Deloitte.

Managing third-party risk in financial services

Key considerations for the extended enterprise

Executive Summary

Increasingly viewed as a strategic imperative in financial services, extending the enterprise via the use of third parties has allowed companies to focus on core competencies, pursue growth and innovation, improve time to market, and reduce costs. After 10-plus years of inconsistently managing this exposure, and now in response to both a greater awareness of risk and heightened regulatory scrutiny of third-party relationships, financial services institutions should feel pressure to transform their risk-management capabilities.

Strong risk management across the extended enterprise can be best achieved by embedding third-party risk management (TPRM) capabilities firmly into the fabric of the business and its operations. Institutions that perform TPRM well should benefit by reducing risk and increasing agility and resiliency—enabling them to pursue growth while also reducing areas of vulnerability.

To that end, this paper presents a road map to help institutions elevate their TPRM capabilities:

- **Understand the institution's third-party landscape and level of risk.** Management should assemble an inventory of active third parties and associated engagements, conduct an inherent risk analysis of each (including how important each engagement is to the business/value chain), and assess the institution's aggregate risk position for a given third party.

- **Drive risk management attention to the highest risk relationships.** Management should identify processes that are core/critical to the institution's value chain, and then focus risk management investments and resources on the third parties supporting those processes.

- **Engage the board and senior management for the most critical and highest risk relationships.** The board and senior management should determine the risk posture and define what can or cannot be outsourced. They should identify, validate, and oversee the third-party relationships that support the institution's most critical processes and capabilities.

- **Drive accountability into the business line and beyond.** Ultimate accountability for managing individual third-party relationships and associated risks should reside in the line of business and be built into the fabric of management processes and operations.

- **Enable end-to-end risk and control management through standards, procedures, and technology enablement.** Management should drive risk assessments and controls across the complete life cycle of the third-party relationship, including pre-contract assessment, contract execution, and ongoing monitoring post-contract execution.

- **Incorporate sustainability and continual improvement into your capabilities.** Organizations should design processes to routinely evaluate the effectiveness of their TPRM programs and controls, including rigorous event analysis, quality assurance, and independent reviews.

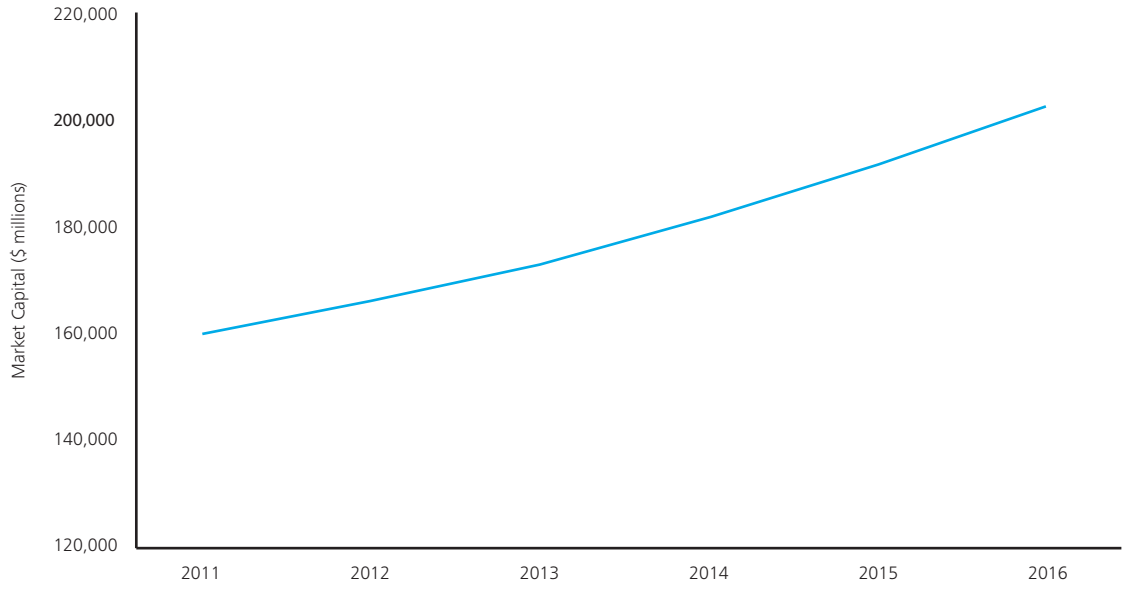
Managing third-party risk in financial services
Key considerations for the extended enterprise

Why third-party relationships are proliferating—along with risks

There are many reasons why financial services institutions leverage third parties. Third parties—whether traditional vendors, business partners, or inter-affiliates—often reduce time to market, lower service delivery costs, and improve customer experiences. An extended enterprise can allow a company to access specialized talent not available in-house, driving product or service innovation. The use of third parties can also help an institution better focus on its core capabilities.

Not surprisingly, the engagement of third-party providers has exploded over the past 20-plus years. For example, fueled by competitive pressures, information technology and business services outsourcing in US banking and financial services is expected to mushroom by more than 25 percent between 2011 and 2016.[i] (See **Figure 1.**)

Figure 1: US banking and financial services outsourcing market



*2011 Actuals, 2012-2016 forecast based on projected 5.2% CAGR

Source: HfS Research, Ltd., January 2013

While there are many benefits for using third parties, there are also added risks. Reliance on an extended enterprise exposes financial institutions to the risk of other companies' management and infrastructure. It increases the complexity of risk management, as it's inherently difficult to understand the third party's "black-box" inner workings. And it introduces different types of risks to which the institution may not have been previously exposed, such as concentration risk, location risk, or legal/jurisdiction risk.

Weighing the inside/outside decision

It's a question many institutions face: Should they engage third parties for certain business activities, or perform these activities themselves? In our view, such considerations shouldn't be taken lightly, as they carry implications that reach to the core of the enterprise and can pose significant risks.

When weighing this decision, companies should consider the following issues:

- Business justification for using a third party
- Significance of the activity to the institution
- Level of risk and exposure
- Cost and complexity of oversight and control
- Longer term organizational implications (e.g., loss of capabilities over time).

Ideally, senior management should identify which business capabilities should be kept in house and which could be handled by third parties.

In turn, these risks drive a unique set of potential impacts. Examples include:

- **Financial reporting errors/monetary losses** arising from a third-party service provider approving processing transactions on the institution's behalf (e.g., financial records reconciliation), because the outsourcing institution did not validate or test the provider's internal controls

- **Regulatory fines/penalties** resulting from non-compliance with new consumer protection laws by a third party that is marketing add-on products to credit-card customers

- **Breaches of sensitive customer data** due to weak security controls at a third party that is performing processing on behalf of a financial services institution

- **Service disruptions** caused by an earthquake or natural disaster in a city supporting multiple third-party suppliers on which the outsourcing institution has a high business dependency (e.g., multiple customer call centers or processing centers)

- **Non-compliance with regulatory requirements** to maintain customer records caused by the bankruptcy of a third-party record keeper/archivist.

A strong TPRM program can help institutions manage inherent risks in the use of third parties. (See **Figure 2**.)

Not all these risks are necessarily applicable to a given third-party relationship. For example, if an institution does not share confidential or restricted information with a third party, then information security risk is significantly reduced.

In addition, the assessment of risk may be conducted at the company level or at a contract or engagement level. An institution that has multiple engagements with one third party might only conduct one assessment of the third party's financial viability or geopolitical risk. However, it may need to conduct multiple information security assessments—one for each engagement—where project-specific information security risks are introduced.

Figure 2: What's putting you at risk?

Inherent Risks in the Use of Third Parties	
Strategic Risk	Risk of inappropriate sourcing decisions by the financial services institution due to a lack of third-party alignment with the institution's business strategies and objectives
Contractual Risk	Risk that the institution does not receive products/services in line with expectations due to incomplete or inadequate third-party contract provisions, or a third party's inability to meet contract terms and conditions
Reputation Risk	Risk of brand damage to the institution due to a third party's inability to meet the institution's expectations
Financial Viability Risk	Risk of disruption to the institution's operations due to a third party no longer being able to provide products/services as it's unable to generate profit or maintain necessary capital for supporting its ongoing operations
Credit Risk	Risk of a financial loss to the institution that arises when credit exposure is caused by a third party holding, settling, or collecting the institution's funds; or issuing a guarantee to the institution; or creating a liability for the institution that is not adequately managed
Compliance/Legal Risk	Risk that the institution is not in compliance with laws, ethical standards, or its own policies/standards/procedures because a third party does not have adequate compliance management processes/controls over its products/services/systems
Information Security Risk	Risk of inappropriate disclosure, corruption, or destruction of the institution's information due to a third party's failure to provide appropriate security and privacy controls over the institution's information
Continuity of Service/Product Risk	Risk of the institution's operations being disrupted by the ineffectiveness of a third party's business continuity program, or by the third party's inability to provide services to the institution for an extended period of time
Transactional/Operational Risk	Risk of a financial loss to the institution and/or an adverse impact to the institution's product/service delivery due to inadequacies in a third party's internal processes/people/systems and/or other third-party issues
Geopolitical Risk	Risk of disruption to the institution's operations due to economic, social, and political conditions and events in a country that may adversely affect a third party's operations or viability

Source: Deloitte Development LLC, following guidance provided by the US Office of the Comptroller of the Currency (OCC), the Federal Financial Institutions Examination Council (FFIEC), and the Federal Reserve Board (FRB).

Increasing pressure from new regulatory requirements worldwide

Heightened global expectations about the ways financial services institutions conduct their business can be attributed to increasing global scrutiny from regulating authorities. In short, regulators are paying much closer attention and are employing broader powers to curb activities they deem to be too risky for institutions to engage in.

In the United States, The Office of the Comptroller of the Currency and the Federal Reserve Board issued revised guidance in late 2013 on risk management of third parties.[ii] Key themes include:

- **Board of directors and senior management oversight:** Specifically holding boards of directors, senior management, and relationship managers accountable and responsible for managing third parties
- **Risk-based approach:** Inventorying and assessing the risk of all third parties, with additional focus on third parties supporting critical activities
- **End-to-end risk management:** Formalizing risk-management processes throughout the relationship life cycle and across all risk domains, and documenting them in a management plan
- **Proactive risk management and enhanced due diligence:** Expanding pre-contract phases (e.g., planning, due diligence) to influence contracting and ongoing monitoring
- **Independent reviews:** Conducting independent reviews of the end-to-end risk-management program and critical third-party controls (i.e., by an independent third party)
- **Incentive compensation reviews:** Requiring management to consider the potential impact of incentive-based compensation on the third party's behavior.

Comparison of key terms

To demonstrate heightened interest in TPRM among US regulating authorities, it's instructive to compare the word count of certain key terms emphasized within OCC Bulletin 2013-29 with its previous (and now rescinded) guidance in OCC Bulletin 2001-47.

Figure 3: Word count of key terms in current and prior OCC Bulletins

Term	2001-47	2013-29
Critical activities	0	27
Board (of directors)	11	22
Customer complaints	2	8
Compliance	16	40
Independent	5	17
Subcontract	4	34
Contract/contracting	31	64

Source: Deloitte Development LLC

Of course, the focus on third parties is not solely a US issue. Regulators around the world are driving attention to this topic. Some highlights:

- **United Kingdom:** The Prudential Regulation Authority (PRA) has stated that "a firm cannot contract out its regulatory obligations and should take **reasonable care** to supervise the discharge of outsourced functions."[iii]

- **Singapore:** The Monetary Authority of Singapore (MAS) has stated that it "is particularly interested in **material outsourcing** which, if disrupted, has the potential to **significantly impact** an institution's business operations, reputation or profitability and which may have systemic implications."[iv]

- **Australia:** The Australian Prudential Regulatory Authority (APRA) aims to ensure that all outsourcing arrangements involving **material business activities** entered into by a regulated institution are subject to appropriate **due diligence, approval, and ongoing monitoring**.[v]

- **Hong Kong:** The Hong Kong Monetary Authority (HKMA) states that institutions "should not enter into, or continue, any outsourcing arrangements [that] may result in their **internal control systems or business conduct being compromised or weakened** after the activity has been outsourced."[vi]

While US and global regulatory guidance on TPRM is significant, it's important for institutions to balance these requirements against how they want to operate. Rather than implementing the regulations line-item by line-item, institutions should reassess their overarching risk tolerance for third parties. For example, an institution may want to reduce the amount of third-party exposure to its customers rather than build extensive assessments and controls to monitor these types of third-party interactions.

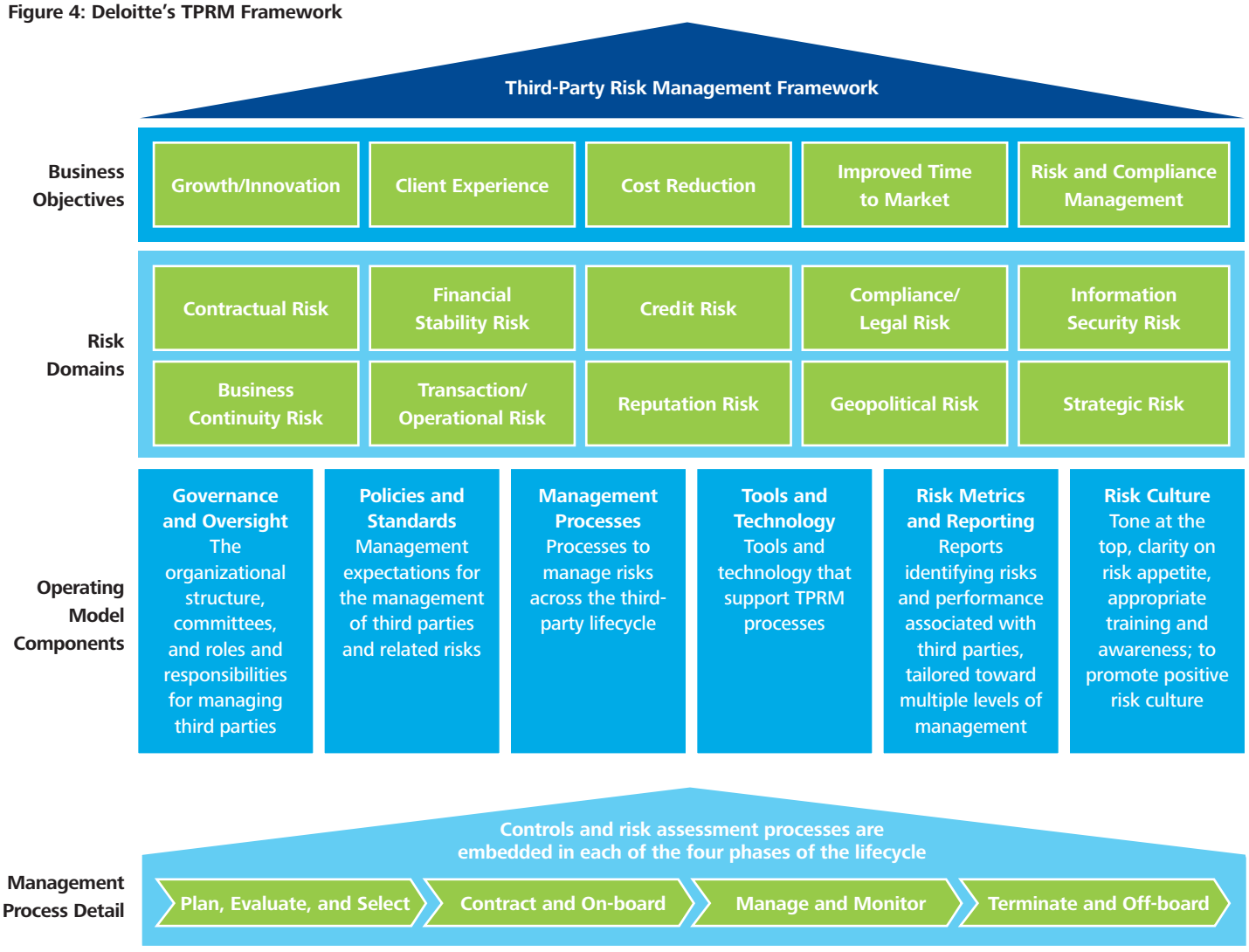
Deloitte's third-party risk management framework

Properly considered, TPRM is an extension of operational risk. Operational risk is the possibility of loss resulting from inadequate or failed internal processes, people, and systems, or potential loss stemming from external events. TPRM provides management with the discipline and capability to mitigate operational risk.

To help boards and senior management in this area, Deloitte has developed a comprehensive TPRM framework, shown in **Figure 4**. The framework is intended to guide management's thinking for designing a structured approach for third-party risk management, including aspects of the business objectives for using third parties; the associated risks of using third parties; the required operating model components for end-to-end risk management; and detailed management processes for enabling a sustainable, effective program. Like many other risk domains, TPRM requires enterprise-wide accountability, including support from the business, as well as procurement, legal, risk management, information technology, compliance, and other functions.

Although TPRM programs will differ for each institution, there is a common goal: to consistently and effectively evaluate and monitor third-party performance and risk. This requires good governance, as well as contributions from multiple business areas. In our view, effective financial services companies extend compliance and risk-management programs to their supply chains and third-party relationships—leveraging compliance as an engine for creating and preserving organizational value.

Figure 4: Deloitte's TPRM Framework



Keys to successful third-party risk management

Most large financial institutions expect that regulators will soon ask them to demonstrate their TPRM capabilities against recently issued OCC and Federal Reserve Board (FRB) guidance. Specifically, OCC Bulletin 2013-29, released on October 30, 2013, redefined the scope of the financial services institution's risk-management responsibilities to include any business relationship between the institution and another entity, including affiliate relationships.[vii] Shortly following this release, the FRB issued regulatory guidance that raises the bar for institutions to treat TPRM as a formal, enterprise-wide risk discipline, and to follow a process that is commensurate with the level of risk and complexity of the given activity.[viii]

To help boards and senior management teams prepare for the eventuality of enhanced regulatory scrutiny of their TPRM programs, we have identified the following essential capabilities that institutions should cultivate.

- **Understand the institution's third-party landscape and level of risk.** Management should assemble an inventory of active third parties and associated engagements, conduct an inherent risk analysis of each (including how important each engagement is to the business/value chain), and assess the institution's aggregate risk position for a given third party. Determining which third-party engagements are critical to the institution's success is not simply based on the dollar value of the contract; the operational risks the third party could pose to the company must be considered as well. Inventories should include all types of third parties—including suppliers, outsourced service providers, joint ventures, and inter-affiliate services—and they should be organized by standard service categories or taxonomies to enable further customization of risk-management practices.

- **Drive risk management attention to the highest risk relationships.** Once management has identified third parties that are core/critical to the institution's value chain, it should focus risk management investments (e.g., oversight through quality, performance, and capacity reviews) and resources on those third parties. More advanced institutions will prioritize scarce time and resources on managing the highest risk third parties and will perform more frequent and in-depth assessments (or controls testing) to a zero-defects level.

- **Engage the board and senior management for the most critical and highest risk relationships.** The board and senior management should determine the risk posture and define what can or cannot be outsourced or supported by a third party. Senior management should identify, validate, and oversee the third-party relationships that support the institution's most critical processes and capabilities. They should understand the types of third-party failures that would create significant brand risk or reputational damage—whether those failures arise internally or at the third party.

- **Drive accountability into the business line and beyond.** Ultimate accountability for managing individual third-party relationships and associated risks should reside in the line of business and be built into the fabric of management processes and operations. While regulators look for evidence of consistent and repeatable governance processes at the highest level, they also expect risk to be managed by those who should understand it best. As part of the structured three lines of defense model, an independent risk capability, along with internal audit, should be in place to objectively assess the adequacy of the line of business oversight of third parties.[ix]

- **Enable end-to-end risk and control management through standards, procedures, and technology enablement.** Management should design risk assessments and controls across the complete life cycle of the third-party relationship, including pre-contract assessment, contract execution, and post-contract monitoring. To further drive effectiveness of these risk-management processes, we recommend that the institution's TPRM capabilities and processes be fully integrated with its operational risk program and governance.

- **Incorporate sustainability and continual improvement into your capabilities.** Organizations should design processes to routinely evaluate the effectiveness of the third-party risk management program and controls, including rigorous event analysis, quality assurance, and independent reviews. Institutions that sample, test, and improve their TPRM processes and controls are better positioned to weather future risk events and take advantage of growth opportunities. An occasional re-evaluation of the portfolio of third-party risk will help prevent institutions from being subject to inappropriate exposures.

As companies consider implementing or enhancing their third-party risk management programs, they should prioritize which capabilities to address. Factors to consider may include:

- **Level of exposure:** What is the level of exposure if the risk assessment is not performed or if the control is not implemented? Capabilities, such as sanctions screening, to address key exposures should be given higher priority

- **Current process maturity:** What's the maturity level of the current risk assessment or control—for example, is it optimized, standardized, ad hoc, or not yet developed? Current mature capabilities should become more consistent and automated. Immature processes could be implemented at an elementary level and matured over time.

- **Process complexity:** What's the complexity of the process or control, and what resources or investments are required to implement it? Low-complexity, high-impact processes should be given more attention.

- **Foundational versus emerging capabilities:** How does the institution compare with its peers and regulatory expectations for risk assessment and control? For example, information security reviews, financial viability assessments, and background screening are generally considered a foundational capability. Institutions should focus on them before developing emerging capabilities, such as geographic concentration risk assessments.

TPRM: The new risk domain

Given growing regulatory interest, the industry's realization that TPRM is important to operational safety and soundness, and the market pressures that continue to drive the use of third parties, TPRM has emerged as a critical topic in financial services. The risks are real, and TPRM is now considered a new risk domain within operational risk.

It will require significant attention of senior leadership and a commitment of investment to enhance and mature most institutions' end-to-end risk management capabilities to a level that is commensurate with their level of risk and exposure. Institutions should advance their capabilities not only by addressing the regulatory requirements but also by taking a thoughtful approach to developing practical, cost-effective, and sustainable solutions. Better risk management of the extended enterprise ultimately raises the resiliency of each financial services institution, leading to improved performance and resiliency industry-wide.

Getting TPRM right: Quick takeaways

The consequences of getting third-party risk wrong can be serious. With this in mind, we offer the following guidance when developing and implementing a TPRM framework:

- **Stop awarding work to third parties based solely on price or financial value.** Evaluate outsourcing decisions based on broader concepts of foundational and emerging risks and decide which areas of the business are "off limits" to outsourcing. Include total compliance costs, and assess how they align with compliance risks that could impact your brand or result in costly fines or litigation.
- **Hold business lines ultimately responsible** for managing, implementing, and overseeing each third-party engagement, while recognizing that accountability for TPRM resides with the board and senior management.
- **Invest in real risk-management tools, processes, and skill sets** to focus on higher risk relationships or help uncover hidden dangers that pose strategic risks. Keep in mind that third parties may not have the resources to implement risk controls themselves.
- **Rationalize and rank third-party relationships at an aggregate portfolio level,** taking into account that different entities carry different types of risks, and then manage them based on how much risk they present to your institution.
- **Trust, but verify.** Verify that your internal organization is doing what it needs to do to execute your TPRM processes, while making certain that vendors are performing to expectation. Although it may not be feasible or cost-effective to audit all third-party relationships, some level of formal assessments conducted through internal audit or by independent parties may make sense.

How Deloitte can help

Deloitte helps organizations harness innovation and address heightened demands for managing the risk of third parties and the complexity of the extended enterprise. We provide end-to-end services across several dimensions, including advisory and strategy, third-party assessments and assurance, program transformation, managed services, and remediation/crisis management.

References

i. Michael Koontz, Reetika Joshi, "Business Services Outsourcing in Banking and Financial Services," HfS Research, Ltd., January 2013.

ii. OCC Bulletin 2013-29 rescinds Bulletin 2001-47 and OCC Advisory Letter 2000-9 on Third-Party Risk. The latest bulletin follows similar guidance released by other regulatory bodies, such as FDIC FIL-43-2013 (Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities) and the Consumer Financial Protection Bureau (CFPB) Bulletin 2012-03 (Service Providers).

iii. Bank of England, *Prudential Regulation Authority SYSC 19.9: Outsourcing.* http://fshandbook.info/FS/html/PRA/SYSC/13/9.

iv. Monetary Authority of Singapore, *Guidelines on Outsourcing*, October 2004 (last updated 1 July 2005). http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing20Guidelines.pdf

v. Australian Prudential Regulatory Authority, *Prudential Standard CPS 231: Outsourcing*, July 2012. http://www.apra.gov.au/CrossIndustry/Documents/Prudential%20Standard%20CPS%20231%20Outsourcing.pdf

vi. Hong Kong Monetary Authority, Supervisory Policy Manual (SA-2, Outsourcing), 28 December 2001. http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf

vii. OCC Bulletin 2013-29.

viii. Federal Reserve Board, SR-13-19/CA 13-21, Guidance on Managing Outsourcing Risk, December 5, 2013.

ix. First line of defense may require taking a shared, decentralized approach for managing controls and risks among financial services institutions and vendors across all business relationships (e.g., business-line oversight and service-level agreements); the second line involves centralizing and implementing enterprise-wide business-process definitions, protocols, standard operating procedures, exceptions, training curricula and performance reviews; and the third line involves internal audit (or an equivalent function) to ensure the first two lines are working.

Contacts

Walter Hoogmoed
Principal
Deloitte & Touche LLP
+1 973 602 5840
whoogmoed@deloitte.com

Edward Appert
Director
Deloitte & Touche LLP
+1 212 436 7511
eappert@deloitte.com