THE RMA

THIRD-PARTY/VENDOR RISK MANAGEMENT SURVEY

AN EXPERT'S INSIGHTS

THE GOAL WAS TO ESTABLISH A 2014 BASELINE OF CURRENT PRACTICES FROM WHICH FINANCIAL INSTITUTIONS CAN MEASURE PROGRESS OVER TIME.

SHUTTERSTOCK, INC.

BY LINDA TUCK CHAPMAN

In late 2013 the Office of the Comptroller of the Currency and the Federal Reserve issued updated guidance on third-party/vendor risk management. In response to increased regulatory pressure on its members to implement effective programs in this area, RMA established a new Vendor Management Round Table.

This new round table offers an opportunity for risk management practitioners from across the North American financial services sector, including foreign-owned entities, to meet on a regular basis to discuss current issues, challenges, and solutions, as well as identify opportunities for accelerating advances in third-party/vendor risk management practices.

The agenda and direction for each Vendor Management Round Table are developed by a steering committee consisting of Deborah Manos-McHenry, chief sourcing officer, Huntington National Bank; Linda Tuck Chapman, president, Ontala Performance Solutions and chief procurement officer emeritus; Eric Sierka, senior vice president and head of procurement risk governance and contract, strategic sourcing, TD Financial Group; John Klapmust, senior vice president and head of operational risk, One West Bank FSB; Ed DeMarco, director of operational risk and general counsel at RMA; and Sylwia Czajkowska, associate director of operational risk at RMA.

This collaboration resulted in a sector-wide survey of the state of third-party/vendor risk management. The goal was to establish a 2014 baseline of current practices from which financial institutions can measure progress over time.

The Results

The RMA Third-Party/Vendor Risk Management Survey was a resounding success, gathering responses from 114 participants in 102 financial institutions. These institutions are in the jurisdiction of all primary regulators in North America—the OCC, Federal Reserve, FDIC, Financial Industry Regulatory Authority, Securities and Exchange Commission, state banking agencies, and Office of the Superintendent of

KNOWING WHO YOUR CRITICAL VENDORS ARE IS FOUNDATIONAL TO EFFECTIVE THIRD-PARTY RISK MANAGEMENT.

Financial Institutions. Some 97% of the respondents are directly responsible for third-party/vendor risk management in their institutions.

The intent of the survey was to obtain information of sufficient detail to allow individual institutions to compare the current state of their vendor management program with those of peer financial institutions and the financial services sector in general. Responses were consolidated in order to safeguard the confidential information provided, and none of the responses in the final report can be attributed to an individual institution.

For most of the questions, the responses are relevant to all financial institutions, regardless of size. In circumstances where this did not apply, the responses were analyzed and reported according to the asset sizes of the institutions, grouped as follows: 1) under $10 billion, 2) $10 billion to $50 billion, 3) $50 billion to $100 billion, and 4) over $100 billion.

Background Information

Prior to the introduction of relatively new risk management practices that separate the roles and responsibilities of operational risk management into the "first, second, and third lines of defense," responsibility for vendor risk management was not defined.

Before rigorous third-party risk management (3PRM), some of these responsibilities rested with the sourcing and procurement function, if one existed. A key metric of its success continues to be cost savings. Business leaders typically involved this function at their discretion. Accordingly, sourcing and risk experts may not have been aware of activities to initiate, renew, or amend third-party/vendor relationships.

Sourcing and procurement typically assumed responsibility for gathering risk-related information as part of the request-for-proposal process. In their responses to RFPs, vendors were usually required to submit certain risk-related information, such as financial statements, details concerning company officers, and information security and business continuity practices. Risk experts, such as those in information security and privacy, may or may not have been involved in assessing risks.

As a result, before heightened regulatory expectations were introduced in 2008 and 2013, due diligence, risk analysis, and risk controls were inconsistent at best. Risks were rarely documented, and relationships were never formally risk rated. Line-of-business (LOB) leaders had full authority to accept risks of virtually any type or level of exposure.

Relationships with non-vendor third parties such as debt buyers, correspondent banks, channel partners, and indirect auto lenders were typically established entirely by LOB leaders. As a result, they have not been subject to any risk oversight.

OCC Bulletin 2013-29 makes it clear that effective risk management includes all third parties. This means relationships with any entity that is not a customer, regardless of whether there is a formal contract in place.

3PRM Program Maturity

In response to the request "Rate the maturity level of your vendor management program," respondents reported the following:

TABLE 1: RATE THE MATURITY LEVEL OF YOUR VENDOR MANAGEMENT PROGRAM

	<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
1 Completely mature	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
2	29	25.4%	16	26.2%	5	22.7%	2	18.2%	6	30.0%
3	58	50.9%	30	49.2%	10	45.5%	7	63.6%	11	55.0%
4	21	18.4%	13	21.3%	4	18.2%	1	9.1%	3	15.0%
5 Not mature at all	6	5.3%	2	3.3%	3	13.6%	1	9.1%	0	0.0%

On average, 50% of survey respondents believe that their program is at a reasonable level of maturity.

Knowing who your critical vendors are is foundational to effective third-party risk management. Here is what respondents said in answer to "Describe the definition of 'critical activity' used at your institution":

TABLE 2: DESCRIBE THE DEFINITION OF 'CRITICAL ACTIVITY' USED AT YOUR INSTITUTION

	<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
Undefined	3	2.7%	3	5.1%	0	0.0%	0	0.0%	0	0.0%
In the process of being defined	53	47.3%	24	40.7%	8	36.4%	8	72.7%	13	65.0%
Already fully defined	56	50.0%	32	54.2%	14	63.6%	3	27.3%	7	35.0%

With only half of respondents having fully defined critical vendors, it is natural to question their assessments of the maturity level of 3PRM programs. Maturity assessments should determine completeness. For institutions regulated by the OCC and Consumer Financial Protection Bureau, in-scope third-party relationships extend beyond "traditional" vendors.

Accordingly, responses to the maturity assessment question should also be considered in the context of responses to

a related question: "What types of third parties are in your organization's program today? (Select all that apply.)"

procurement (19%). Other functions that have responsibility include compliance, legal, and IT/operations.

TABLE 3: WHAT TYPES OF THIRD PARTIES ARE IN YOUR ORGANIZATION'S PROGRAM TODAY?

			<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
Agents	60	52.6%	31	50.8%	12	54.5%	3	27.3%	14	70.0%
Agency agreements	54	47.4%	27	44.3%	9	40.9%	4	36.4%	14	70.0%
Channel and distribution agreements	59	51.8%	31	50.8%	11	50.0%	4	36.4%	13	65.0%
Debt buyers	22	19.3%	6	9.8%	5	22.7%	1	9.1%	10	50.0%
Co-branded products or services	62	54.4%	32	52.5%	13	59.1%	4	36.4%	13	65.0%
Affiliates ownership < 50%	21	18.4%	7	11.5%	3	13.6%	2	18.2%	9	45.0%
Correspondent banking agreements	56	49.1%	28	45.9%	10	45.5%	3	27.3%	15	75.0%
Other (please specify)	33	28.9%	19	31.1%	6	27.3%	3	27.3%	5	25.0%

On average, fewer than 50% of participating institutions have defined "critical vendors" and/or have expanded the scope of their 3PRM program to include "non-vendor" third parties. And only a handful included debt buyers and affiliates, which have access to highly regulated customer data or trade secrets.

Reinforcing concerns about slow progress in 3PRM program development or weakness in managing third-party risk, many regulatory exams have resulted in MRAs (matters requiring attention), MRIAs (matters requiring immediate attention), consent, or other enforcement orders. Common deficiencies are found in due diligence, governance, monitoring, reporting, data quality, financial viability assessment, and outdated contract terms.

This raises the question of whether, at the time of the survey, practitioners had an understanding of regulatory expectations, and how the maturity level of their 3PRM program stacks up with regulatory expectations and with programs in peer institutions.

Roles and Responsibilities

Responsibility for developing and maintaining the framework, policy, and standards for 3PRM is predominantly in enterprise risk management (48%), followed by

These numbers change according to asset size. In financial institutions with assets ranging from $50 billion to $100 billion, procurement is responsible 55% of the time. In the largest institutions, responsibility is predominantly in procurement (35%) or the shared services/vendor management office (30%).

Regardless of the institution's asset size or which function owns the framework, policy, and standards, responsibility for third-party risk management oversight lies predominantly with enterprise risk management, including operational risk management committees.

Oversight of a second-line-of-defense function (third-party risk management) by another second-line-of-defense function (enterprise risk management) may be causing some confusion. This lack of clarity is expected to resolve itself as 3PRM matures.

Regulatory guidance makes it clear that the line of business owns any risks

REGARDLESS OF THE INSTITUTION'S ASSET SIZE OR WHICH FUNCTION OWNS THE FRAMEWORK, POLICY, AND STANDARDS, RESPONSIBILITY FOR THIRD-PARTY RISK MANAGEMENT OVERSIGHT LIES PREDOMINANTLY WITH ENTERPRISE RISK MANAGEMENT.

associated with their third-party relationships. An average of only 43% of institutions have a quality assurance process to validate risk management activities and monitoring by the first line of defense. Larger institutions have a higher positive response rate (more than 60%).

In addition to reliance on a wide range of risk experts, there is a very large role for the lines of business. Here is how the majority of institutions responded to "In my organization, vendors are managed…":

TABLE 4: IN MY ORGANIZATION, VENDORS ARE MANAGED…

			<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
Centrally	18	15.9%	14	23.3%	3	13.6%	0	0.0%	1	5.0%
In the business	79	69.9%	42	70.0%	13	59.1%	9	81.8%	15	75.0%
Other	16	14.2%	4	6.7%	6	27.3%	2	18.2%	4	20.0%

While many institutions have implemented centralized oversight with decentralized vendor owners, there may be a lack of consistency in specific tasks and risk assessments throughout the life cycle of third-party relationships. Comments submitted with survey responses include the following:

- There is a move toward centralization of certain activities, such as central databases for documentation.
- Business owners handle due diligence, risk assessment, negotiation, and renewal of contracts.
- All functional heads have responsibility for their respective areas.
- Vendor risk management oversees true vendors centrally, but non-vendor third parties are decentralized and oversight is conducted by various teams.

In an effective, evidence-based 3PRM program it is crucial to have clear ownership, accountability, and consistency and to be able to document that 3PRM activities have been completed (trust, but test). It is important to clarify the roles and responsibilities of subject-matter experts in third-party risk.

Here is how survey respondents replied to the question "What areas of your organization are involved in active due diligence and vendor selection?":

TABLE 5: WHAT AREAS OF YOUR ORGANIZATION ARE INVOLVED IN ACTIVE DUE DILIGENCE AND VENDOR SELECTION?

			<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
IT	104	91.2%	58	95.1%	21	95.5%	11	100.0%	14	70.0%
Business Continuity Management/ Planning	78	68.4%	40	65.6%	13	59.1%	9	81.8%	16	80.0%
Compliance	86	75.4%	46	75.4%	17	77.3%	8	72.7%	15	75.0%
Legal	81	71.1%	35	57.4%	17	77.3%	9	81.8%	20	100.0%
Information Security	104	91.2%	53	86.9%	20	90.9%	11	100.0%	20	100.0%
Human Resources	22	19.3%	11	18.0%	4	18.2%	2	18.2%	5	25.0%
Finance	70	61.4%	39	63.9%	12	54.5%	7	63.6%	12	60.0%
SMEs	45	39.5%	17	27.9%	13	59.1%	5	45.5%	10	50.0%
Other (please specify)	30	26.3%	12	19.7%	5	22.7%	4	36.4%	9	45.0%

Given the intense regulatory focus and the daily threat of cyber attacks, it is surprising to see anything less than 100% in response to a question about involvement in information security.

In larger institutions, more than 80% of companies send out risk assessment questionnaires. This number drops to 39% in the smallest institutions. The majority of institutions also conduct periodic site visits for critical vendors (73%) and/or secondary due diligence, which means more in-depth risk assessments than simply questions included as part of an RFP.

The following secondary risk assessments are being conducted (numbers in parentheses indicate percentage of respondents):

- Information security (79%).
- Technology (67%).
- Business continuity management (46%).
- Legal (31%).
- Privacy (30%).
- Other (35%): credit, anti-money-laundering, compliance, physical security, and insurance.

Despite regulatory guidance on monitoring relationships throughout their life cycle, some programs may be deficient in this area. This conclusion was suggested by responses to the question "In addition to RFP questions, how often do you send questionnaires to your vendors for risk assessment purposes?":

TABLE 6: IN ADDITION TO RFP QUESTIONS, HOW OFTEN DO YOU SEND QUESTIONNAIRES TO YOUR VENDORS FOR RISK ASSESSMENT PURPOSES?

			<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
Only when doing due diligence on the vendor	21	29.6%	14	48.3%	3	20.0%	2	20.0%	2	11.8%
Annually	24	33.8%	10	34.5%	6	40.0%	3	30.0%	5	29.4%
When the performance is not satisfactory	3	4.2%	1	3.4%	1	6.7%	0	0.0%	1	5.9%
Other (please specify)	23	32.4%	4	13.8%	5	33.3%	5	50.0%	9	52.9%

Customization of questionnaires may make it challenging to compare risk exposure across a portfolio of third-party relationships if an institution is among the 41% that customize risk assessment questionnaires for individual third-party relationships.

Risk Tiering

To ensure risk management activities are commensurate with the level of risk (risk adjusted), institutions typically segment their vendor relationships, mostly by level of risk. A handful of institutions segment relationships by spend (dollars). Spend may be an indicator of the strategic importance of the relationship, but it is not an indicator of the level of risk. In the majority of institutions, there are either three (43%) or four (27%) risk tiers.

Risk and criticality are not the same thing. Criticality is how much of an impact the third-party relationship will have on an institution or line of business in the event of a material failure to deliver services, a breach, or poor performance. Risk is an assessment of the many categories of risk

each relationship presents to an institution. This includes the risk exposure and impact if things go wrong.

The number of in-scope vendors in 3PRM programs varies widely and is not necessarily directly correlated to size. Here is what the survey revealed about the number of vendors in 3PRM programs, by asset size.

- *< $10 billion:*
  97% have < 500 vendors
- *$10-50 billion:*
  50% have < 1,000 and 50% have > 2,500 vendors
- *$50-100 billion:*
  46% have < 500 and 46% have > 2,500 vendors
- *> $100 billion:*
  40% have < 1,000 and 50% have > 2,500 vendors

In smaller institutions, the number of in-scope vendors included in 3PRM programs is generally expected to grow over the next two years. In larger institutions, the majority of respondents expect this number to retract.

Not all "critical" relationships are equal. Among in-scope critical relationships are those relationships that have the potential to affect the entire enterprise. Some institutions call these "enterprise critical" relationships. In response to a question about the number of enterprise critical relationships, 60% of institutions have fewer than 15 and 29% of institutions have more than 25. As might be expected, these numbers closely correlate to the asset size of the institution.

In addition to due diligence conducted at the time the relationship is established, 78% of institutions reassess risk every year.

Other Considerations

Concentration risk assessments rely on mature programs. Currently, 66% of institutions don't identify vendor concentration risk across their portfolio of risks. Only 57% use standard contracts and only 23% have a standard Supplier Code of Conduct that they must acknowledge. Fourth-party (subcontractors) risk assessment processes are not yet mature. Only 33% perform due diligence on fourth parties. One respondent asked, "What is a fourth-party supplier?" and another said, "Hopefully, business areas are asking about subcontractor usage."

Cyber liability insurance is becoming more common: 67% of respondents require cyber insurance from vendors that handle confidential information.

AMONG IN-SCOPE CRITICAL RELATIONSHIPS ARE THOSE RELATIONSHIPS THAT HAVE THE POTENTIAL TO AFFECT THE ENTIRE ENTERPRISE.

Resources

Investment in technology and people is an issue. Of the responding institutions, 86% rely on Excel® or are using in-house solutions. Considering the complexity, commitments, regulatory issues, and workload, institutions may be reconsidering whether they have invested sufficiently in people and resources. The survey asked, "How many FTEs are dedicated to third-party management in the centralized/center-led supplier risk management oversight function?":

TABLE 7: HOW MANY FTEs ARE DEDICATED TO THIRD-PARTY MANAGEMENT IN THE CENTRALIZED/CENTER-LED SUPPLIER RISK MANAGEMENT OVERSIGHT FUNCTION?

			<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
< 3	67	60.4%	53	91.4%	9	40.9%	3	27.3%	2	100.0%
3 - 5	14	12.6%	1	1.7%	9	40.9%	2	18.2%	2	10.0%
6 - 10	10	9.0%	2	3.4%	3	13.6%	2	18.2%	3	15.0%
11 - 15	9	8.1%	1	1.7%	1	4.5%	3	27.3%	4	20.0%
16 - 25	5	4.5%	0	0.0%	0	0.0%	1	9.1%	4	20.0%
> 25	6	5.4%	1	1.7%	0	0.0%	0	0.0%	5	25.0%

OPPORTUNITIES TO COLLABORATE AND LEARN

IN FORUMS LIKE THIS SURVEY AND THE RMA VENDOR MANAGEMENT ROUND TABLE ARE A GOOD WAY TO ADVANCE YOUR INSTITUTION'S 3PRM PROGRAM IN THE RIGHT DIRECTION AND AT THE RIGHT PACE.

This information is hard to interpret at just a glance. Analysis reveals that, in smaller institutions, there is one person in the oversight function for every ~200 vendor relationships. In larger institutions, each person is responsible for ~100 vendor relationships.

Risk Oversight

The majority of institutions report risk issues to the company's line of business, risk experts, and upper management (77%) and/or operational risk and management committees (67%). Only 12% of institutions conduct trend analysis to evaluate the overall risk the vendor relationship poses to the company.

Risk appetite is a relatively new concept, confirmed by responses to the question "For which of the following risks does your organization report risk tolerance versus risk appetite?":

TABLE 8: FOR WHICH OF THE FOLLOWING RISKS DOES YOUR ORGANIZATION REPORT RISK TOLERANCE VERSUS RISK APPETITE?

			<$10 B		$10-50 B		$50-100 B		>$100 B	
RESPONSE	#	%	#	%	#	%	#	%	#	%
Level of risk	40	42.1%	20	41.7%	11	50.0%	6	60.0%	3	20.0%
Information security	17	17.9%	9	18.8%	6	27.3%	1	10.0%	1	6.7%
Financial viability	11	11.6%	7	14.6%	1	4.5%	0	0.0%	3	20.0%
Technology	4	4.2%	4	8.3%	0	0.0%	0	0.0%	0	0.0%
Business continuity management/ planning	2	2.1%	2	4.2%	0	0.0%	0	0.0%	0	0.0%
Other (please specify)	21	22.1%	6	12.5%	4	18.2%	3	30.0%	8	53.3%

The majority of "other" responses were statements that risk appetite reporting includes all of the factors listed. Some institutions are just embarking on this leg of the 3PRM journey, as evidenced by such comments as "We have not set risk appetites yet, but are planning to" and "Appetite and tolerance [are] being revised."

Exceptions to standard contract terms and conditions are typically approved by the line of business or legal. In some cases they are escalated to a formal or informal committee for approval. There is a lack of consistency as to which group is responsible for tracking and communicating 3PRM regulatory and compliance updates or changes except in the smallest institutions, where this is predominantly the responsibility of a regulatory liaison function (45%).

Independent reviews are the cornerstone of effective 3PRM programs. Of the responding institutions, 76% are validating regulatory compliance and 3PRM program effectiveness annually. In 33% of institutions, this review is conducted by internal audit. Other responsible parties include a centralized unit (15%), different areas for business analysis (25%), a third-party auditor (13%), and other stakeholders (14%), with many reporting that this responsibility belongs to the first line of defense.

Conclusion

Effective third-party risk management is a journey and likely to be a long one. Based on the responses to RMA's 2014 Third-Party/Vendor Risk Management Survey, there is still much work to be done. As programs mature, improvement is expected in the level of rigor, depth, and scope of 3PRM.

Confirmation that your institution is on the right track can be found in praise given by regulators. This may come in the form of a regulatory exam with findings but no formal sanctions, a comment that the leadership team for 3PRM understands third-party risk management, or an observation that the institution's program is commensurate with those in other financial institutions of a similar size and complexity.

Opportunities to collaborate and learn in forums like this survey and the RMA Vendor Management Round Table are a good way to advance your institution's 3PRM program in the right direction and at the right pace. Being mindful of anti-trust regulations, regulatory agencies highly encourage collaboration. Risk management is a team sport. ®

Linda Tuck Chapman is an expert in third-party risk management and outsourcing governance. As a former chief procurement officer in three major banks and president of ONTALA Performance Solutions, and through her association with Crowe Horwarth Global Risk Consulting, she brings hands-on experience designing, assessing, and executing effective programs. She can be reached at lindatuckchapman@ontala.com.