Checklist

10 Steps to Implementing an Effective Third-Party Risk Program
Modern banks and financial services companies depend on a vast network of third-party relationships that extend beyond traditional product and service providers to include dealers, brokers, joint ventures, affiliates, and many others.

The top 10 U.S. banks each average between 20,000 and 50,000 third-party relationships. This complex web of relationships can sometimes have unexpected consequences and needs to be monitored and managed correctly. Faced with increased regulatory scrutiny, record-breaking settlements, and compromised reputations, some banks and financial services organizations are fortifying their third-party risk management programs. Yet in a recent study by Crowe Horwath LLP and Compliance Week, just 12 percent of financial services companies reported that their third-party risk management programs have achieved the highest maturity level.

In other words, more companies take a reactive, get-the-job-done approach rather than a comprehensive, organizationwide stance. Banks and financial services companies need to bridge this gap if they want to protect themselves against the rising threat of third-party risk.

This checklist details how banks and financial services companies can streamline the implementation and optimization of an effective third-party risk program.

Establish roles and responsibilities

A primary issue with many third-party risk programs is their decentralized nature, with no organizationwide policy, authority, or data. It is essential, then, to begin implementation by establishing a third-party risk management policy (preferably board-approved) that makes clear where the program’s authority resides and clearly defines roles and responsibilities.
Thirty percent of companies reported that they centralize their programs entirely or largely in the procurement function, but that may not always be the best option. Procurement is primarily concerned with spend, and may not be effectively incentivized to minimize risk across the various disciplines inherent in the industry. Banks and financial services companies with a more mature model centralize third-party risk within their enterprise risk management or operational risk management functions.

Centralizing the third-party risk management program in this way provides the authority to support cross-functional collaboration among the procurement, contracting, and legal departments. In addition to representatives of these functions, the implementation team should determine risk domain subject-matter experts in the areas of information security, compliance, physical security, privacy, finance, business resiliency, and any other areas where there may be significant inherent risk for the bank or financial services company.

**Inventory third-party relationships**

The next step is to identify and inventory traditional and nontraditional third-party relationships throughout the organization and map third-party relationships to the company’s business processes, products, or services. Surprisingly, 32 percent of companies found this basic component of their third-party risk program to be a challenge and often are not even sure which areas of the organization to consider.

The best place to begin identifying and inventorying third-party relationships is in accounts payable, since many of these relationships will eventually generate payments. Similarly, examining receivables can reveal noncustomer revenue sources that should be inventoried. The implementation team could also examine the company’s referral agreements and catalog the parties that have access to its information systems and physical facilities. A more sophisticated search could involve technology tools such as email filters. In addition to traditional suppliers of goods and services, the inventory should include:

- Joint marketing agreements
- Settlements (e.g., debt collectors)
- Affiliates, joint ventures, and intragroup arrangements
- Fourth parties (e.g., third-parties’ subcontractors)
Each relationship should be mapped to business processes and the company’s products and services to identify areas of potential risk concentration. This is also helpful for identifying otherwise hidden areas where regulatory compliance risk may be high. Finally, the third-party risk management program should establish control processes to assess the completeness of the inventory.

Assess inherent third-party risk
With a complete inventory in hand, the next step is to assess the inherent risks related to the various relationships. The team should base these assessments on its understanding of the nature of the products and services offered by the third party and the impact they may have on the bank or financial services company. Assessment criteria should include:

- **In scope and out of scope.** It may not be necessary to include every relationship in the final inventory. However, the implementation team should be prepared to justify how it determines if an individual relationship is within or beyond the program’s scope for ongoing risk management activities.
- **Criticality.** Is the relationship mission-critical or can it be easily replaced? Does the relationship provide a critical activity that has the potential to significantly impact the company?
- **Access.** What access, physical or virtual, does the third party have to sensitive information or valuable assets? What is the volume or impact of this access?
- **Geography.** Is the third party subject to volatile political conditions? Is it in a region with reliable transportation or communication infrastructure? Is it at risk of severe weather? Are there information sharing or privacy concerns for the country where the third party operates?
- **Resiliency and viability.** Is the third party financially sound? Are there business continuity concerns? Is it a merger or acquisition target?
Perform enhanced due diligence
For those relationships that warrant further assessment, perform enhanced due diligence including control assessments, and identify, document, and communicate unmitigated control weaknesses or gaps. This process often involves subject-matter experts in areas such as IT, information and physical security, compliance, and legal, or professionals specialized in areas of concern such as default management, sales practice, fraud, or business continuity.

It’s important to consider how well the company or third party is controlling inherent risks. Perform a gap analysis to determine current and future goal states. Discuss remediation plans with the third party and establish exception tracking and approval processes to monitor progress and assess performance.

Develop and track action plans
The due diligence process can result in findings that require resolution. For each finding, establish an action plan internally and with the third party to mitigate identified control weaknesses or gaps, and make sure to track them through completion.

In many cases, the relationship manager already responsible for day-to-day interaction with the third party is best positioned to communicate with it, as well as monitor and report on progress to the third-party risk management function.

Create assessment-driven contract clauses
Only when all assessments are complete should the companies finalize a contract for the relationship. The agreement should include assessment-driven clauses to verify that all risks are appropriately addressed, especially considering any open findings coming out of the assessments. Other components of a well-crafted contract can include:

- A requirement to participate in risk management activities
- The right to audit relevant processes
- Service-level agreements
- Policy and approval processes for subcontractors (fourth parties)
- Notification requirements covering significant changes and adverse events
- Regular meetings and reports
Formulate ongoing management activities

Ongoing management activities include regular or continuous monitoring for contract compliance, adverse events, and change. The day-to-day relationship manager may be responsible for this process, which might also include relevant subject-matter experts in fields such as information security. This process can often be streamlined using technology that monitors litigation, reputation, news, the security of public- and web-facing sites and apps, data breaches, and the financial health of the third party.

The third-party risk management function should also establish processes for internal monitoring of change, such as new or modified statements of work, changes in data provided, and changes in access to networks and physical locations. If significant external events or internal change is identified, a reassessment of the third-party relationship may be warranted.

Implement regular reporting

Ongoing reporting may include scorecards and key risk indicators (KRIs) at the relationship level as well as KRIs and key performance indicators (KPIs) at the portfolio level. The third-party risk management function should focus on aggregating data across the company to develop a complete picture of the company’s third-party risk portfolio.

This perspective can expose concentration risk, including multiple relationships with a single third party or overreliance, through multiple third parties, on individual fourth parties. Portfolio-level KRIs can reveal aggregate risk, total cost of relationship, and compliance monitoring. KPIs illuminate how well the third-party risk management program is operating in terms of the responsiveness of third parties and the timeliness of assessments and reassessments.
Deploy technology

Technology remains a stumbling block for many third-party risk management programs, with 41 percent to 55 percent of respondents relying on end-user applications such as spreadsheets, which make data aggregation and management difficult or nearly impossible. The most mature third-party risk management programs implement comprehensive technological solutions that assist with workflow, reporting, and monitoring, including:

• Data and metadata capture from multiple sources, including continuous monitoring and automated data gathering whenever possible
• Extensive and flexible reporting and analysis capabilities, including visual representation to indicate trends and aggregation
• A centralized document repository
• Workflow automation tools with reminders
• Integration with other systems

Track program performance and quality

With the program up and running, it is critical to maintain visibility into its performance by measuring risk reduction and quality assurance. This involves monitoring KPIs and addressing issues before they negatively affect program efficacy. Verify that assessments and reassessments are occurring in a timely and efficient manner, that third parties and internal staff are responsive in addressing concerns, and that adverse events or internal and external changes are reported appropriately.

The third-party risk management team should investigate negative trends in any of these areas. For example, if it’s determined that staff or third parties aren’t fully engaged, what is the root cause? In some cases, it may turn out that the process is too cumbersome and, subsequently, requires streamlining or automation to get back on track.

It is no less important to see that the third-party risk management program receives the necessary support and funding. Keeping the board of directors and senior management up to date with appropriate reporting will aid in this effort.
Conclusion

Don’t let hidden third-party risk threaten your bank or financial services company. Your third-party risk management program can only be effective when it is comprehensive and ongoing. If your company finds itself reacting to risk as it arises, or if your program lacks insight into risk at the organizational level, it is time to review and revamp your program. Begin by establishing the parameters of your policy, and build on that foundation to create an effective and efficient third-party risk management program.

Connect With Us

Gayle Woodbury
Managing Director
Crowe Horwath LLP
+1 630 586 5325
gayle.woodbury@crowehorwath.com

2 “Crowe Horwath 2016 Third-Party Risk Management Survey,” Crowe Horwath LLP and Compliance Week, 2016. All data cited in this document is from this source unless otherwise indicated.