WHITE PAPER
THIRD PARTY MANAGEMENT: FUNDAMENTALS
by Linda Tuck Chapman

Sponsored by hiperos
an Opus Global Company

Third Party Management Fundamentals

Third Party Management isn't new, but its importance is growing in every industry and the financial services sector is leading the way. With an average of three years' experience to learn from, risk oversight experts and practitioners are re-assessing their programs for opportunities to strengthen them.

In his address to the American Bankers Association, Thomas J. Curry, Comptroller of the Currency, OCC said "It is well that we are finally giving these [operational] functions the attention they deserve. It is also good that we are finally recognizing the individuals responsible for performing risk management and compliance."

The effectiveness of third party management is a component of safety and soundness exams, and severe deficiencies can affect an institution's CAMELS rating (Capital, Assets, Management, Equity, Liquidity). This intense regulatory focus on effective lifecycle management and governance practices means that third party management is on the agenda the Board of Directors, Audit and Risk Committees, C-suite executives, business line and corporate function leaders.

Context for Action:

- According to the Risk Management Association's 2014 Vendor Management Survey, 0% of participating financial institutions rated their program as "completely mature".

Beyond the basics, regulators consistently signal where institutions should be focused on evolving their programs. For example, FFIEC IT Examination Handbook recently published Appendix J: Strengthening the Resilience of Outsourced Technology Services. The focus is on business resilience and business continuity planning.

- 40% of large financial institutions have less than 1000 vendors in their programs today; 50% have in excess of 2500. As their programs mature, 45% of large financial institutions expect these numbers to increase over the next three years, in some cases substantially.

In practice, most institutions risk-assess 100% of their third party "vendor" relationships. Approximately 10% of the total vendor population in the Accounts Payable database are typically found to have risk characteristics that require them to be actively managed in a third party management program. And an average no more than fifteen of these critical

relationships are "enterprise critical", ones whereby a serious failure could bring the institution's operations down.

- As of October 2013, OCC regulated institutions in the US are required to incorporate "non-vendor" third parties in their programs. Most institutions are at initial stages addressing non-vendor relationships.

In most institutions, this work is just beginning. Leading practitioners are finding that this population of critical "non-vendor" third party relationships is expected to be larger than the population of critical "vendor" third party relationships.

- 91.4% of survey respondents have < 3 FTE dedicated to vendor management in their centralized/center-led function, excluding those in the line of business who are responsible for day-to-day vendor management.

Since the RMA survey in mid-2014, many financial institutions are investing in more third party management resources within center-led functions. And many high-potential, high-performance individuals are attracted to these new roles.

Strive for Compliance and Completeness

While the number of MRAs and MRIAs that financial institutions are receiving from regulators is declining, the closer your institution gets to "Compliance and Completeness" with your third party management program, the more likely that your institution will also pass the "Trust but Test" examination hurdle.

The top portion of this "Know your 3rd Party" framework describes the lifecycle management activities. The bottom section describes sustainability elements that your program needs to support effective goverance. A robust program includes all the elements in this framework.

The "book of record" is the single source of information about critical third party relationships including documentary evidence that confirms all program activities have been completed, and that your institution is proactively managing third party risk. The "book of record" is a purpose-built technology system with embedded tools, templates and processes, robust workflow and reporting capabilities, data governance protocols, and an audit trail.

A strong program and robust technology minimizes manual work effort associated with thousands of third party relationships and dozens of actvities and records for each.

Identifying Critical Relationships

In alignment with the "Getting to Strong" regulatory principle, some financial institutions are redefining what constitutes a "critical" relationship. To complicate matters, in addition to the Consumer Financial Protection Bureau, which is focused on any third party relationship that has consumer credit-related exposure, the two primary regulators – The OCC (Office of the Comptroller of the Currency) and the FRB (Federal Reserve Bank) define "critical relationships" differently. Referring to regulatory guidance provides some insight into differences in their focus.

FRB SR13-19: the focus is on outsourced activities that…

- have a substantial impact on a financial institution's financial condition
- are critical to the institution's ongoing operations
- involve sensitive customer information or new bank products or services
- involve new bank products or services
- pose material compliance risk

The challenge with this definition is reaching a common understanding of an outsourced activity. At this time, the FRB's focus appears to be on "vendor" third party relationships.

OCC 2013-29: more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities:

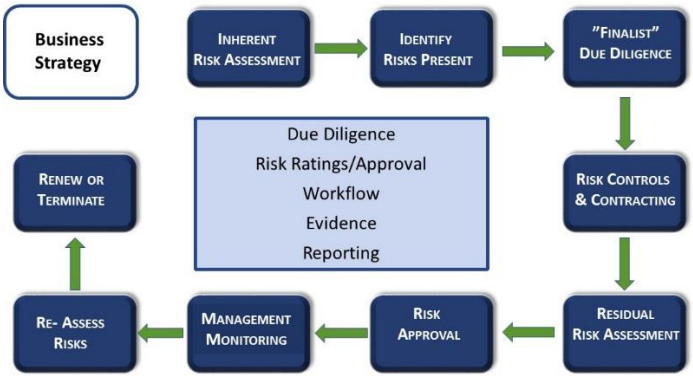
- significant bank functions (e.g., payments, clearing, settlements, custody)
- significant shared services (e.g., information technology)

- 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 and manage risk
- could have a major impact if the bank has to find an alternate third party or if the activity has to be brought in-house.

The OCC has made it clear that their focus is on all third party relationships. Quoting OCC Bulletin 2013-29: "A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise." This means a business relationship any individual or company, excluding customer relationships.

Translating Guidance into an Operating Model

Risk management is a team sport, and none more so than third party management. Regardless of whether your program translates guidance into an operating model with ten or twenty steps, it's important that lifecycle management processes are thorough, consistent and easy to communicate to the hundreds or even thousands of users across the institution.



Most of the larger institutions have done a good job of implementing a framework. In many cases there is room for enhancements to:

- due diligence processes including risk-rating findings from due diligence assessments

- standardizing risk and contract controls, including risk-adjusting these to reflect different tiers of risk
- adding a formal risk approval step for the first line of defense – the risk and relationship owner - to the process
- post-contract monitoring activities, including performance management

Another question that practitioners often ask is how to share data across multiple technology platforms. For example, Information Security assessments may be stored in one system, contracts in another, and third party relationship data in another.

Founded in the principle of creating a single "book of record" for third party relationships, most institutions either cross-reference records in discrete systems and/or implement automated data transfer processes. True integration is costly and complicated.

What is most important is easy access to related records and strong data governance principles. Data integrity is the hard part because there are so many users and stakeholders. That is why formal, scheduled Quality Assurance testing is so important.

Risk Categories and Due Diligence

The list of third party risks that institutions need to assess continues to grow. While financial institutions can learn a lot about assessing anti-corruption, anti-bribery risks such as the oil and gas and information technology sectors, financial services are in the lead in developing processes to manage the rest of the following third party risks.

Certain risks are highlighted in the following list because they are attracting particular interest from regulators. Anti-Money Laundering is related to identifying criminal activity and terrorist financing. Business Continuity Management/Resilience is the subject of new Appendix J to the FFIEC IT Examination Handbook (referenced above). Financial viability assessments have long been a focus of regulators. These can easily be automated, so many institutions are reassessing financial viability every year for all in-scope critical relationships. Model risk is a relatively new focus for third party management. Model risk is commonly be presented by algorithms in technology systems or quantitative models developed by consultants. Privacy risk assessments typically form part of Information Security Assessments as they relate to sensitive and regulated information.

1. Anti-Corruption/Anti-Bribery
2. **Anti-Money Laundering**
3. **Business Continuity Management/ Resilience**
4. Cloud computing
5. Company officers and corporate viability
6. Contract
7. **Financial viability**
8. Foreign service delivery location
9. Human Resources
10. Incentive compensation
11. **Information Security**
12. Insurance
13. **Model**
14. Performance
15. **Privacy**
16. Physical Security
17. Records
18. Reputation
19. SOX- reportable financial loss
20. Sub-contractor
21. Technology

Workloads are heavy. The goal should be to automate as many of these due diligence and risk assessment processes as possible, minimizing tactical work effort in order to free up resources to focus on proactive risk management.

Service providers are struggling to respond to third party risk assessments. In addition to managing their own critical service providers, they are asked to respond to hundreds of incoming risk assessments. These assessments typically seek similar or the same information but are rarely identical.

In turn, financial institutions are struggling to get completed risk assessments back from there critical service providers on a timely basis. How long will it take the sector to find an acceptable solution(s) for due diligence and risk assessments?

Lifecycle Management

In Bulletin 2013-29, the OCC did a good job of describing their expectations for lifecycle management of third party relationships. Here are some highlights:

- ✓ plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
- ✓ proper due diligence in selecting a third party.
- ✓ written contracts that outline the rights and responsibilities of all parties.
- ✓ ongoing monitoring of the third party's activities and performance.
- ✓ contingency plans for terminating the relationship in an effective manner.
- ✓ clear roles and responsibilities for overseeing and managing the relationship and risk management process.
- ✓ documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
- ✓ independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

Some practitioners are concerned about how to build global programs that address differences in regulatory requirements across geographies. With a robust system, this is easily done by leveraging what is the same for all, and implementing specific requirements in automated workflows to address and report on the differences.

Principles of Good Governance

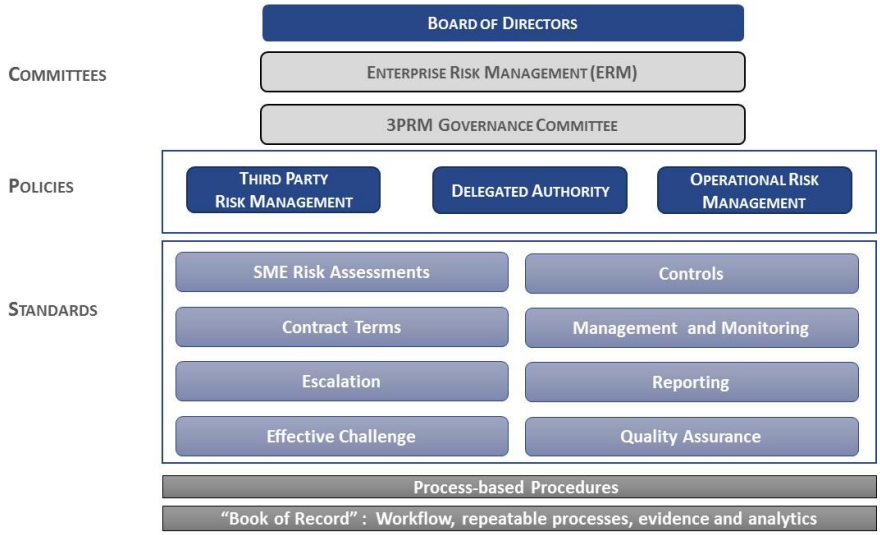
Key Performance and Risk Indicators are widely used tools in financial institutions. What's new is defining them for third party management. Key performance indicators help center-led organizations, Enterprise Risk Management and Audit determine whether the program design, tools and processes are effective. Key Risk Indicators need to be aligned with Risk Appetite Statements and Risk Tolerance thresholds specifically designed for third party management. These are new tools for financial institutions and as a results, lots of work still needs to be done on these by most, if not all institutions.

Working with risk reports is where executive management and regulators will spend most of their time. There is still a lot of work to be done in most, if not all financial institutions to provide the right information, at the right time, to a wide range of stakeholders.

In the future, financial institutions will be much better at analyzing risks and designing triggers to identify third party relationships that are in decline. Before they fail.

A Strong Governance Framework

Implementing a strong governance framework and "inspecting what you expect" are long-held governance principles in all financial institutions. This following governance model and oversight model is becoming common in larger institutions. In smaller ones, the principles are the same but multiple roles can be assumed by individuals.



An emerging practice is to appoint a Third Party Governance Committee consisting of senior executives from lines of business, risk and procurement. In some cases they report to Enterprise Risk Management and in others to the Audit or Risk Management Committee of the Board.

Critical Success Factors

If you can answer "yes" to the following questions, your third party management program may be an industry leader:

- ✓ Capture all third parties?
- ✓ Address relationships through their lifecycle?
- ✓ Fully comply with all applicable regulatory guidelines?
- ✓ Include repeatable, risk-rated due diligence programs?
- ✓ Establish clear accountabilities including risk acceptance and escalation?
- ✓ Respect the principles of the "three lines of defense"?
- ✓ Risk-adjust requirements, commensurate with risks?
- ✓ Define required tasks and frequency for monitoring and management?
- ✓ Warehouse accessible and auditable documentary evidence?
- ✓ Includes evidence of execution of Effective Challenge and Quality Assurance processes, KRI's, KPI's, Risk Appetite Statements and Risk Tolerance thresholds?
- ✓ Generates insightful and actionable reporting?

Conclusions

Over time, third party management practices will eventually reach the same level of maturity as credit and market risk management practices. For now, it's a steep learning curve and no institution can yet claim that they've got it right.

This is not a "check the box" exercise in compliance, the expectation is for proactive third party management of all critical relationships throughout their lifecycle. It may be time for your institution to go back to basics, and reassess their program in the context of the current environment and emerging practices. Like sound credit and market risk management practices, executive management is learning that investments in effective third party management pay dividends. The rate of return is up to them.

References

1. OCC Bulletin 2013-29
2. FRB SR-19, CA 13-21
3. FFIEC Outsourcing Technology Services 2004. Appendix J

About the author

Linda Tuck Chapman, President Ontala Performance Solutions Ltd. and CPO Emeritus, in association with Crowe Horwath Global Risk Consulting is subject matter expert in third party management, outsourcing governance and sourcing optimization. You can contact her at lindatuckchapman@ontala.com or 416.452.4635

About Hiperos

Hiperos is an Opus Global company. We were founded with a single focus – to help our customers get more value from their third parties and third party relationships. Today, Hiperos customers engage with their third parties in 182 countries worldwide, and depend on the Hiperos 3PM™ platform to control the risks and optimize the value of their third party relationships.

For further details: +1 908 981 0080 | info@hiperos.com | www.hiperos.com