THIRD-PARTY RISK MANAGEMENT ROUND TABLE

THE POWER OF COLLABORATION

BY LINDA TUCK CHAPMAN

MEMBERS OF RMA's Third-Party Risk Management Round Table are experienced leader-practitioners, individually and collectively creating emerging best practices in third-party risk management. As the round table's facilitator, subject matter expert, and member of the Steering Committee, it's exciting and rewarding for me to be integral to this evolution.

The pace is really picking up. Institutions across the sector are taking third-party risk management very seriously, and a new professional discipline is emerging. It's fair to say that third-party risk management is on the minds of senior management, practitioners, and, increasingly, boards of directors.

This focus was highlighted in the RMA's 2015 Vendor/Third-Party Risk Management Survey, developed by the RMA Third-Party Risk Management Round Table Steering Committee and sponsored by Metric Stream. (For more on the survey, see Susan Palm's article, "Third-Party Risk Management: Moving Up the Maturity Curve," in the May issue of *The RMA Journal*.)

Thanks to the practitioners from 80 financial institutions who responded to the survey, RMA now has a valuable body of research data to share. In addition to questions about non-vendor practices, the 2015 RMA survey also included questions associated with vendor and non-vendor third-party relationships and practices.

The survey separated institutions by asset size: 1) less than $10 billion, 2) between $10 billion and $50 billion, 3) between $50 billion and $100 billion, and 4) over $100 billion. On almost every dimension, institutions in the $50 billion to $100 billion range have made the most progress. The reason may be that they are large enough to invest the necessary resources, yet small enough to be in a position to wrap their arms around this topic and drive it forward in an orderly manner.

One of the most significant changes to third-party risk management is the scope. Unlike the 2014 survey results, in 2015 the scope of programs expanded well beyond the vendor population. In fact, more than 90% of responding institutions have captured and are managing all critical third-party relationships throughout their life cycle or are in the process of doing so.

In preparation for the 2015 survey, the RMA Third-Party Risk Management Round Table Steering Committee created two definitions that cover all types of third-party relationships. These definitions improve the level of clarity around the questions and responses, especially with regard to the commonality and differences between vendor and non-vendor programs and practices.

THIRD-PARTY RELATIONSHIPS INCLUDE		Any entity, including individuals and affiliates, that has a business relationship with the institution or its customers and is itself not a customer. This includes vendors and non-vendors.
	Non-Vendors	Are typically acquired directly by a business line or segment, not through a procurement process. Financial remuneration, if applicable, is typically transacted outside of the accounts payable processes. These relationships may be managed solely by a business line or segment, or managed in conjunction with a corporate risk management function. Requirements vary.
	Vendors	Are relationships that are typically sourced through a procurement process. Payment is transacted by accounts payable. These relationships are managed by the first line of defense, using the same or similar requirements.

Reassessing the Non-Vendor Component

Survey results provide interesting insight into what's happening with the non-vendor component of third-party risk management programs, including how non-vendor relationships are captured and addressed. In the 2015 survey, 51% of participating institutions rated the non-vendor component of their program as substantially mature. This may be overly optimistic, considering the responses to questions about specific program elements. One may question whether these self-assessments are accurate, or whether expectations are so new that it's more that practitioners don't know as much as they need to.

To provide context, let's look back at the 2014 survey results. At that time, 86% of participating institutions rated their third-party risk management program as substantively mature. Despite regulatory guidance to the contrary, non-vendor relationships were not in scope. In the 2015 survey, this number fell from 86% to 71%.

This drop in confidence has been reinforced during discussions around RMA's Third-Party Risk Management Round Table. Several member institutions reported that they are retracing their steps, now that they have more experience. They're reworking and improving risk assessments and risk calculators and monitoring requirements. And regulators are still issuing matters requiring attention (MRAs) at almost the same rate as in prior years. This is not surprising. Third-party risk management is now part of almost every regulatory exam.

The first step in developing anything new is to assess its current state. Of all the institutions participating, 71% have a complete inventory of non-vendor relationships or are in the process of creating one. Institutions with an asset base of

between $50 billion and $100 billion are out in front with an 87% completion rate.

In sharp contrast to the situation in 2014, 44% of institutions have created the non-vendor component of their third-party risk management program. Some 75% of institutions from two groups categorized by asset size—those between $10 billion and $50 billion and those between $50 billion and $100 billion—report that the non-vendor component of their program is substantially similar to the vendor component and they use the same policies and standards.

Categories of Non-Vendor Relationships

In addition to creating definitions of vendor and non-vendor third-party relationships, the RMA Third-Party Risk Management Round Table Steering Committee, with valuable contributions from 11 member institutions, created a list of 19 categories and 52 subcategories of non-vendor relationships. Round table members agreed that these made sense in the context of their business. Practitioners, please feel free to use this list. Sharing knowledge and expertise across the sector is a key part of RMA's mandate.

In the survey, each of these categories was presented with a brief description and one or two examples. They were then used to gather specific information about four practices, by category: 1) how non-vendors are procured, 2) how they are governed, 3) what the contracting norms are, and 4) which function is responsible for internal reporting. There are notable differences between the practices in smaller versus larger institutions.

Regardless of the size of the institution, financial market utilities (such as SWIFT, the Depository Trust & Clearing Corporation, and Automated Clearing House) are leading the "in scope" pack, with 75% of institutions responding positively. These non-vendor financial institutions are beginning to experience an onslaught of requests about the strength of their third-party risk management programs, as well as incoming due diligence questionnaires.

Correspondent banking is next on the list of "in scope" relationships (64%), followed closely by affiliate relationships (60%), and joint marketing and co-branding relationships (58%). Notable absences from the list of top in-scope relationships include servicers (55%) and indirect lending (33%).

THE STEERING COMMITTEE,
WITH VALUABLE CONTRIBUTIONS FROM **11** MEMBER INSTITUTIONS, CREATED A LIST OF **19** CATEGORIES AND **52** SUBCATEGORIES OF NON-VENDOR RELATIONSHIPS.

1	Analysts and Advisors
2	Agents
3	Affiliates
4	Affinity Relationships
5	Alliances and Partnerships
6	Brokers
7	Correspondent Banking
8	Counterparties
9	Debt Underwriters, Securitization, Trustees
10	Financial Product Providers
11	Financial Market Utilities (FMUs)
12	Government Special-Purpose Entities (GSEs)
13	Indirect Lending
14	Joint Marketing and Co-branding
15	Rating Agencies
16	Servicers
17	Tenants
18	Trade Associations
19	Wholesale Banking

Comparing the Vendor and Non-Vendor Components

An emerging theme across the sector is that the vendor and non-vendor components of third-party risk management programs can be substantially the same or similar to the point of contract execution. Past that point, they are notably different.

For vendor third-party relationships, management, monitoring, and reporting are quite similar across the board. For non-vendor relationships, the first line of defense and the risk control functions typically work together to define these practices on a category-by-category basis. The first line of defense then reports key data and results to a central group, which also provides overall governance.

Although practitioners have suggested that the population of non-vendors in their program will exceed the vendor population, results in the 2015 RMA survey dispute this assumption. Regardless, the numbers of non-vendor third-party relationships are significant and still growing. While this aspect of third-party risk management is only a year into execution, larger institutions have already captured more than 2,500 non-vendor relationships in their programs today. As senior managements and practitioners learn more, these numbers are expected to continue growing.

Some institutions that were given a clean bill of health in prior regulatory exams have received an unwelcome surprise in more recent exams—in many cases, because they fell out of step with the evolution of third-party risk management programs and practices in their peer institutions.

With another year of the vendor component of third-party risk management behind us, the headcount for resources dedicated to third-party risk management in centralized and center-led functions is growing. While 55% of smaller institutions have fewer than three dedicated full-time equivalents (FTEs), 47% of the largest institutions now have more than 25 dedicated FTEs.

Whether the relationship is with a vendor or a non-vendor third party, the primary drivers for risk identification are the products or services provided and the risk rating as determined by the risk calculator in the risk assessment questionnaire. For vendors and non-vendors alike, risk segmentation is determined primarily on the basis of risks that are present, as well as criticality or reliance.

Other Third-Party Issues

FFIEC published "Appendix J: Strengthening the Resilience of Outsourced Technology Services" about a year ago. This is very detailed guidance, offering much greater clarity regarding expectations. As a result, 70% of responding institutions now require their business units to have documented contingency plans and exit strategies for critical vendors and activities. Depending on their quality, this guidance may be having a positive impact on the resiliency of the sector.

Cyber insurance is relatively new, but 31% of responding institutions require it of third parties with access to nonpublic personal information and 24% have their own policy in place.

Workload is becoming a serious issue. Consider that to meet the "completeness" test, all new, renewing, and amending third-party relationships are in scope for processes associated with identification, assessment, management, and controlling relationships throughout their life cycle. Then add in the many tasks and activities required for keeping close tabs on critical relationships, managing incidents and issues, and refreshing due diligence on a risk-adjusted basis.

To increase efficiency in program execution, 74% of institutions either have granted blanket exceptions for specific types of relationships, or plan to do so. These include third-party relationships that they consider to be inherently low risk. Specifically, they cite food services, travel, office supplies, equipment, certain types of real estate transactions, corporate sponsorships, shrink wrap software, regulatory agencies, and transactions of less than $2,500.

One creative institution is implementing a new technology that enables premapping of specific spend categories and service types to a risk tier. Relationships in the low-risk categories are exempt from due diligence and ongoing management activities. To meet the completeness test, these relationships are recorded in the third-party risk management program "book of record" software.

Aside from information security assessments, few institutions have outsourced third-party due diligence assessments.

Another great opportunity to improve workload management is to acquire automated data feeds and alerts, independent due diligence reports, and other data from third-party providers. This is a nascent practice today, but it is expected to gain traction in the next year or two.

There has been great progress in the use of standard contracts and risk control clauses for third-party relationships. Some 60% of responding institutions have implemented this practice. As one respondent commented, "We have a list of key clauses we require for all contracts. When we review new contracts, we negotiate inclusion or require a formal exception approval."

In terms of heightened oversight, 66% of responding institutions have specific risk oversight committees in place, formed specifically to oversee third-party risks. And oversight has risen to a much higher level. In 22% of responding institutions, this committee reports to the board of directors, and 35% of responding institutions report that their risk oversight committee reports to the risk, operational risk, or audit committee of the board. This is dramatically different from 2014, when institutions were still trying to determine whether they needed a third-party risk oversight committee.

For those institutions that have not reached an acceptable level of maturity, the most frequently cited regulatory findings were related to completeness (47%), consistency (19%), monitoring (19%), and governance and oversight (13%). Some specific deficiencies include inconsistent reviews by risk control groups, subcontractor assessments, cybersecurity, model risk, and concentration risk.

Conclusion

The 12 months between the 2014 and 2015 surveys passed so quickly. Investments are being made, and practitioners across the sector are collaborating and openly sharing their expertise, experiences, challenges, and solutions. Best practices are emerging. Senior managements and boards are keenly engaged.

The pace has picked up and the results are impressive. Seventeen participating institutions reported that their most recent regulatory program review was "MRA free." Bravo! ®

WITH ANOTHER YEAR OF THE VENDOR COMPONENT OF THIRD-PARTY RISK MANAGEMENT BEHIND US, THE HEADCOUNT FOR RESOURCES DEDICATED TO THIRD-PARTY RISK MANAGEMENT IN CENTRALIZED AND CENTER-LED FUNCTIONS IS GROWING.

Linda Tuck Chapman is an expert in third-party risk management, specializing in financial services. As president of Ontala Performance Solutions and former chief procurement officer of three major banks, she brings practical, hands-on expertise to designing, assessing, and enhancing third-party risk management programs. She can be reached at lindatuckchapman@ontala.com.