hiperos
an Opus Global Company

WHITE PAPER

VENDOR AND THIRD PARTY MANAGEMENT: WHAT BOARDS OF DIRECTORS AND C-SUITE EXECUTIVES NEED TO KNOW

by Linda Tuck Chapman

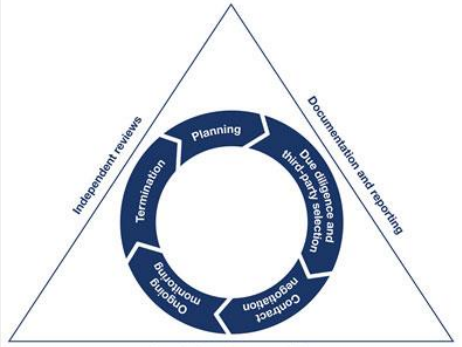
ONTALA PERFORMANCE SOLUTIONS
REDEFINING THIRD PARTY MANAGEMENT

Hiperos | www.hiperos.com | 908-981-0080

TABLE OF CONTENTS

Vendor and Third Party Management: What Boards of Directors and C-Suite Executives Need to Know

Regulatory stakes are rising at a pace that exceeds many financial institutions' ability to respond. Similar to FACTA, Anti-Money Laundering and other "Know Your Customer" guidance, regulators expect institutions to know their third parties. Since October 2013, the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Consumer Financial Protection Bureau (CFPB) and the Federal Financial Institutions Examination Council (FFIEC) have issued new guidance for the management of third party risk. Now within the scope of virtually every regulatory exam are scope, consistency, and execution rigor of processes that proactively identify, assess, manage and control third party risk. The responsibilities of the board of directors and executive management have expanded accordingly.



Source: OCC

The consequences for failure are severe. Many large and mid-sized financial institutions have received multiple Matters Requiring Attention (MRAs), and some institutions have received Matters Requiring Immediate Attention (MRIAs) or Consent Orders. Regulatory attention is already starting to intensify for smaller institutions.

The CFPB and the Department of Justice (DOJ) have levied multi-million dollar fines for violations.

Control deficiencies and service failures by third parties can seriously impact customers, exposing institutions to reputation risk, financial loss and litigation.

Third party risk management has recently become a component of regulatory safety and soundness assessments, an indicator of management capabilities. "Serious deficiencies may result in management being deemed less than satisfactory"[1.] , affecting the institution's CAMELS rating.

A degree of collaboration is starting to occur across the financial services sector and some best practices in third party management are emerging. Even so, there is wide disparity in scope, processes and practices. Regulators are not satisfied with the current state, but some acknowledge that third party risk management is a new focus, one with a steep learning curve.

Context for Action

Financial institutions rely extensively on third parties in almost every aspect of their operations. With significant barriers to entry and highly specialized expertise, multiple institutions collectively rely on a core group of third parties to deliver critical services domestically and internationally, creating institution-specific and systemic concentration risk.

A third party "is any business arrangement between a bank and another entity, by contract or otherwise"[2]; and "all entities that have entered into a contractual relationship with a financial institution to provide business functions and activities". [3] This encompasses traditional goods and services vendors, and non-vendor relationships such as debt buyers, agents, joint ventures, resellers and correspondent banking relationships.

Financial institutions also buy and sell services to each other and rely on shared utilities for many services. With the 2008 crisis still clearly visible in the rear-view mirror, it is easy to understand why regulators are focused on preventing institution-specific and system-wide crises, and seek early warning for potential failures.

What You Should Know

A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.[4] In SR-19 "Guidance on Managing Outsourcing Risk", the FRB describes what are typically understood to be the responsibilities of the board of directors and senior management for effective governance and management of third party risk.

What's new can be found in OCC Bulletin 2013-29 "Risk Management Guidance for Third Party Relationships". In OCC Bulletin 2013-29 strategies, activities and contracts (referred to as "relationships") that involve critical third parties require board approval, including a review of a summary of due diligence results and management's recommendations[5]. This is a significant departure from the historical role of the board of directors, particularly in larger banks.

Regardless of board requirements, both the FRB and OCC expect a significant increase in the level of involvement by senior management in the assessment and decisions relating to third party relationships, the activities of the first, second and third lines of defense and the level of detail in risk oversight activities.

Critical Success Factors

Regulators expect institutions to have an evidence-based, risk-centric, risk-adjusted program that actively manages a wide range of third party risks. This is not is not a "check the box" compliance exercise.

"Risk-centric" means investing in tools, processes, practices, skills and technology that enable proactive identification, assessment, management and control of risk." **Risk-adjusted"** means that risk controls and work effort are commensurate with criticality and the identified level of risk.

Every relationship should be assessed and assigned a tiered (sometimes referred to as "ranked") **Inherent Risk rating.** Management effort should be concentrated on critical relationships that are material and/or high risk. These must be closely managed and periodically reassessed.

Regulatory guidelines highlight six to eight primary risk factors. Once sub-risks are included, many institutions assess twenty or more risk factors. Primary risks include information security, information technology, reliance on subcontractors, physical security, resilience, human resource management, incident reporting and insurance coverage. Sub-risks include business continuity management, model, fraud, country, anti-bribery, privacy, financial reporting, anti-money laundering, credit, scalability, transaction volumes, business background, and risks specifically pertaining to an outsourced function.[6]

Three Lines of Defense

The first line of defense is the line of business. Accountable executives and their teams develop business strategies, establish and manage third party relationships, and execute controls developed in the second line of defense. They are expected to proactively manage risk and performance of all third parties throughout their lifecycle.

The second line of defense consists of Operational Risk, a Third Party Management organization, Procurement, Legal and specialized risk experts. Each function has accountability for creating risk-adjusted Standards and procedures, and executing their management responsibilities to identify, assess, and control third party risk.

Internal Audit is the third line of defense. Audit is responsible for performing periodic independent reviews of third party management processes and critical relationships. Their results must be reported to senior management and the board of directors.

Governance and Oversight

Regulatory guidance for third party risk management is specific but not prescriptive. Regulators acknowledge that the size and complexity of institutions differs. As a result, risk management policies and processes are expected to be commensurate with "the size and complexity of the institution"7 and "the level of risk and complexity of its third party relationships"8. During the February 2014 Risk Management Association (RMA) Vendor Management Roundtable, the OCC informally acknowledged that board of directors may choose to delegate some of their responsibilities to a senior level committee. This does not minimize the responsibility of the board, but can help manage a heavy workload.

In larger institutions, implementing a senior level third party governance committee is becoming a common practice. A strong governance committee can deliver timely, consistent oversight, act as an informed point of escalation and enable informed decision-making on key issues. In smaller institutions, the board may already be directly involved in establishing and governing critical third party relationships.

Alignment between Operational Risk and Procurement

Most financial institutions have implemented professional procurement functions in the past ten to fifteen years. Until now, their primary goal has been to reduce costs by leveraging professional procurement practices and consolidating spend. Many, but not all, of these organizations have the authority and competencies necessary to effectively integrate procurement and third party risk management. More recently, institutions have made significant investments in operational risk management, built on the concept of the three lines of defense. Both procurement and risk management will continue to evolve, but must now learn how to evolve together, in tandem.

Regulatory requirements are bringing procurement and operational risk together more closely than ever before. Regardless of which is responsible for the Framework, Policies, Standards, processes and practices for third party management, each function must learn a great deal more about the professional disciplines embedded in the other's area of expertise. Misalignment between these two departments will result in a failure to meet business and regulatory expectations.

Reputation risk arises when the actions or poor performance of a third party causes the media or the public to form a negative opinion about a financial institution. Reputation risks are typically due to failure in one or more risk factors.

Following completion of contract negotiations, and once contractual, performance and operational controls have been established, Residual Risk should be assessed and a **Residual Risk rating** calculated. Residual risk is a consolidated measure of the risks that remain after mitigating actions to reduce or eliminate inherent risks have been implemented, and the effectiveness of controls for remaining risks has been determined. All third party risks are owned by the line of business, so Residual Risk should be approved by the accountable executive.

Document, Document, Document

Each institution designs a third party management program to comply with regulatory requirements, meet management's expectations and conform to internal operations. Senior management should have a good understanding of their institution's third party risk management program, key design decisions and rationale. Effective third party risk management is a journey.

Comprehensive Framework, Policies, and procedures will guide this unprecedented level of matrixed activities to identify, assess, manage and control risk. Another relatively new

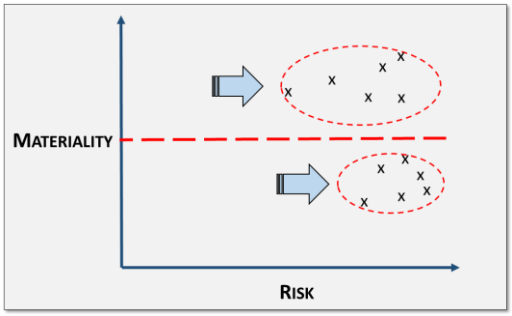
aspect of regulatory guidance is a demonstrated ability to manage, store and access documentary evidence of assessments and activities to identify, assess, manage and control third party risk throughout the lifecycle of these relationships. Regulators expect investments in processes, people and technology to be commensurate with the size and complexity of the institution and its third party relationships.

Some institutions have developed a multi-year Roadmap to describe how their program will evolve over time. A well-constructed Roadmap can guide evolution of the program in an iterative, structured manner and enable steady progress.

Oversight and Governance

Management reporting creates insight into the portfolio of third party relationships, risks by risk factor, line of business third party risk, and critical relationships. Senior management's focus should be on the most critical relationships, commonly called material relationships, and those that present the highest levels of risk.

Sharpening Your Focus



Management reporting should distinguish between materiality and risk.

Materiality is a measure of how critical the third party relationship is to the institution or line of business.

Risk is how risky the third party is to your institution as a result of its own internal controls and practices.

The more material the third party relationship is to the institution or the line of business, the greater the impact on operations and to customers if there is a significant failure.

The higher the level of risk, the more time, effort and resources your institution will invest in creating and managing controls, developing risk mitigation strategies and contingency plans, and monitoring and managing the relationship and performance.

Senior management should understand why third party relationships are designated as material or high risk, and whether these relationships are performing to contract and expectations. Unlike non-performing loans, processes for managing non-performing third parties are underdeveloped.

Key Risk Indicators and **Risk Appetite versus Risk Tolerance** are the foundation on which actionable trend analysis and reporting are built. Key Risk Indicators are the metrics by which third party risk is measured. Risk Appetite is the amount of risk the institution and the lines of business are willing to take on. Risk Tolerance is the amount of risk they've actually assumed.

These metrics are relatively new in most institutions. As institutions collect information over time, the quality of information and the ability to create actionable insight will improve over time.

Consumer Financial Protection Bureau (CFPB)

The CFPB is a relatively new regulatory body established by Congress to protect consumers by carrying out federal consumer financial laws. Financial Institutions with assets in excess of $10 billon are regulated by the Consumer Financial Protection Bureau.

With a contingent of enforcement attorneys participating in every exam, institutions have no second chances to comply if there are violations by their third parties. Regardless of the cause of the violation, the financial institution itself is solely responsible for all fines and sanctions. Cost recovery by the financial institution from the third party is prohibited by the CFPB.

Financial institutions should identify all third parties (or any of their sub-contractors) in direct communication with its customers, and all third party products the institution is reselling. These relationships are subject to third party risk management throughout their lifecycle.

In the past four years, CFPB supervisory work "contributed to recent enforcement actions against GE Capital Retail Bank, ACE Cash Express, U.S. Bank, Flagstar Bank, and M&T Bank resulting in relief of approximately $308 million to more than 1.2 million consumers for illegal practices related to credit cards, payday loans, mortgage servicing, and checking accounts".[9] A CFPB study reveals that no institution or third party is fully complying with credit card product rules.

Conclusion

Today, virtually every financial institution spends more than 30% of their total operating costs with third parties. Many lines of business are dependent on revenue share agreements and/or the ecosystem of services with and through their third party relationships. These relationships touch every aspect of every business, most of the institution's customers, and all of their employees.

Approaching third party management merely as a compliance exercise is no longer acceptable to regulators. Nor will it provide appropriate levels of visibility and control necessary to systematically reduce operational risks and improve business outcomes.

There are significant benefits and advantages to developing and deploying robust third party management programs. Institutions that embrace new practices, processes and technologies that truly enable effective management of third party costs, risks and performance will build a lasting genuine competitive advantage.

References

1. OCC Bulletin 2013-29, page 16: “Supervisory Reviews of Third-Party Relationships”
2. OCC Bulletin 2013-29, page 1: “Summary”
3. FRB SR-19, CA 13-21, page 1: “Purpose”
4. FRB SR-19, CA 13-21, page 2: “Board of Directors and Senior Management Responsibilities”
5. OCC Bulletin 2013-29, page 13: “Board of Directors”
6. OCC Bulletin 2013-29, page 6: Risk Management”; FRB SR-19, page 43 “Due Diligence and Selection of Service Providers”, FFIEC Outsourcing Technology Services: page 5 “Risk Management”
7. FFIEC Outsourcing Technology Services 2004. Page 3 “Board and Management Responsibilities”
8. OCC Bulletin 2013-29, page 1: “Highlights”
9. CFPB Supervisory Highlights Fall 2014:, page 3: Introduction

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.

We are fortunate to have earned the business of some of the greatest brands in the world who leverage the Hiperos Network and the power of Hiperos 3PM™ to protect their organizations against reputational impact, regulatory exposure, and revenue loss. Our customers include many of the world's leading companies such as Aetna, Alcoa, AON, Arrow Electronics, Astra Zeneca, AXA, Bank of Montreal, CA Technologies, Charles Schwab, Halliburton, Huntington Bank, Kraft Foods, Mondelez, Microsoft, News Corporation, Peabody, PNC Bank, Rockwell Automation, Sun Life Financial, State Street, TD Bank, and United Technologies.

We recognize the ever-increasing pressure on organizations to do more with less in an environment where the number of third parties, third party relationships, regulations, elements of risk, and costs continue to increase, with no signs of a slowdown. Our dedication to optimize the user experience and create innovative ways for our customers to take control and has led to the highest user adoption rates, and the lowest total cost of ownership.

Whatever your current or future business drivers for third party management, Hiperos is there to support you every step of the way; from initial planning and due diligence, to risk management, regulatory compliance requirements, compliance management, onboarding, contract risk management, and performance management. Hiperos solutions are proven to make you and your third party relationships more effective and to ensure you drive value in days and weeks, not months and years.

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

About the author

Linda Tuck Chapman, CPO Emeritus, President Ontala Performance Solutions Ltd. and in affiliation 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

Deleted: &

Deleted: ,

Deleted: ,