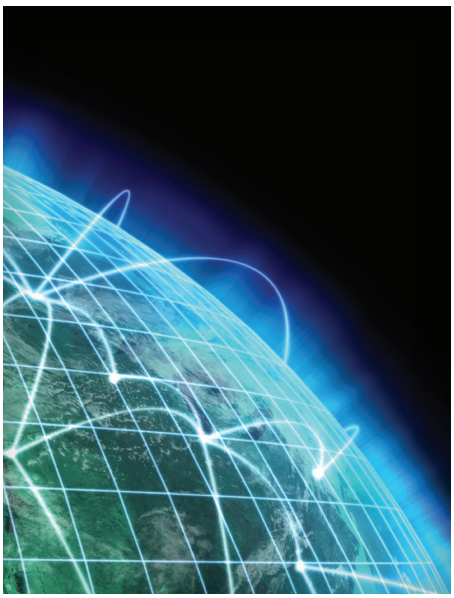
Crowe Horwath

May 2015

The New Imperative in Risk Management: Know Your Third Parties

Implementing a Robust Third-Party Risk Management Framework

By Jill M. Czerwinski, CIPP, CISA, CISSP, Michele Sullivan, CPA, and Linda Tuck Chapman



Third-party risk management is a growing concern for a variety of financial services companies – including banks, investment companies, investment advisers, broker-dealers, transfer agents, clearing agencies, and servicers. Such firms rely heavily on other companies to provide products and services, and regulators are scrutinizing the controls the firms maintain on the relationships with these companies. To meet regulatory expectations, financial services companies should establish a robust framework, standards, and processes for managing third-party risk – plus a "center of excellence" to implement their efforts.

Extensive risk management regulatory guidance exists for financial services companies that have relationships with outside service providers and other third parties. The guidance emphasizes adopting risk management processes that are "commensurate with the level of risk and complexity of their third-party relationships." Comprehensive risk management and oversight of third-party relationships throughout the life cycle of the relationships, from planning through operation termination, are also stressed.

Not Just Vendors

People typically think of "third parties" as vendors that provide banks with IT and other services, but third parties extend well beyond the realm of IT vendors. From the regulators' perspective, third parties include non-vendor entities such as debt buyers, mortgage servicers, correspondent banks, product resellers, channel partners, payments processors, organizations that interact with bank customers, foreign-based service providers, subcontractors (known as fourth, fifth, and sixth parties), affiliates, and joint venture, investment, and revenue-sharing relationships.

With so many types of organizations qualifying as third parties, financial services companies easily can have hundreds, even thousands, of relationships to monitor and manage. That's why it's important for them to have comprehensive, efficient, and effective third-party risk management programs in place. Such programs:

- Span all types of relationships throughout their life cycles
- Are risk-centric and adjusted according to the level of risk

- Are technology-enabled
- Include protocols for effective challenges and quality assurance processes
- Use appropriate existing skills and processes
- Deliver a clear return on investment
- Align with enterprise risk management and operational risk management frameworks
- Enable actionable reporting and insight

A Framework for Managing Risk

Many financial services companies lack adequate focus and strategy in the area of third-party risk management – starting with an absence of strategic direction and extending to staffing issues. Many banks have an aged vendor management policy that originated under the *Gramm-Leach-Bliley Act* of 1999. Many also still have the resources allocated under this old policy, with smaller banks often having three or fewer people dedicated to managing third-party risk management programs.

Due diligence for a new third-party relationship requires greater rigor, depth, and breadth than ever before.

Larger banks might have proportionately more resources, but they often also have a growing number of third parties to manage, especially in the wake of acquisitions or mergers. Given the required level of rigor and the volumes of outsourced services, vendors, and other third parties, financial services companies of all sizes are beginning to respond but sometimes are doing so without an established and proven framework. To help companies get the most from their limited resources, it's useful to adopt a framework that encompasses all the tasks third-party risk management requires. Such a framework should include the following foundational, governance, and management elements.

Fundamental Principles

Effective third-party risk management is built on a foundation of risk identification, due diligence, ongoing management, and periodic evaluation.

1. **Due diligence.** To start, after identifying the in-scope relationships, the financial services company needs to assess the risks presented by new relationships, changes to existing relationships, and relationships up for renewal. It also needs to determine current and planned controls to manage these risks. When soliciting products and services from a third party, traditionally financial services companies have relied on a request-for-proposal procurement process to identify major risks by asking questions about prospective partners' financial stability and experience. Today, this due diligence requires greater rigor, depth, and breadth than ever before.
2. **Ongoing management.** After selecting a third party, completing due diligence, and implementing appropriate controls, the financial services company needs to manage the day-to-day relationship and monitor the party's performance. The company should confirm that management and control activities are performed and that any incidents and other problems are dealt with promptly and appropriately.
3. **Periodic evaluation.** Next, the company implements the third foundational element of effective third-party risk management: monitoring the relationship and reassessing the risks. Filters such as how critical the relationship is, any incidents that have occurred,

The Total Cost of Outsourcing

Often third-party relationships are a result of outsourcing, which might be considered a way to cut costs. However, many organizations fail to take into account the cost of managing third-party relationships and risks. Inadequate management and oversight can raise the risk level.

For example, a bank might decide to outsource loan servicing to a third party that specializes in that function. Management of the risks and relationship with the third party requires time, skills, training, knowledge, and visibility. If the bank doesn't make necessary investments, it can't govern and manage the loan servicer. In turn, this resource deficit increases the bank's third-party risk.

Organizations need to calculate the total cost of outsourcing by including all the internal resources required – including resources to train the third party's personnel, negotiate the contract, implement any shared technology, and conduct initial due diligence, ongoing monitoring, and periodic reviews.

and any performance issues that have arisen should be used. As a result, the financial services company might need to make changes to the relationship, introduce new controls, or modify how it manages the third party.

After these elements are in place, financial services companies can apply the following governance and management principles for the appropriate oversight of third-party risk.

Governance Principles

Financial Services companies should adopt four principles as the basis for the appropriate oversight of third-party relationships: identification, assessment, management, and control of risks.

1. **Identification.** Financial services companies must know with whom they are doing business. This is easier said than done. Many third-party relationships can be buried in the far corners of an organization. They could have existed for years, controlled by line managers who regard these relationships as theirs alone. Senior leadership should make clear to all managers that all third-party relationships pose risk to the organization and therefore need to be identified and managed transparently. New third-party relationships should be identified and reviewed early in the process so that the appropriate due diligence can be performed.
2. **Assessment.** Once all third-party relationships have been identified, financial services companies need to understand the risks that the relationships pose by following standardized procedures for assessing and documenting risk. There is no one-size-fits-all approach when it comes to the appropriate steps for the risk and controls assessment, either initially or periodically. The recent guidance on this topic from the Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board (FRB), however, can provide organizations with a solid framework for their program.

   For new or changing relationships, this assessment should tie directly to the contract negotiation. Simply accepting a contract presented by a third party is inadequate; a company should negotiate terms that strengthen its controls. There will be the usual give-and-take of a negotiation, but a financial services company should insist on the inclusion in the contract of a formal agreement by the third party to implement risk-mitigating controls and help establish standards for ongoing reporting and management.
3. **Management.** Financial services companies also need to manage third-party risks during the execution of the agreement. This can be challenging, as line-of-business management might be focused on performance rather than risk management. In addition, risks are changing constantly as new threats emerge in the business environment. Considering these challenges, organizations need to be staffed appropriately to manage third parties. This means that the total cost of outsourcing extends beyond the company's payment to the third party (see sidebar, "The Total Cost of Outsourcing"). Many financial services companies will need to make widespread changes to existing processes to be able to assume and manage higher levels of risk. Third-party relationships have a life cycle, and there is a need to periodically reevaluate current and prospective risk management efforts to increase business value while complying with regulators' expectations.

4. **Control:** Another critical aspect of oversight is controlling risk, which financial services companies can do with some degree of confidence via contracts with third parties.

Management Principles

Standards and procedures, as well as technology, are necessary for executing the day-to-day tactics of third-party risk management.

1. **Standards and Procedures.** Management principles begin with a policy or standard for conducting due diligence, ongoing management, and periodic reevaluation of third parties. Standards should be supported by detailed procedures, which can be extensive because they involve other parts of the organization, such as the legal, information security, and compliance functions. Procedures should extend to the individuals managing the third-party relationships in the lines of business. Different lines of business should not have different procedures for coordinating third-party reviews and other management activities.
2. **Technology.** Financial services companies also need to implement technology that supports efficient and effective execution of their third-party risk management programs. Spreadsheets are not an effective way to manage risk. There are several good software applications for automating third-party risk management. It's important that institutions define their requirements before selecting and investing in the best software solution for their needs.

Managing the Framework

The framework for managing third-party risk also requires implementing an appropriate organizational structure to oversee the program. Typically, third-party risk management programs have five levels of oversight:

1. The board of directors
2. An enterprise risk management function or committee
3. An operational risk management function or committee
4. A third-party risk governance committee
5. Line-of-business relationship owners and their third-party risk managers

To get the most from their investments, some organizations have established a third-party risk management "center of excellence," comprising a dedicated third-party risk management team and supported by risk subject-matter experts. The purpose of this team is to bring together individuals who typically have no management or reporting structures in common but need to collaborate on third-party risk management. This model, which is gaining traction in the marketplace, facilitates communication among the employees closest to the third-party relationships and demonstrates the commitment to third-party risk management that the regulators expect.

Contact Information

Jill Czerwinski is with Crowe Horwath LLP and can be reached at 630.575.4317 or jill.czerwinski@crowehorwath.com.

Michele Sullivan is a partner with Crowe and can be reached at 574.235.6824 or michele.sullivan@crowehorwath.com.

Linda Tuck Chapman is President, ONTALA Performance Solutions Ltd., and CPO Emeritus in association with Crowe Horwath Global Risk Consulting. She can be reached at 416.452.4635 or lindatuckchapman@ontala.com.

[1] See OCC Bulletin 2013-29, "Third-Party Relationships, Risk Management Guidance" Oct. 30, 2013, http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html, and FRB SR13-19, "Guidance on Management Outsourcing Risk Dec. 5, 2013, http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm#access

"The New Imperative in Risk Management: Know Your Third Parties," a recording of the Feb. 24, 2015, Crowe webinar presentation by Jill Czerwinski, Michele Sullivan, and Linda Tuck Chapman, is available at http://www.crowehorwath.com/ContentDetails.aspx?id=11108.

Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction. © 2015 Crowe Horwath LLP RISK15912