KPMG

cutting through complexity

Financial Services Regulatory Point of View

The New Third-Party Oversight Framework: Trust but Verify

kpmg.com

Financial services regulatory focus on third-party risk management in the United States as well as in other jurisdictions has increased as firms continue to expand the number and complexity of relationships with both foreign and domestic third parties. Recent releases from the U.S. Office of the Comptroller of the Currency (OCC) and the Board of Governors of the Federal Reserve System (Federal Reserve) focus on enhanced bank and bank holding company examination guidance in this area, and reflect the evolution in regulatory thinking about how firms must manage the third-party oversight (TPO) process.

The OCC's updated guidance on the risk management of third-party relationships (OCC Bulletin 2013-29, *Third-Party Relationships: Risk Management Guidance*, dated October 30, 2013) signals a fundamental shift in how financial institutions need to assess third-party relationships.[1] In particular, it calls for robust risk assessment and monitoring processes to be employed relative to third-party relationships, and specifically those that involve "critical activities" with the potential to expose an institution to significant risk.[2] It further directs institutions to ensure their boards of directors receive adequate risk reporting on third-party relationships, effectively requiring third parties to be fully integrated into an institution's existing enterprise-risk management (ERM) and compliance framework.

Heretofore, financial institutions, in many instances, have managed third-party risk through siloed risk domain oversight accompanied by procurement and supplier management processes. The OCC notes that a siloed approach is fundamentally insufficient for those relationships that reflect high-risk characteristics, including consumer compliance risk, information security risk, and business continuity risk. The challenge, then, is for institutions to involve existing risk and compliance domain experts in both the first and second lines of defense in third-party oversight and management processes. Furthermore, the OCC calls for independent review assessments of third-party risk management processes, particularly where third parties are involved in "critical activities," which necessitates increased participation from the third line of defense through internal audit or other third parties.

---

[1] The guidance defines a "third-party relationship" as any business arrangement between a bank and another entity, by contract or otherwise. Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal Reserve Act (12 USC 371c and 12 USC 371c-1) as implemented in Regulation W (12 CFR 223). Third-party relationships generally do not include customer relationships.

[2] The guidance defines "critical activities" as "significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that:

- Could cause a bank to face significant risk if the third party fails to meet expectations.
- Could have significant customer impacts.
- Require significant investment in resources to implement the third-party relationship and manage the risk.
- 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."

The Federal Reserve's guidance (Supervision and Regulation Letter 13-21, *Guidance on Managing Outsourcing Risk*, dated December 5, 2013) is substantially similar to the OCC's, though narrower in focus. That is, it is intended to address the characteristics, governance, and operational effectiveness of a financial institution's service provider risk management program for outsourced activities that are beyond traditional core bank processing and information technology services. These are activities such as accounting, appraisal management, internal audit, human resources, sales and marketing, loan review, asset and wealth management, procurement, and loan servicing.[3]

Notably, the guidance from each of the agencies is principles-based, and the degree to which the assessment and risk management processes need to be coordinated with a financial institution's ERM and compliance functions is left to the institutions themselves. We believe certain institutions will take a very proactive approach to this integration across the first and second lines, whereas others may take a "wait-and-see" approach, awaiting more prescriptive guidance or looking to see what industry practices emerge. For those institutions that take the latter course, we believe there is significant risk of regulatory criticism given that the OCC, Federal Reserve, and other bank regulators continue to conduct target reviews of third-party risk. We also believe this may be a missed opportunity to help shape leading practice.

From recent experience, it is clear that the banking industry needs to self-assess whether they are appropriately considering monitoring and managing compliance risk associated with third parties that touch consumers. We have seen the industry move toward a more "hands-on," enterprise-wide assessment of the compliance risk, but we believe more steps need to be taken. The guidance is a wake-up call to enlighten institutions on this critical aspect of the enterprise-risk and compliance assessment.

Finally, as institutions look to enhance the comprehensiveness of their risk and control self-assessments, we recommend specific attention be given to hand-offs to third parties, including affiliated parties, and to identification of the associated risks and controls at these points. These risk assessments are fundamental to a firm's ability to identify, measure, monitor, manage, and report risk as well as to ensure the effectiveness and sustainability of its enterprise/line of business (LOB) risk appetite process.

[3] For purposes of the Federal Reserve's guidance, a "service provider" is broadly defined to include all entities (bank or nonbank, affiliated or nonaffiliated, regulated or nonregulated, or domestic or foreign) that have entered into a contractual relationship with a financial institution to provide business functions or activities. Broadly, the guidance covers: risks from the use of service providers; board of directors and senior management responsibilities; and service provider risk management programs.

Three Lines of Defense

The "three lines of defense" model provides an effective framework for governance risk management and assurance by defining clear roles and responsibilities across the organization.

- The "first line" is the business owners. The business is responsible for complying with risk management processes and procedures, implementing actions to manage and treat risk and to identify emerging risk.
- The "second line" is the standards setters, comprising the oversight functions. They are responsible for establishing policies and procedures for risk management, providing oversight over certain risk areas, and identifying enterprise trends, synergies, and opportunities for change.
- The "third line" is the assurance providers (internal and external audit). Their role is to provide independent and objective assurance that risk management processes are adequate and appropriate.

Fundamentally, third-party risk management is different from the contracting function, and while institutions are permitted to outsource a variety of operations and activities, they may not outsource accountability for the activities performed on their behalf. The OCC states in its guidance, "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 and in compliance with applicable laws." The Federal Reserve guidance echoes these sentiments.[4]

The new guidance is a response to the agencies' concern that "the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships,"[5] adding that the number and complexity of relationships with both foreign and domestic third parties continue to increase. We see not only an increase in third-party relationships, but also a clear evolution of the traditional business model that reflects an increased reliance on third parties.

The OCC specifically outlines a new third-party risk management process that is intended to cover each relationship from end-to-end, as well as continuously, over the relationship life cycle. The following eight phases are identified:

- Planning (incorporating risk strategy, identification of inherent risks of activities, and use of third parties)
- Due diligence and third-party selection
- Contract negotiation
- Ongoing monitoring
- Termination, including contingency plans
- Roles and responsibilities for oversight and relationship management
- Documentation and reporting
- Independent review

[4] "The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations." Federal Reserve SR 13-19, page 2 of 12.

[5] OCC Bulletin 2013-29.

In the context of this framework,[6] institutions must develop a suitable risk-based approach to third-party management giving consideration to a variety of questions:

What is a third party?

The OCC (and the other bank regulators) has a very broad view of third-party relationships, which generally excludes customers but encompasses:

- Vendors and vendors' vendors
- Suppliers
- Outsource providers including IT outsourcing providers, business process outsourcing providers, call center providers, HR outsourcing providers, and real estate and facilitates management
- Joint ventures partners
- Affiliates for which the institution is deemed to have control
- Professional service firms
- Business alliance members
- Contingency arrangement participants
- Contingent workers
- Counterparties

Similarly, it encompasses all of the paths by which a financial institution interacts with these third parties including on-site and off-site; onshore and offshore; "cloud"; out sourced and cosourced; and integrated and continuous.

Who are the third parties associated with the institution, and what do they do?

We suggest institutions list all third-party relationships with which they are involved or have an obligation to become involved with. Many financial institutions will have a list of thousands.

Consider developing a matrix of risk information that can be used to categorize/prioritize each relationship, e.g., does this third-party relationship involve the institution's customers? Or sensitive data? Or critical IT systems? Or regulated products and services? Is the third party in a domestic or foreign location? Can the third party's role be easily replaced if the third party fails to meet its contractual obligations? Does the third party participate in a "critical activity"?

[6] Federal Reserve SR 13-19 outlines consideration of: risk assessments; due diligence and selection of service providers; contract provisions and considerations; incentive compensation review; oversight and monitoring of service providers; and business continuity and contingency plans.

What are "critical activities" to the institution, and which third parties participate in these activities?

The OCC guidance defines "critical activities" to include "significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that:[7]

- Could cause a bank to face significant risk if the third party fails to meet expectations.
- Could have significant customer impacts.
- Require significant investment in resources to implement the third-party relationship and manage the risk.
- 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."

Third-party arrangements that involve "critical activities" are expected to have "more comprehensive and rigorous" oversight, including:

- Board review of summary results of senior management due diligence reviews and recommendations regarding whether to retain a third party to engage in critical activities.
- Board approval of a management plan for each relationship with a third party involved with critical activities in advance of entering into the relationship.
- Board approval of contracts with third parties involved with critical activities.
- Board review of ongoing monitoring results for third parties involved with critical activities.
- Institutions must consider how their boards can best accommodate the new responsibilities for third-party risk management, including possible new reporting lines and requirements and functional responsibilities.

[7] Note that the Federal Reserve guidance is directed to outsourced activities that are beyond traditional core bank processing and information technology services.

Where does each third party enter the institution's operations or product/service life cycle? How important is the third party to the process?

For critical processes and services, consider determining through process mapping where the exact hand-offs are between the institution and third parties.

How do we identify the risks associated with handing off the operations or the product at this point?

There is a need to identify risk at different points in the third-party life cycle: at the commencement of the relationship, and on a regular basis thereafter, based on a number of factors that influence the risk the third party generates, such as privacy, regulatory compliance, business continuity planning, and information security. However, there also needs to be an early warning system that can alert management to a potential increase of risk outside of these scheduled assessments. This is where the link to risk appetite, key performance, and risk indicators comes into play.

The risk oversight functions need to work together to build a set of factors that can assess the inherent risk associated with an activity plus any increase in risk associated with outsourcing the activity to a third party, the mitigating effect of existing measures employed by the institution and the third party to control that risk, and the determining of the remaining risk,or residual risk that the institution continues to bear. These assessments should be flexible to accommodate an initial risk due diligence exercise or an ongoing monitoring and testing assessment, as well as to accommodate on-site or off-site reviews. An increase in residual risk that exceeds the institution's risk appetite threshold should be further evaluated.

Who is responsible for managing the relationship? What are the parameters of oversight?

From a risk perspective, the board is ultimately accountable for risk management, even though it has delegated daily management of this responsibility to the second line oversight functions. The board sets the standards and policies for the organization to follow, and their responsibility is to make sure that the lines of business (LOBs) are implementing and following these standards and policies.

With day-to-day responsibility for management of third parties, LOBs should be managing each third party as if it were a part of the LOB's in-house operations (i.e., if you conduct a monitoring activity in your LOB, it should also cover third parties). Contracts should incorporate measures that serve as triggers to permit increased LOB oversight in cases of increased risk.

In general, financial institutions use third parties to (1) outsource internal operations, (2) make available to their customers products or services that they do not generally provide, and (3) lend their name or regulated status to activities or services conducted by others for a fee. In some cases, they use third parties to address resource constraints, develop additional products or services, and provide expertise that would not otherwise be available internally.

How are problems identified? How are problems addressed?

Developing an understanding of the risk that a third party generates allows the organization to build an early warning system to identify risk outside of the formal risk assessment activities of initial and ongoing risk assessments. Contracts can be drafted to address the need for various risk and control performance metrics and measures to be collected from a third party to assist the management and oversight functions. However, in some cases a need may develop for increased monitoring of third parties to gather reliable performance metrics and measures. It is these additional costs of oversight that often tend to reduce the reward associated with a particular third-party relationship, and may result in total costs (monitoring and controls and risks) that outweigh the benefits of contracting with that third party. In addition, the risk that the costs could outweigh the benefits highlights the importance of a thorough risk assessment and a broad understanding of the third party and its relationship to the institution.

What do we do with existing third parties?

Financial institutions may be challenged by how to address current third-party relationships in light of the OCC guidance. Like all other potential third parties, existing relationships should be incorporated into planning and risk analyses. The OCC guidance clearly states that experience with, or prior knowledge of, a third party is not considered to be a proxy for an objective, in-depth due diligence assessment. In addition, existing contracts should be reviewed periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections. Where problems are identified, the institutions should seek to renegotiate the contract at the earliest opportunity.

What factors should be considered in whether to use a third party for the independent review?

The new guidance requires institutions to conduct periodic independent reviews on the third-party risk management process, particularly when third parties are involved in critical activities. The institution's internal auditor or an independent third party may perform the reviews, and senior management should ensure the results are reported to the board. The volume of such reviews, the risks they involve, and when they need to be done will drive the number and type of resources required. In some cases, the independent review requirements can be met by an institution's Internal Audit group, but in other cases, it will be necessary to use outside third parties to conduct the assessment.

Financial institutions derive benefits from the use of third parties primarily through the realization of cost-savings or gained expertise. Generally, they use third parties to (1) outsource internal operations, (2) make available to their customers products or services that they do not generally provide, and (3) lend their name or regulated status to activities or services conducted by others for a fee. In some cases, they use third parties to: address resource constraints, develop additional products or services, and provide expertise that would not otherwise be available internally.

The identified industry shift toward an increasing use of third-party providers is a fundamental and real change in the financial institutions' business model that is not likely to abate. It is driven largely by rising costs, though the savings are met with an increase in the risk generated by those third parties. As such, the past approach of managing third parties needs to be updated to reflect a more comprehensive approach to risk management.

Again, the OCC's third-party management framework is a reaction to this shift, recognizing that an increasing percentage of financial institutions entrust a growing percentage of their businesses to outside vendors, and sometimes their vendor's vendors, bringing a commensurate increase in risk that comes with this change. To accommodate the shift, the OCC and the other bank regulators have:

- Elevated the focus on risk management and introduced a process that evaluates every relationship from end-to-end over the continuous life cycle of the relationship
- Elevated the role of senior management and the board with respect to those third parties that expose an institution to the most risk
- Insulated the institution from business interruptions related to a third party's failure to meet its obligations by requiring consideration of contingency plans to replace third parties that default, or to evaluate more viable options.

To address these requirements in a piecemeal or siloed approach would be to miss an opportunity for better risk management. Institutions should use their experiences setting up enterprise-risk and compliance programs to bring an institution-wide risk lens and mind-set to view in a holistic manner the risks that third parties generate.

As the shift to third-party relationships continues to increase, the ultimate future state would be wholesale outsourcing of activities, perhaps even the risk management processes. What would the regulatory expectations be in response to this situation? Tighter controls? Tighter oversight? Similarly, how would institutions manage the risk exposure? Independent audits? Embedded teams? Definitely worth consideration and strategic analysis.

It will likely take a focused enterprise effort for financial institutions to fully develop third-party relationship management programs that are consistent with the framework provided by the OCC and the existing risk culture and enterprise risk management framework in the firm. However, as with the due diligence requirement, ignorance is not a defense, and institutions should be able to demonstrate to their regulators that they are evolving their third-party risk management framework, conducting effective and consistent risk assessments, ensuring effective challenge from the 2nd and 3rd lines, and effectively reporting on third-party risk to the board.

Starting Points:
A Path Forward

Clarify the current state of third-party risk exposure and management, for example:

- Define critical activities for the institution.
- Identify all existing and planned third-party relationships, noting whether they are subject to contract.
- Develop a matrix that includes each third-party relationship and prioritizes each one based on its relevance to the defined critical activities.
- Identify existing management and oversight of third-party relationships.
- Begin to map product and service process to identify the hand-off and/or entry points for third parties.
- Consider obtaining an independent review of certain critical activities to set a baseline for risk management processes.

Modify third-party risk management processes, as appropriate:

- Clarify oversight roles and responsibilities for board members and senior management.
- Clarify oversight roles and responsibilities for line functions.
- Evaluate contracts, and renegotiate as needed and if possible.
- Evaluate and strengthen monitoring, testing, and internal controls processes and reporting requirements for third parties involved in critical activities.
- Streamline third-party relationships as possible.

Contact us

Hugh Kelly
Principal, Bank Regulatory Risk
hckelly@kpmg.com

Philip Aquilino
Managing Director, Financial Services Regulatory
paquilino@kpmg.com

Pamela Martin
Managing Director, Americas' FS Regulatory Center of Excellence
pamelamartin@kpmg.com

Greg Matthews
Managing Director, Financial Services Regulatory
gmatthews1@kpmg.com

Contributions by:

Karen Staines
Associate Director, Americas' FS Regulatory Center of Excellence

Neerav Shah
Manager, Financial Services Regulatory

kpmg.com

About KPMG's Americas' FS Regulatory Center of Excellence

This point of view document is a publication of KPMG's Americas' FS Regulatory Center of Excellence. Additional articles and publications are available through the Global CoE web site. KPMG's Americas' FS Regulatory Center of Excellence is based in Washington, DC and comprised of key industry practitioners and regulatory advisers from across KPMG's global network. These individuals work with engagement teams and clients to provide insights into the implications of regulatory changes, distill the impact of regulatory developments on clients' businesses, and advise on how to adapt clients' business models to better thrive in this dynamic environment.