Everest Group

Managing Risk for Third-Party Relationships in Financial Services

Todd Hintze, Managing Partner
Marvin Newell, Managing Partner

Introduction

In late 2013, the Office of the Comptroller of the Currency (OCC) issued a bulletin "providing guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third party relationships."[1] This risk management guidance clarifies regulators' expectations regarding what banks are expected to do related to third-party risk management.

Discussions with Everest Group bank and service provider clients directly affected by these risk management expectations suggested a wide range of approaches to interpreting and implementing the OCC guidance.

Everest Group has synthesized a "market perspective" on how organizations perceive and manage these regulatory risk requirements as they relate to services delivered by third parties. This perspective included the requirements and implementation actions and plans with a representative sample of large and mid-sized (regional) banks, service providers with substantial financial services business, law firms with outsourcing and risk management practices, and regulatory agency staff. While these discussions focused on the risks associated with outsourced solutions, they also touched on activities delivered by offshore internal delivery centers.

Summary

From these interactions with the range of stakeholders, we synthesized the common themes that appear to be emerging as third-party relationship risk management programs evolve. This report summarizes those themes and provides some example illustrations of what some institutions are doing to strengthen their overall risk-management programs in the context of their third-party services portfolios.

Expansion of formal risk management for third parties is intended to drive better monitoring and decision making; it is not about "bright line" compliance. All stakeholders with whom we discussed risk management for third-party relationships acknowledged the growing importance of third parties in important activities to the bank and its customers. The regulators highlighted that the focus needs to be on risk management, not a "check the box" compliance exercise. Most also see the logical extension of more formal risk management programs' scope to encompass processes/services performed by organizations within the bank (whether onshore or offshore).

1 OCC Bulletin 2013-29

Large banks with well-developed service delivery centers have integrated comprehensive risk management into their sourcing and governance programs. Many large financial institutions have a sophisticated mix of third-party providers and internal service centers that support an array of operational and support processes. As these internal and external provider portfolios have evolved, these banks have established the governance approaches for managing this complex delivery model, including risk management processes. All noted continued evolution of their overall risk management program in general, and the third-party relationship risk management components in particular, to ensure they are taking prudent actions across the institution. Most continue to strengthen aspects of third-party risk management to assess and monitor potential risks (e.g., concentration risk) and risk mitigation steps within the context of their overall risk profile. These mature programs will likely continue to evolve as the banks adjust their business strategies and balance their service delivery portfolios.

Mid-tier banks often manage third-party risk at the transaction level; enterprise-wide risk programs focused on third-party service are slowly emerging. Many mid-size banks have sourcing programs that are only loosely integrated into an overall enterprise service delivery strategy. While each decision for a specific service may have the risks for that set of activities well documented with appropriate risk mitigation actions applied, we observe that many mid-size banks only recently are starting to consider how those individual vendor/process risks affect the enterprise-wide risk portfolio. These mid-size bank risk management programs are evolving quickly and should leverage the lessons learned from large financial services firms' efforts to manage enterprise risk related to third-party relationships.

Risk programs related to third-party relationships orient around four pillars:

- Defined risk appetite
- Risk segmentation
- Clear accountability alignment
- Robust risk management life cycle

Most banks apply a consistent set of risk management program principles aligned with these four pillars for third-party relationships. Defining the risk appetite for the bank is perhaps the most challenging area across financial services firms. All banks appear to have approaches for segmenting their risks so they can orient the most time and effort to the most critical activities. Organizational approaches are evolving to achieve the right alignment of roles, responsibilities and accountabilities. Additionally, most institutions have some sense of the risk management life cycle embedded in their programs. This will be explored in more depth below (see page 5).

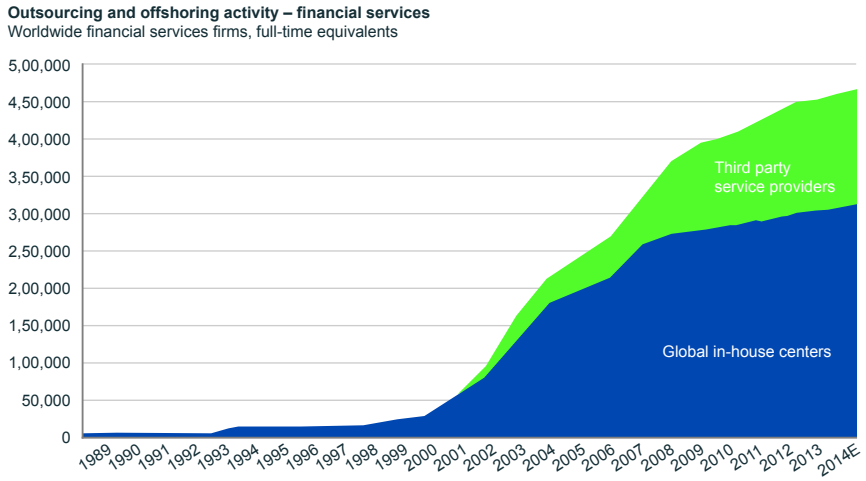
Emerging Pressure

The financial services industry worldwide has moved dramatically to take advantage of lower cost locations to deliver many important services. Over the past decade, the use of third-party service providers, most with offshore delivery models, has increased five-fold. This activity comes atop the continued growth of Global In-house Centers, or GICs. These captive subsidiaries are located in low cost, primarily offshore, locations.

EXHIBIT 1

Global financial services outsourcing & offshoring activity

Source: Everest Group analysis



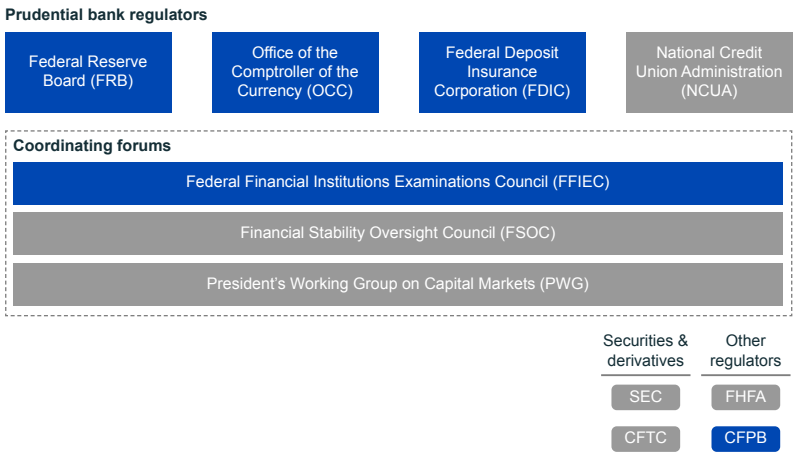
Given this migration of important services to third parties and remote locations, the need for rigorous risk management processes is obvious, and it is not surprising that the regulators are expecting banks to have strong programs in place.

The OCC has provided clear guidance on risk management for third-party relationships. Other major regulators, such as the Federal Reserve Board (FRB) and The Federal Deposit Insurance Corporation (FDIC), appear to be marching in step on the topic. Moreover, actions by the Federal Financial Institutions Examinations Council (FFIEC) demonstrate consistent follow-through directly with individual financial institutions in driving greater attention on the status and progress of third-party programs to manage risk related to third-party relationships.

EXHIBIT 2

U.S. regulatory landscape

Source: Regulator publications



The level of focus and information regulators are providing will position them not only to assess risk exposures and mitigation plans at an institution level, but also to assemble an overall industry view to enable an analysis of systemic risk from an aggregated third-party perspective. Such micro and macro views appear to support the overall objectives of the regulators, including the Financial Stability Oversight Council (FSOC).

Third-party Risk Management in Banking

Third-party risks are the potential risks that arise from financial institutions relying upon outside parties to perform services or activities on their behalf. The fundamental principle regarding banks' overarching responsibility for all activities, regardless of whether performed by a third party or internal resources, has been in place for many years. The OCC's recent clarification on risk management guidance, however, clarifies that such responsibility flows up to the Board of Directors of the bank. The board and senior management are ultimately responsible for managing activities conducted through third-party relationships as if the activities were handled within the institution itself.[2]

Third parties include all entities outside a bank's direct control that provide or perform services on the bank's behalf. These extend to third parties that perform functions on a bank's behalf, provide access to a bank's products and services, market the bank's processes and activities, utilize the bank's charter or legal authority, and perform monitoring and/or audit functions of processes, services, etc. The intent of these services may include helping the bank achieve its strategic objectives through increasing revenue, reducing cost or expanding the customer base, as well as enhancing competitiveness, providing diversification and strengthening the soundness and compliance management system.

A bank can outsource a task, but it cannot outsource the responsibility.

Within this overall framework of third-party services is a focus on critical services, including those that:

- Could significantly impact customers
- Require significant investment to implement the relationship and manage the risks
- Impose significant risk to the bank if the third party fails to meet expectations
- Would have a major impact on bank operations if the bank has to find an alternative or bring services in-house.

Examples of these services may include payments, clearing, settlements and information technology.

2 Financial Institution Letter 4-2008 "guidance for Managing Third-Party Risk"

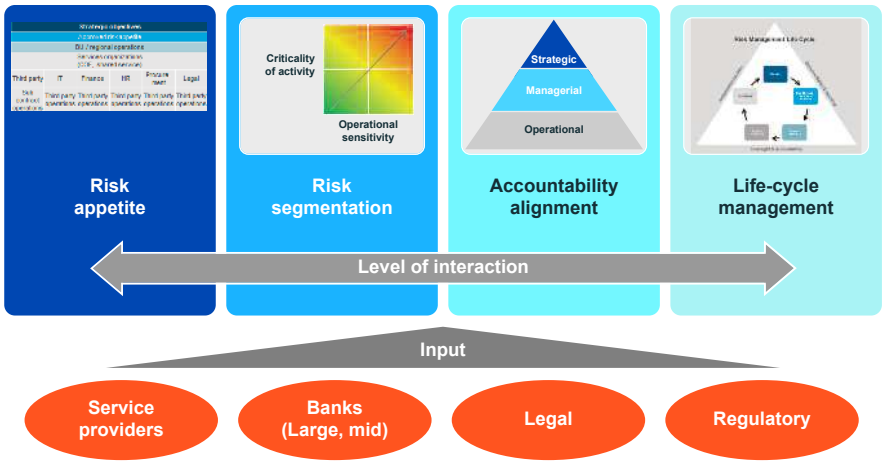
The "Four Pillars" of Third-party Risk Programs

As mentioned briefly on page 2, Everest Group discussions with stakeholders across the industry suggest many levels of maturity and approaches of banks' third-party risk management programs. However, nearly all initiatives across both large and mid-sized banks shared four common pillars as the banks' leadership structured their risk managed programs and the organizations to implement them (Exhibit 3).

EXHIBIT 3

Third-party risk management program themes

Source: Industry interviews, Everest Group analysis



Banks with more mature third-party risk management efforts have program components supported by specific processes that address each of these pillars. Those with emerging programs recognize these elements must play a key role in their activities. Most banks have action plans to address them in the near term.

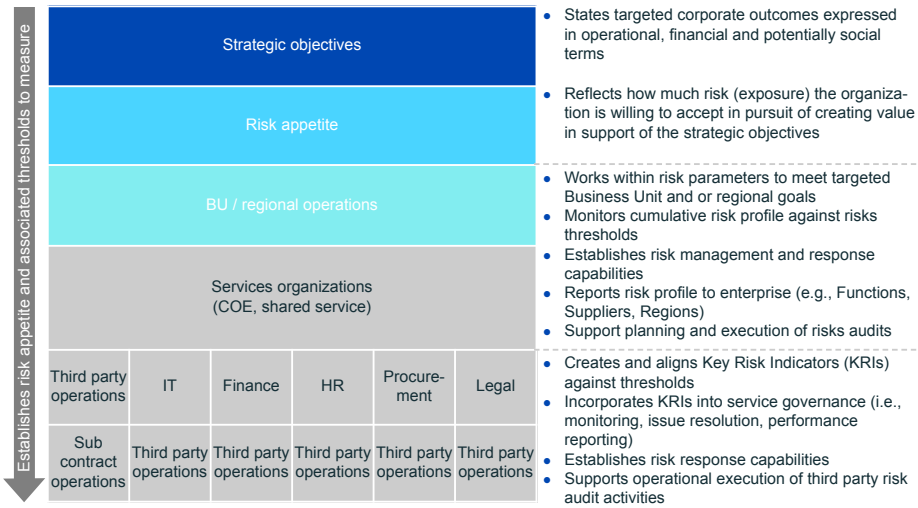
Risk appetite

A fundamental principle for managing third-party relationship risk is that it must link directly to the overall risk appetite of the financial institution. Most banks, however, gauge defining their risk appetite as one of the most challenging activities as they continue to evolve their risk management programs. The third-party relationship component is not an exception to this challenge.

EXHIBIT 4

Developing the risk agenda

Source: Industry interviews, Everest Group analysis



The strongest approaches begin with a clear tie to the overall strategy of the bank. These strategic objectives inform the priorities and targeted outcomes, often expressed in operational terms, financial expectations, and, potentially, social goals.

Overall risk – risk mitigation = residual risk

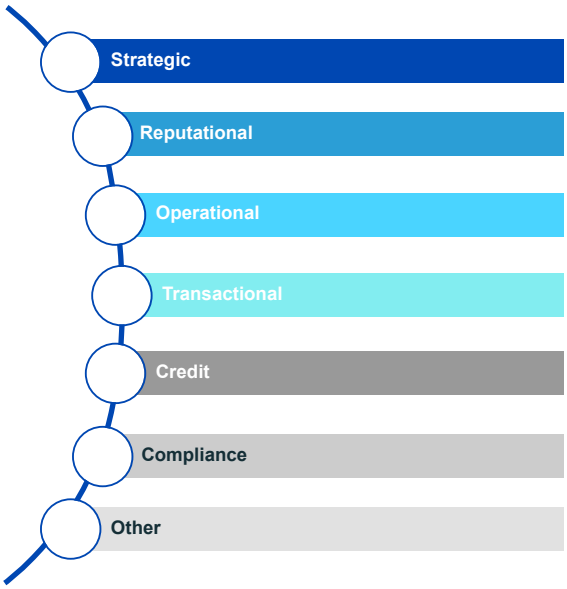
The risk appetite quantifies how much risk (i.e., exposure) the organization is willing to accept as it drives the business to achieve its strategic objectives. This risk appetite needs to cascade down to the business unit and functional operations, where the cumulative risk profile can be monitored against unit-specific risk thresholds. The risk management and response capabilities emerge from these activities and define reporting requirements across the enterprise (e.g., functions, service providers, geographies). This approach also supports planning and execution of risk-related audits.

At the services organization levels, whether internal or external, the risk management program requirements establish the Key Risk Indicators (KRIs) that provide the metrics for tracking against specific thresholds. KRIs are frequently integrated into service governance that specifies monitoring, issue resolution and performance reporting requirements. Moreover, this level builds and maintains the risk response capabilities.

The risk appetite and associated program activities at each level of the organization are oriented to assess and manage risks of different types (Exhibit 5).

EXHIBIT 5

Managing different types of risk



Source: Regulatory publications, Everest Group analysis

The interplay of how each risk may affect exposures and sensitivity of other risks is core to the development of the risk appetite. For example, a risk event that might fundamentally affect a mid-size bank's reputation creates strategic implications at the enterprise level; the same event for a large bank, which services different customer segments and can absorb different levels of exposure, may have little strategic impact.

The risk appetite also reflects a bank's ability to mitigate overall risks, resulting in "residual risk." For example, a bank's risk response plans and sourcing strategy might include relationships with more than one vendor for a type of service and/or service delivery locations in multiple geographies. Such plans or strategies may also provide strong capabilities to respond effectively to risk events, thus reducing residual risk. Such plans or strategies may create the concept of risk "credits" that enable different options for services throughout the bank's portfolio of services delivered by third parties or the bank's in-house operations.

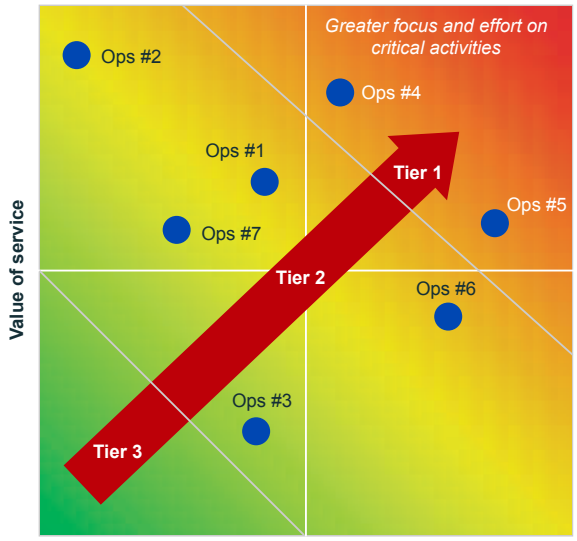
Risk segmentation

An explicit element included in the risk management guidance from regulators is risk segmentation. The concept focuses a bank's attention and resources on the most critical processes. Different banks take distinctive approaches to their segmentation. Most, however, recognized criteria that reflects the importance or value of the service and at least some dimensions of operational sensitivity. These include the probability of a risk event's occurrence, the speed with which a risk event may happen or adversely affect the bank, and the scope/breadth of potential impact.

EXHIBIT 6

Segmenting risks

Source: Interviews, Everest Group analysis



Regulators' perspectives on risk include both **institution-specific** and **systemic risk** arising from risk concentration. Specific guidance focuses on institution-specific third-party risk management that puts banks on a path to consider explicit contingency plans for risk responses, for critical services that a single vendor delivers. It also extends to services within a geographic region and/or for services delivered by a single vendor to multiple banks as well as for overall market concentration of critical services among only a few vendors. Some stakeholders suggest that regulatory agencies may eventually consider systemic risk exposures in future policy-making as they aggregate third-party services data from individual banks.

Most banks' segmentation results in several tiers of services. Almost all banks interviewed articulated three major segments:

- Tier 1 services (or vendors) are critical activities that warrant individual focus and dedicated resources to assess and manage risks, including specific actionable plans for key risk exposures
- Tier 2 services are typically those activities with lesser-value exposure and operational sensitivity. These services require moderate time, attention and resources
- Tier 3 services are low-risk activities, which may be managed as a group or on an exception-basis only

Most banks use an annual process to validate their risk segmentation and assess concentration risk (by geography, function, service provider, etc.) with the criticality of the services aligned with the bank's evolving strategic.

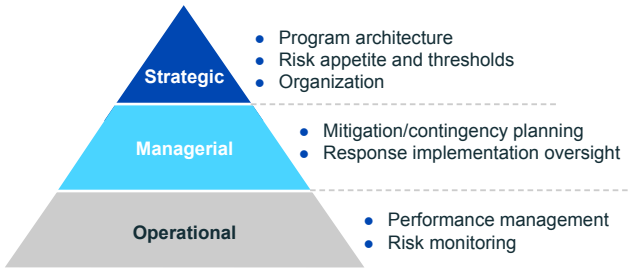
Accountability alignment

> "It is about managing risk, not "check the box" compliance…
> *– Regulatory agency staff*"

Most third-party risk management programs observed had elements that defined responsibility and accountability at different levels of authority. Senior leadership and the Board of Directors oversee strategic activities driving overall program architecture, establishing the bank's risk appetite and thresholds, and ensuring the organization is in place to execute the risk management program. Such program architecture and organization help ensure safeguards are in place and executed via independent review and audits of processes and procedures. Such an approach sets the stage for effective management of risks related to third-party relationships.

EXHIBIT 7

Aligning accountability



Source: Industry interviews, Everest Group analysis

At the managerial level, core responsibilities include development of the risk mitigation plans and actions that must occur in the case of a risk event. Leaders at this level also oversee the implementation of these plans as needed.

Performance management and risk monitoring typically occur at the operational level. Reporting cascades upward on the overall Key Risk Indicators and aggregate risk metrics. Exceptions are highlighted on a case-by-case basis.

Life cycle management

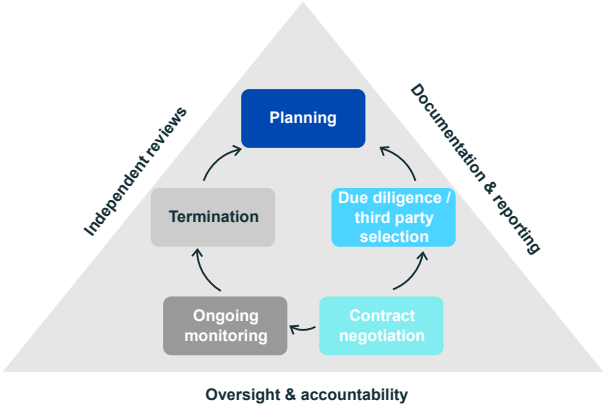
A clear expectation from regulators is that a financial institution will manage

risks across the life cycle of its third-party relationships. The regulators have not suggested adoption of a uniform set of rules from which to govern, but have provided guidance in adopting risk management processes **commensurate with the level of risk and complexity** of a bank's third-party relationships. The OCC has outlined a life cycle highlighting essential activities for documentation and reporting; independent reviews and clear oversight and responsibility are inherent at each stage.

EXHIBIT 8

Managing the risk management life cycle

Source: OCC Bulletin 2013-29



The planning activities within the bank's risk-management program differ by service type. These efforts are straightforward for commodity services. More complex and fluid partnership models are difficult to plan to the required level of certainty (e.g., financial benefit, volume of activity, delivery model, on-off shore mixture, security implications), making the incorporation of next generation services models (e.g., cloud computing services) challenging for many enterprises. Risk-planning activities are typically incorporated into demand allocation processes (e.g., assessment, prioritization, allocation). Proactive, rigorous reporting on risk-related dimensions is emerging as a prerequisite for stronger risk management programs. Many mid-sized banks are early in establishing the organizational infrastructure to sustain ongoing risk-management processes.

For vendors serving financial institutions, the third-party risk-management planning process is largely opaque for net new services. For the continuation and/or expansion of existing services, the traditional planning topics are typically well covered. However, there is little visibility into how a (customer) bank will assess third-party solutions relative to risk.

The next stage in the risk-management life cycle spans the selection of third-party service providers and the due diligence associated with that selection process. For most large financial institutions, existing procurement and sourcing practices typically examine the 22 due diligence categories[3] identified by the OCC. Due diligence is relatively straightforward with large, mature service providers of information technology and business process

3 OCC Bulletin 2013-29, Strategy and Goals, Legal and Regulatory Compliance, Financial Condition, Business Experience and Reputation, Fee Structure and Incentives, Qualifications, Backgrounds, Reputation of Company Principals, Risks Management Information Security, Management of Information Systems, Resilience, Incident-Reporting and Management Programs, Physical Security, Human Resource Management, Reliance on Subcontractors, Insurance Coverage, Conflicting Contractual Arrangements.

outsourcing services; it is much more difficult with smaller, niche service providers and many software/cloud services providers whose multi-tenant models create challenging issues.

During most procurement processes, the service providers initially request that the banks define regulatory compliance requirements, citing their discomfort with interpreting those requirements in the context of the specific bank. The degree to which banks push back to require the vendors to understand and assume appropriate responsibility for their part in the compliance chain differs widely by the process involved. For many of the critical services that are mature in terms of outsourcing, the service providers generally are capable and have a deep understanding of what in the end are "table stakes" for being in the business. Vendors that provide solutions that involve a shared delivery model (e.g., software-as-a-service firms, some software providers) may resist due diligence requests related to physical resilience, citing the nature of their shared delivery that prevents accurate assessments.

The contract negotiations stage of the life cycle presents unique challenges and opportunities to reduce residual risk for the bank. For most financial institutions, existing sourcing practices incorporate the contract categories[4] identified by the OCC. In general, banks can achieve their desired outcomes for indemnification, liability, termination assistance and/or calibrate them for "commensurate" risks. The nature of smaller, niche service providers and next-generation services, such as cloud infrastructure services, makes it harder for many banks to achieve their desired contract terms. Moreover, the emphasis on oversight responsibilities of the Board of Directors for third-party relationship risk often makes Board approval a logistical burden for many banks.

Established service providers familiar with delivering services to the financial services sector typically can find acceptable negotiated solutions to contract terms on the OCC's list. However, vendors struggle to accept time and frequency requirements of yet another full set of potential supervision/audits related to third-party risk management activities that may be driven directly by the customer or by other external parties/regulatory bodies.

Once the risk-management plan is in place, the third-party service provider is selected and thoroughly vetted, appropriate contractual arrangements are finalized, and the provider commences operations, risk management turns to management, continuous monitoring and assessment. Our experience in the global services/outsourcing arena suggests that the buying organization often lacks the strong governance resources and processes to effectively monitor the breadth of due diligence categories in an ongoing manner. The bank's sourcing and procurement organizations typically monitor the categories at

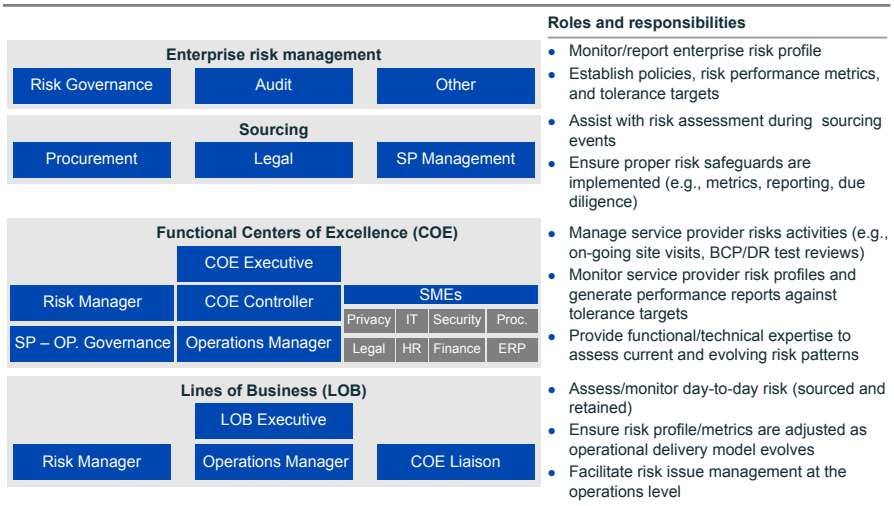
4 OCC Bulletin 2013-29, Nature and Scope, Performance Measures or Benchmarks, Responsibilities for Providing, Receiving, and Retaining Information, Right to Audit and Require Remediation, Compliance with Applicable Laws and Regulations, Cost and Compensation, Ownership and License, Confidentiality and Integrity, Business Resumption and Contingency Plans, Indemnification, Insurance, Dispute Resolution, Limits on Liability, Default and Termination, Customer Complaints, Subcontracting, Foreign-Based Third Parties, OCC Supervision.

the enterprise level but have only recently begun to drill down to track key metrics at the process and sub-process level. This is particularly true for mid-size banks. Such monitoring is complicated by gaps in service performance platforms, which often lack the capability to track/record additional categories. However, most banks do adapt their issue identification and escalation processes to facilitate prioritization of issues related to risk management.

EXHIBIT 9

Organizing to support third party relationship risk management

Source: Industry interviews, Everest Group analysis



Banks are also organizing to reflect the accountability alignment discussed above (Exhibit 9). The roles and responsibilities cascade from the direction-setting and oversight at the senior-most levels to risk assessment and monitoring activities at the function and line of business levels.

From a service provider point of view, beyond service levels and fees management (i.e., invoices/credits), service providers often lack an integrated method for retrieving and publishing reports against the core risks categories (KPIs). While they often seek to define the level of detail, and frequency of reporting for non-core categories, doing so with banks has been problematic and undercuts some of the fundamental risk-management principles. Recognizing this, several large service providers are developing specific service lines to address this "opportunity."

The final element of the risk-management life cycle is termination. Our experience suggests that most banks' sourcing processes do not include a detailed termination plan (i.e., alternative service plan) that some interpretations of regulatory guidance would lead one to infer should be in place for important services. Even if one exists, governance activities do not currently focus on maintaining the integrity/currency of the termination plan over the course of the contract term. However, termination rights are generally well-defined in most service provider agreements. Only the largest banks generally have the scale to maintain relationships with multiple service providers for important services to provide "step-in" capability.

Service providers have different challenges in this area. They struggle to understand the potential exposure (i.e., costs) of termination assistance.

Since plans should adapt to the changing market and customer requirements over time, no prudent vendor would sign up for open-ended obligations. However, some termination-related activities, such as handling joint intellectual capital, system connections and access controls, appear to be well understood and generally agreed upon from the outset of a relationship.

Implications for Stakeholders

As financial institutions of all sizes continue to evolve their approaches to managing risks related to third-party relationships, several important action themes should be considered in the near to medium term:

- *Adapt existing governance processes to support more explicit risk assessment and monitoring activities across each risk-management element.* We anticipate that this will involve creating an integrated governance/risk organization. Leadership will need to ensure that this organization possesses strong capability to assess and periodically monitor risk throughout the life cycle as described above. Moreover, senior management (or the Board) should consider chartering this organization to evaluate areas of risk beyond traditional factors. For example, some critical activities may warrant much more granular tracking of concentration risk. Exhibit 10 illustrates that a bank's aggregated concentration, by geographic region in this example, may not accurately describe exposures when services are examined by process and subprocess. This does not necessarily mean a different sourcing approach should be taken. It does suggest that KRIs around those more concentrated subprocesses would be prudent.

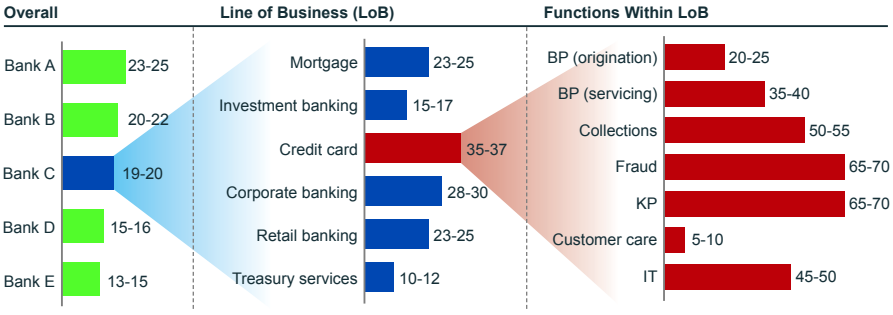
EXHIBIT 10

Managing concentration risk

Source: Everest Group analysis

LEADING FINANCIAL SERVICES FIRMS

Offshore penetration in India[1]
2013; Percentage



1 Defined as ratio of offshore headcount in India to the global headcount in the bank

The integrated governance/risk organization should also reflect the need for independent review mechanisms

- *Develop and integrate actionable termination planning (contingency planning) activities into the sourcing approach.* Some banks interpreted OCC guidance as suggesting the bank should have detailed, actionable plans for termination that ensure continuity of critical services. Most banks will likely evolve toward development of explicit termination-scenario planning with

action plans analogous to business continuity strategies already in place for such areas as information technology. Extending the planning aspects to incorporate similar rigor for third-party relationships at termination (for whatever reason) appears to make sense and is a modest investment to substantially reduce residual risk

- *Consider risk mitigation approach requirements for select new services.* Our 360-degree perspective on the global services market clearly reveals increasing adoption of next generation "as-a-Service" solutions, such as:
  - Software-as-a-Service
  - Infrastructure-as-a-Service
  - Business Process-as-a-Service

  The robust standardization of proven processes that these services can provide may reduce risk along many dimensions, but also may create different challenges along others. At the core of these services' value proposition is leverage of approaches in a delivery model that is shared with other customers. Use of these services to achieve lower cost and other service benefits (e.g., flexibility, faster time-to-market, etc.) requires the bank to adapt its processes to fit what the vendor is providing

- *Determine how to incorporate risk exposures of in-house operations into integrated internal/third-party services portfolio.* As regulators have widened the discussion of third-party risk management, the question not directly addressed revolves around a similar proactive, rigorous risk-management approach for services delivered by internal resources. As **Exhibit 1** illustrated, many banks (mostly large) have complex networks of service delivery by internal resources from locations across the globe. Those remote operations present many of the same issues highlighted for third-party relationships. Additionally, operations within the U.S. also have embedded challenges ranging from talent management issues (e.g., aging workforces expose many bank processes to loss of critical knowledge and challenges maintaining qualified staff) to cyber security requirements to concentration risks. While control and visibility of internal service delivery should be easier, our experience suggests that many institutions have gaps in documentation, governance, and other areas across the risk-management life cycle for these internal operations

Conclusion

The Office of the Comptroller of the Currency's guidance regarding its expectations surrounding assessment and management of risks associated with third-party relationships provides a backdrop for addressing risk in the banking sector. That leaves national banks, federal savings associations and other financial services enterprises to establish risk-management approaches befitting their unique situations relative to their perception of inherent risks and in accordance with regulatory risk-management expectations. By working closely with third-party solution providers, enterprises can address risk, mitigate potential outcomes, and ensure the outsourced solutions are in line with the organization's risk needs and cost constraints across the life cycle of the engagement, while also adhering to regulatory expectations.

About Everest Group

Everest Group is an advisor to business leaders on next generation of global services with a worldwide reputation for helping Global 1000 firms dramatically improve their performance by optimizing their back- and middle-office business services. With a fact-based approach driving outcomes, Everest Group counsels organizations with complex challenges related to the use and delivery of global services in their pursuits to balance short-term needs with long-term goals. Through its practical consulting, original research and industry resource services, Everest Group helps clients maximize value from delivery strategies, talent and sourcing models, technologies and management approaches. Established in 1991, Everest Group serves users of global services, providers of services, country organizations, and private equity firms, in six continents across all industry categories. For more information, please visit www.everestgrp.com and research.everestgrp.com.

For more information about Everest Group, please contact:
+1-214-451-3000
info@everestgrp.com

For more information about this topic please contact the author(s):

Todd Hintze, Managing Partner
todd.hintze@everestgrp.com

Marvin Newell, Managing Partner
marvin.newell@everestgrp.com