle, including the following:

- Plans that outline the bank's strategy, identify the inherent risks of the outsourced activity, and detail how the bank selects, assesses, and oversees the third-party.
- Proper due diligence in selecting a third-party, including consideration of the third-party's resilience.
- Written contracts that outline the rights and responsibilities of all parties.
- Ongoing monitoring of the third-party's activities and performance.
- Contingency plans for terminating the relationship in an effective manner.
- Clear roles and responsibilities for overseeing and managing the relationship and risk management processes.
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
- Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

For detail of the Bulletin's key changes from prior issuances, please see **Appendix I.**

The OCC has broadened its definition of "third-party relationships"

The Bulletin defines third-party relationships as "any business arrangement between a bank and another entity, by contract or otherwise," which strongly suggests that the OCC will take a broad view as to which third-party relationships fall within the Bulletin's scope.[7]

The following are illustrative examples of in-scope third-party relationships provided in the Bulletin:

- Activities that involve outsourced products and services.
- Use of independent consultants.
- Networking arrangements.
- Merchant payment processing services.
- Other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records.

Importantly, the definition also captures bank and nonbank affiliates and joint ventures, which greatly expands the number of in-scope third-parties for complex banking organizations. The definition even covers banks' relationships with other OCC-supervised institutions. The Bulletin requires the same standard of oversight to be applied to relationships with both banks and nonbanks.

This scope expansion[8] means that the OCC will be looking for banks to establish risk management infrastructure that entirely covers their operational interconnectedness and interrelationships.

---

[7] Prior OCC issuances identified certain types of third-party relationships of regulatory interest, but did not attempt to broadly define third-party relationships. For example, OCC Bulletin 2001-47 does not define third-party relationships, but explains that banks utilize third parties in three main ways: third parties performing services on the bank's behalf; third parties providing products and services that the bank does not originate; and the bank franchising its name or regulated entity status to a third party. OCC Advisory Letter 2000-9 similarly does not define third-party relationships. Instead, it lists examples of third parties (e.g., vendors, agents, dealers, brokers, marketers, etc.) and discusses risk management as related to certain third-parties: credit repair vendors and marketers, vendor-supplied accounts receivable financing software, loan participations in large, syndicated national credits, and third-parties engaged to monitor and control real estate construction loan disbursements.

[8] This scope expansion is also evident from the relationships the OCC cites as examples of the complexities that the Bulletin aims to address: (a) outsourcing entire bank functions such as tax, legal, audit, or information technology operations to third parties; (b) outsourcing lines of business or products; (c) relying on a single third party to perform multiple activities (often to such an extent that the third party becomes an integral component of the bank's operations); (d) working with third parties that engage directly with customers (e.g., in a franchising arrangement); (e) contracting with third parties that subcontract activities to other foreign and domestic providers; (f) contracting with third parties whose employees, facilities, and subcontractors may be geographically concentrated; and (g) working with a third party to address deficiencies in bank operations or compliance with laws or regulations.

The OCC will focus on third-party relationships that involve "critical activities"

The Bulletin introduces the concept of "critical activities," and a corresponding expectation that banks will have more comprehensive and rigorous due diligence, management, and oversight of third-party relationships that involve such activities.[9] Accordingly, in its future assessments of banks' risk management of third-party relationships, the OCC will likely prioritize relationships that involve critical activities and hold banks to a higher risk management standard for them. Consistent with the Bulletin's definition of critical activities, the OCC will take a multi-dimensional approach to determining what activities are "critical" and will expect to see a high degree of board involvement in the risk management of corresponding relationships, as described below.

What are "critical activities"?

The Bulletin defines "critical activities" to include:

- Significant bank functions (e.g., payments, clearing, settlements, and custody).
- Significant shared services (e.g., information technology).
- Other activities that
  - Could cause a bank to face significant risk if the third-party fails to meet expectations;
  - Could have significant customer impact;
  - Require significant investment in resources to implement the third-party relationship and manage the risk; or
  - Could have a major impact on bank operations if the bank has to find an alternate third-party or if the outsourced activity has to be brought in-house.

This definition provides three very different pathways to finding an activity to be "critical." First, an activity can be critical based on the significance of the bank *function* involved. Second, an activity can be critical based on whether it involves a *shared service* and whether that shared service is significant. Third, and more open-ended, an activity can be critical based on its potential impact, or its *inherent risk*. Applying this third definition of "critical activity" will require consideration of potential adverse impacts under a wide range of risk-event scenarios which will make it the most challenging element of the definition to apply.

[9] Neither of the prior OCC issuances had used the term "critical activities." OCC Bulletin 2001-47 had referred to "material" third-party relationships, but did not define the term "material."

The OCC's view of whether a particular activity is "critical" for purposes of the Bulletin may be influenced by how a bank characterized the same activity for purposes of RRP. The Bulletin addresses "critical activities" (e.g., payments, clearing, and settlement), and the RRP processes address "critical operations" and "critical services."[10] While those terms are not identical, operations or services that a bank has already determined to be "critical" in RRP may effectively be presumed to be "critical" in this context as well.

Expectations of board involvement for relationships involving "critical activities"

The OCC's expectation of more rigorous oversight of third-party relationships involving critical activities includes increased board involvement in the risk management of those relationships.[11] For example, among other requirements, the board is explicitly required to take the following actions:

- Approve the bank's risk-based policies that govern third-party risk management processes and identify critical activities.
- Review and approve management plans for establishing the relationships.
- Review summary of due diligence results and management's recommendations for the relationships.
- Approve contracts that govern the relationships.
- Review the results of management's ongoing monitoring of the relationships.

A full listing of board responsibilities is provided in **Appendix II**.

[10] "Critical operations" and "critical services" are terms used by the Fed and the FDIC, respectively, in the context of recovery and resolution planning. See 12 C.F.R. § 243.2(g), defining "critical operations" as "those operations of the covered company, including associated services, functions and support, the failure or discontinuance of which, in the view of the covered company or as jointly directed by the Board and the Corporation, would pose a threat to the financial stability of the United States." See also 12 C.F.R. § 360.10(b)(5), defining "critical services" as "services and operations of [an insured depository institution with $50 billion or more in total assets], such as servicing, information technology support and operations, human resources and personnel that are necessary to continue the day-to-day operations of the [institution]."

[11] The Bulletin also increases the involvement of senior management in the risk management of third-party relationships.

The OCC will take a holistic approach to third-party relationship risk management

The Bulletin signals that the OCC will take a holistic approach to assessing banks' risk management of third-party relationships, a theme also seen in the OCC's "heightened expectations" program for larger banks. This approach is consistent with the OCC's long-held expectation that banks should practice effective risk management regardless of whether they perform an activity internally or through a third-party, and that a bank's use of third-parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner in compliance with applicable law.

The Bulletin's strongest signal of the OCC's holistic approach is its articulation of its overarching standard for risk management of third-party relationships – the standard from which all other standards within the Bulletin are derived – as follows:

> A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.[12]

Another signal is the Bulletin's guidance to OCC examiners reviewing third-party relationships, which begins its list of review activities with "assess the bank's ability to oversee and manage its relationships."

A third indicator of the OCC's holistic approach is that the Bulletin incorporates other regulatory issuances (by way of Appendix B to the Bulletin), both with respect to third-party risk management as well as other areas of risk management.

What this means to banks is that the OCC will base its assessment on the overall effectiveness of a bank's risk management processes, rather than solely on whether the bank has faithfully incorporated all applicable standards from the Bulletin (although the latter will also be taken into account). Therefore, while banks need to take seriously all of the specific standards set forth in the Bulletin, they must not lose sight of the ultimate objective, which is to adopt risk management processes commensurate with the level of risk and complexity of their third-party relationships.

Achieving this objective may result in decisions to go beyond the minimum standards required under the Bulletin for some third-party relationships. On the other hand, it also may provide a common touchstone to enable banks and the regulator to agree on sensible, workable approaches to situations where a rigid application of the Bulletin would have unintended adverse consequences (e.g., distracting board attention from matters of greater safety-and-soundness importance).

Adapting to change: how to operationalize the Bulletin's requirements?

Board and senior management

The first step in responding to the Bulletin is to recognize it as a significant regulatory document that requires banks to look differently at their third-party relationships and at how they manage their associated risks. This analysis will no doubt bring about changes in banks' policies, procedures, and infrastructure.

The next step is to prepare an analysis of the Bulletin and what it means for a particular organization. This analysis will assist a bank in communicating the importance of the guidance to its senior management, including the likely impact on the bank's operations and risk management programs.

Efforts to communicate the importance of the Bulletin must also include alerting the board and senior management to their additional responsibilities around third-party relationships involving critical activities. This includes providing guidance to the board and senior management as to what they should be expecting, how they should be preparing, and what information they should be requesting (e.g., reports, briefings and educational materials). This process should also include developing approaches to integrating the Bulletin's expectations for board and senior management involvement into the bank's governance processes. Where strict application of the Bulletin would result in unintended adverse consequences, banks must proactively develop and propose alternative approaches that would be commensurate with the risk and complexity of their relevant third-party relationships.

Existing relationships

Given the broad scope of the third-party relationships that may be of OCC regulatory interest, banks must review and enhance the existing inventory of their third-party relationships, based on the broad definition used in the Bulletin.

Considering the elevated regulatory interest in third-party relationships involving critical activities, banks will also need to identify such relationships applying the criteria set forth in the Bulletin, i.e., function type,

[12] While that standard is articulated as a "should" rather than a "must," the Bulletin later warns that a bank's failure to adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships may be "*an unsafe and unsound banking practice.*"

shared service, and inherent risk factors. Banks then need to prioritize reviewing and assessing risk management practices around identified relationships to align them with the Bulletin.

Simultaneously banks must apply the overarching standard of bringing their risk management processes to a level of effectiveness that is "commensurate with the level of risk and complexity" of each relationship, and develop action plans to address gaps. Banks must keep in mind that compliance is not just a checklist: processes have to be effective in managing risk.

Risk management processes

On a parallel path, banks must assess their third-party risk management processes against the Bulletin (including the overarching standard), and address deficiencies. Third-party risk management processes must be effectively integrated within the enterprise risk management framework. This may include:[13]

- Integrating the third-party risk appetite with the overall risk appetite statement by creating third-party risk appetite metrics and leveraging third-party key risk indicators developed from data metrics.
- Improving the risk stratification process used in identifying the inherent risk of third-party services, to be able to justify necessary but inherently high risk services and critical activities provided by third-parties.
- Identifying and addressing possible cultural impediments to meeting the new standards (e.g., a perception that the bank is not responsible for failures of third-party providers).
- Determining and implementing necessary changes to board and management reporting processes.
- Considering the extent to which governance around initiation and oversight of third-party relationships (including roles and responsibilities) foster or impair effective risk management.
- Developing and implementing necessary training programs.

Strategic assessment

The Bulletin creates both an imperative and an opportunity to strategically re-evaluate how the use of third-parties aligns with a bank's business model, business plans and objectives, and risk appetite, and to implement changes where there is no clear alignment or where the business case is no longer evident. This may include analysis at the function level, the individual third-party provider level, and at the aggregate third-party level.

Resulting business changes could include consolidating particular third-party relationships, balancing efficiencies (e.g., by limiting the number of third-parties relied upon vs. the need to manage concentration risk), and implementing resiliency and termination plans by diversifying third-parties. Banks may also determine that, in light of the risk management burden, it may be more cost effective to repatriate some functions that are currently outsourced.

Organizations that will be most successful in bringing their risk management processes up to the levels of effectiveness contemplated under the Bulletin will be those that take a strategic approach to the exercise. Such an approach would address (1) the specific elements of the new standards, (2) the overarching objective of having risk management processes that are commensurate with the level of risk and complexity of the bank's third-party relationships, and (3) the bank's business objectives.

Conclusion

At one level, the Bulletin makes common sense: banks' risk management processes should be commensurate with the level of risk and complexity of all of their activities, including those conducted via third-party relationships. However, managing the risk of third-party relationships is notoriously hard to perfect because, by definition, delegation entails lesser direct control, as evidenced by a seemingly endless string of enforcement actions. On the other hand, an increasing range of third-party relationships is available to banks to help them achieve efficiencies, increase profitability, and improve operations – and the OCC is not discouraging banks from utilizing such relationships.

In the short-run the process of bringing banks into compliance with the enhanced standards for risk management of third-party relationships will require real effort. However, a parallel process of strategic analysis can result in improvements to banks' organizational capabilities, their operational resilience, profitability, and ultimately competitive advantage. Success means risk management practices that meet the new enhanced standards – in a way that also enables banks to meet their overall business objectives. The OCC will help banks make sure they meet OCC's needs, but only banks can take the steps necessary to also meet theirs.

[13] For insights into additional steps that may be appropriate, see PwC's *Financial Services Viewpoint, Significant Others: How financial institutions can effectively manage the risks of third-party relationships* (September 2013).

Appendix I – Key changes in regulatory standards for risk management of third party relationships

Risk management activities over third party relationship life cycle

Life cycle phase	Key changes from prior OCC issuances
Planning	• Introduces the assessment of inherent risks of the services to be provided by third parties. • Introduces considerations specific to "dual employees," and the potential for conflicts of interest. • Requires senior management to develop and present a plan to engage third parties for board approval when critical activities are involved.
Due diligence	• Introduces senior management's responsibility to review due diligence results. • Expands the concept of third-party resilience, which is broader than disaster recovery and business continuity plans required in Bulletin 2001-47. • Expands upon due diligence areas previously mentioned in Bulletin 2001-47 and introduces new areas such as legal and regulatory compliance, information security, incident reporting and management programs, physical security, and conflicting contractual arrangements with other parties. • Expects due diligence to be conducted on critical fourth parties as necessary.
Contracting	• Requires senior management to obtain board approval before contracting with a third party to provide critical activities. • Introduces guidance to review existing contracts periodically to ensure they continue to include pertinent risk controls and legal protections. • Introduces guidance for contract clauses addressing responsibility for compliance with applicable laws and regulations.
On-going monitoring	• Introduces senior management's role to periodically assess third party relationships for identification of critical activities. • Introduces the need for on-going review of the third party's reliance on, exposure to, or performance of, subcontractors; location of subcontractors; and the monitoring and control testing of subcontractors. • Introduces monitoring for conflicting interests. • Requires closer monitoring of the ability to appropriately remediate customer complaints. • Requires more attention to roles and responsibilities in escalations/reporting during on-going monitoring.
Termination	• Explicitly identifies termination as a step in the life cycle. • Expects a transition plan to be developed and provides guidance on the components that a transition plan should address.

On-going risk management activities

Activity	Key changes from prior OCC issuances
Oversight and accountability	• Sets the clear requirement that a bank's board of directors and senior management are responsible for overseeing the bank's third party risk management processes. • Provides specific guidance on the responsibilities for the board of directors, senior management, and employees who directly manage third party relationships.
Documentation and reporting	• Requires an inventory of all third party relationships and identification of relationships that involve critical activities and the risks posed by those relationships. • Introduces guidance to document analysis of costs associated with each activity or third party relationship, including any indirect costs assumed by the bank. • Introduces guidance to provide regular reports to the board and senior management on the results of internal controls testing, on-going monitoring, and independent reviews of the bank's third party risk management process.
Independent reviews	• Introduces the need for periodic independent reviews of the bank's third party risk management process. The bank's internal auditor or an independent third party may perform the reviews. • Expects senior management to ensure the results of the independent reviews are reported to the board of directors.

Fourth-party (i.e., subcontractor) risks

Risk	New standards
Due diligence	• Evaluate the volume and types of subcontracted activities and the subcontractors' geographic locations. • Evaluate the third party's ability to assess, monitor, and mitigate risks from its use of subcontractors. • Ensure that the same level of quality and controls exists no matter where the subcontractors' operations reside. • Evaluate whether additional concentration-related risks may arise from the third party's reliance on subcontractors. • If necessary, conduct similar due diligence on the third party's critical subcontractors.
Third party contract stipulations	• Periodic independent internal or external audits of the third party and relevant subcontractors. • Restrictions on use of the bank's information by the third party and its subcontractors. • When and how the third party should notify the bank of its intent to use a subcontractor. • The activities that cannot be subcontracted or whether the bank prohibits the third party from subcontracting activities to certain locations or specific subcontractors. • The contractual obligations regarding the performance of the subcontractors and the third party's liability for activities or actions performed by its subcontractors.
Other	• Ensure the third party periodically conducts thorough background checks on subcontractors who may have access to critical systems or confidential information. • Obtain information regarding legally binding arrangements between a third party and its subcontractors or other parties, and evaluate the potential legal and financial implications to the bank of these contracts. • Reserve the right to terminate a contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract. • Perform on-going monitoring of the third party's reliance on, exposure to, or performance of subcontractors; location of subcontractors; and the monitoring and control testing of subcontractors. • As part of the independent reviews of the bank's third party risk management process, assess the adequacy of the process for identifying and managing risks associated with subcontractors.

Appendix II – Board involvement in third party risk management

Life cycle phase	Relevant excerpts from OCC 2013-29[14]
Planning	Before entering into a third party relationship, senior management should develop a plan to manage the relationship. *The management plan should be commensurate with the level of risk and complexity of the third party relationship and should […] be presented to and approved by the bank's board of directors when critical activities are involved.*
Due diligence and third party selection	Senior management should review the results of the due diligence to determine whether the third party is able to meet the bank's expectations and whether the bank should proceed with the third party relationship. If the results do not meet expectations, management should recommend that the third party make appropriate changes, find an alternate third party, conduct the activity in-house, or discontinue the activity. As part of any recommended changes, the bank may need to supplement the third party's resources or increase or implement new controls to manage the risks. *Management should present results of due diligence to the board when making recommendations for third party relationships that involve critical activities.*
Contract negotiation	Once the bank selects a third party, management should negotiate a contract that clearly specifies the rights and responsibilities of each party to the contract. *Additionally, senior management should obtain board approval of the contract before its execution when a third party relationship will involve critical activities.*
On-going monitoring	Bank employees who directly manage third party relationships should escalate to senior management significant issues or concerns arising from on-going monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or compliance lapses. *Additionally, management should ensure that the bank's controls to manage risks from third party relationships are tested regularly, particularly where critical activities are involved. Based on the results of the on-going monitoring and internal control testing, management should respond to issues when identified including escalating significant issues to the board.*

[14] Emphasis added by *italicizing* certain text.

Life cycle phase	Relevant excerpts from OCC 2013-29[14]
Oversight and accountability	The bank's board of directors (or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes. *The board, senior management, and employees within the lines of businesses who manage the third party relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities.* Board of Directors [must:] • Ensure an effective process is in place to manage risks related to third party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite. • *Approve the bank's risk-based policies that govern the third party risk management process and identify critical activities.* • *Review and approve management plans for using third parties that involve critical activities.* • *Review summary of due diligence results and management's recommendations to use third parties that involve critical activities.* • *Approve contracts with third parties that involve critical activities.* • *Review the results of management's on-going monitoring of third party relationships involving critical activities.* • Ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through on-going monitoring. • Review results of periodic independent reviews of the bank's third party risk management process.
Independent reviews	Senior management should ensure that periodic independent reviews are conducted on the third party risk management process, particularly when a bank involves third parties in critical activities. The bank's internal auditor or an independent third party may perform the reviews, and senior management should ensure the results are reported to the board. *Management should respond promptly and thoroughly to significant issues or concerns identified and escalate to the board if the risk posed is approaching the bank's risk appetite limits.*

www.pwcregulatory.com

Additional information

PwC Financial Services Regulatory Practice

Dan Ryan
Financial Services Regulatory Practice Chairman
646 471 8488
daniel.ryan@us.pwc.com

Alison Gilmore
646 471 0588
alison.gilmore@us.pwc.com

Douglas Roeder
703 918 3492
douglas.w.roeder@us.pwc.com

Kenneth Peyer
415 498 7061
kenneth.peyer@us.pwc.com

Daniel Morrison
602 206 3273
daniel.morrison@us.pwc.com

PwC Consumer Finance Group

Richard Altham
207 502 2347
richard.altham@us.pwc.com

John Kowalak
646 471 3519
john.kowalak@us.pwc.com

Jason Chan
214 754 5142
jason.chan@us.pwc.com

Contributors: David Albright, Richard Altham, Jason Chan, John Kowalak, Daniel Morrison, Bruce Oliver, Kenneth Peyer, Douglas Roeder and Gary Welsh.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs