2015 RMA THIRD-PARTY/VENDOR RISK MANAGEMENT SURVEY

FINAL REPORT
DECEMBER 2015

JOIN. ENGAGE. LEAD.

Operational Risk

ACKNOWLEDGMENTS

The survey was conducted by The Risk Management Association between August and October 2015. Most of the questions were multiple choice with many opportunities to provide comments. Some questions were open text, designed to provide information and insight about best and current practices. A total of 80 responses were received covering a wide range of types of financial institutions from four asset sizes: less than $10 billion, between $10 and $50 billion, $50 to $100 billion and over $100 billion, including community, regional, super-regional and money center banks, investment banks and insurance companies, and Financial Market Utilities headquartered in the United States, Canada, and Europe. These groupings will enable further analysis by asset size and subject matter for input into future articles in the RMA Journal.

This RMA survey was designed with the help of the RMA Vendor Risk Management Steering Committee comprised of: Debbie Manos-McHenry (Huntington Bank), John Klapmust (OneWest Bank), Eric Sierka (TD Bank) and Linda Tuck Chapman (ONTALA Performance Solutions Ltd). This RMA survey was designed to capture the range of practices in Third- Party/Vendor Risk Management over a cross section of RMA member institutions, and to gather detailed information on current and best practices and challenges in Third Party/Vendor Risk Management.

The 2014 and 2015 RMA Third Party/Vendor Risk Management surveys were conducted at the request of RMA Third Party/Vendor Risk Management Roundtable members. The 2015 survey was designed as update and expansion to similar content in the 2014 RMA survey Practices are rapidly evolving due to increased regulatory, Board and senior management due to significant changes mandated by the OCC and FRB in updated regulatory guidelines (OCC 2013-29 "Third-Party Relationships" and Fed- SR 13-19 / CA 13-21 "Guidance to Managing Outsourcing Risk") and CFPB expectations relating to vendors and other third parties.

Please note that the use of the terms "vendor" and 'non-vendor" third party throughout this survey. This is an important distinction in identification of in-scope relationships and potential difference in how institutions identify, assess, monitor and control risks throughout the lifecycle of different types of third party relationships, create and record documentary evidence and provide risk reporting.

The following definitions were developed by members of the RMA Vendor/Third Party Risk Management Roundtable and now in common use.

How are Third Parties defined for purposes of this survey?	General Definition	Any person, including any entity, individual and/or affiliate of the institution, that has a business relationship with the institution or its customers, and is not itself a customer. Third-party relationships include: non-vendor and vendor third parties.
	Non-Vendor Third Party	"Non-vendor" third-party relationships are typically developed by a business line/segment directly not through a sourcing/procurement function. Financial remuneration, if applicable, is typically transacted outside of Accounts Payable processes. These relationships may be managed solely by a business line/segment, or managed in conjunction with a corporate risk management function.
	Vendor Third Party	"Vendor" third parties are service providers/vendors that provide a product or service to the institution. These relationships are typically sourced through a sourcing/procurement process. Payment is typically rendered by Accounts Payable.

The following areas were addressed in this year's survey:

1. Program Scope, Design and Maturity
2. Key Stakeholder Roles and Responsibilities
3. Technology and Workload Management
4. Regulatory Criticism
5. Insight and Advice

The final report presentation style provides participants' responses, while protecting the confidentiality of individual institutions by masking the source of responses.
Note: Due to rounding, percentages in the tables may not add up to 100.

RMA staff members contributing to the study were Sylwia M. Czajkowska and Edward J. DeMarco Jr. The final report was written by RMA and Linda Tuck Chapman.

RMA would like to thank **MetricStream** for sponsoring this survey.

Institutions that participated in the survey:

Anonymous (3)	Amarillo National Bank
American Savings Bank	Bank of America
Bank of the West	BB&T
BBVA Compass Bank	Bank of Montreal
Beneficial Bank	Bremer Bank
Broadway National Bank	Brookline Bancorp
Capital One	CenterState Bank
Charles Schwab & Company, Inc.	Chemung Canal Trust Company
Citizens Bank	City National Bank
Colorado Federal Savings Bank	Commonwealth Bank
Community Bank N.A.	CommunityOne Bank, N.A.
Core Bank	CoreFirst Bank & Trust
Depository Trust & Clearing Corporation	Discover Financial Services
East River Bank	Fidelity Bank
Fidelity Bank of Florida	Fifth Third Bank
First Busey Corporation	First Community Bank N.A.
First Federal Lakewood	First Federal Savings Bank
First Horizon National Corporation/First Tennessee Bank N.A.	First National Bank & Trust Company
First National Bank of Omaha	First Niagara Bank
First Virginia Community Bank	Freedom Bank
GE Capital	HSBC
Huntington National Bank	Investar Bank
John Deere Financial	M&T Bank
Mechanics Savings Bank	MetaBank
Middleburg Bank	National Bank of Canada
Newtown Savings Bank	North American Savings Bank
North Middlesex Savings Bank	Nuveen Investments, Inc.
OneWest Bank N.A.	Parkside Financial Bank & Trust
Park Sterling Bank	Pittsfield Co-Operative Bank
Phoenixville Federal Bank & Trust	PNC
Progressive Savings Bank	RBC
Santander U.S Holding Co.	Savings Bank of Mendocino County
Scotiabank	Scottrade Financial Services, Inc.
State Bank of Cross Plains	State Street
Stearns Bank, N.A.	Stifel
TD Bank	The Bancorp
The Home Savings and Loan Company	U.S. Bancorp
Univest Corporation of Pennsylvania	Wells Fargo
Whitney Bank	Zions Bancorporation

Disclaimer

The information contained herein is obtained from sources believed to be accurate and reliable. All representations contained herein are believed by RMA to be as accurate as the data and methodologies will allow. However, because of the possibilities of human and mechanical error, as well as unforeseen factors beyond RMA's control, the information herein is provided "as is" without warranty of any kind, and RMA makes no representations or warranties expressed or implied to a subscriber or any other person or entity as to the accuracy, timeliness, completeness, merchantability, or fitness for any particular purpose of any of the information contained herein. Furthermore, RMA disclaims any responsibility to update the information. Moreover, information is supplied without warranty on the understanding that any person who acts upon it or otherwise changes position in reliance thereon does so entirely at such person's own risk.

The report is provided to participating institutions for internal analytical and planning purposes only. As such, a participating institution may disclose the information to consultants and agents that are engaged to assist that participating institution in analysis and planning; however, such consultant or agent is prohibited from using the information for any purpose other than such analysis and planning for that participating institution.

About RMA

Founded in 1914, The Risk Management Association is a not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA promotes an enterprise-wide approach to risk management that focuses on credit risk, market risk, and operational risk. Headquartered in Philadelphia, Pennsylvania, RMA has 2,500 institutional members that include banks of all sizes as well as nonbank financial institutions. They are represented in the Association by over 18,000 risk management professionals who are chapter members in financial centers throughout North America, Europe, and Asia/Pacific. Visit RMA on the Web at www.rmahq.org.

About MetricStream

MetricStream is simplifying Governance, Risk, and Compliance (GRC) for modern and digital enterprises. Our market-leading enterprise and cloud Apps for GRC enable organizations to strengthen risk management, regulatory compliance, vendor governance, and quality management while driving business performance.

The MetricStream GRC Journey methodology integrates GRC technologies and programs across business, IT, and security functions as we enable organizations to realize the vision of Pervasive GRC. Rich content from GRCIntelligence.com and thriving communities like ComplianceOnline.com, as well as MetricStream Special Interest Groups (mSIGs) support the ongoing success of our customers through real-time content feeds and best practices embedded in our Apps.

Leading companies across industry verticals are benefiting from MetricStream's simple and modular approach to GRC that is transforming risk management in a business environment that is increasingly mobile, social, global, and virtual. We have been consistently rated as a market leader by leading analysts, and have received several awards and recognitions for product innovation and customer success.

MetricStream is headquartered in Palo Alto, California, and has offices across the globe. Visit MetricStream on the Web at www.metricstream.com.

EXECUTIVE SUMMARY

The survey was conducted by The Risk Management Association between August and October 2015. Most of the questions were multiple choice with many opportunities to provide comments. Some questions were open text, designed to provide information and insight about best and current practices.

A total of 80 responses were received from a wide range of financial institutions including community, regional, super-regional and money center banks, investment banks, and insurance companies, and financial market utilities headquartered in the United States, Canada, and Europe. Participating institutions were asked to provide their primary regulator for context and further analysis. As expected, all participating institutions are regulated by one or more of the following: OCC, FRB, FDIC, State, FINRA, and OSFI (Canada).

This is the breakdown of participation by asset size:

Asset Size	Number of Institutions	Percent
Less than $10 Billion	45	56.3%
$10-50 Billion	8	10%
$50-100 Billion	8	10%
Greater than $100 Billion	19	23.8%

The following areas of practice were addressed in this year's survey:

1. Program scope, design, and maturity
2. Key stakeholder roles and responsibilities
3. Technology and workload management
4. Regulatory criticism
5. Insight and advice

Some questions were carried forward from the 2014 baseline survey. This will help financial services companies track their progress and evolution of practices.

Participants were asked to respond to questions about current practices for "vendor" and "non-vendor" third party relationships. It was apparent in RMA round table discussions that this is an important distinction due to different practices for identification of in-scope relationships and potential differences in how institutions identify, assess, monitor and control risks throughout the lifecycle of different types of third-party relationships, create and record documentary evidence, and provide risk reporting. The survey provides clarity on current differences in practices.

To ensure clarity in survey responses and create common language across the sector, the following definitions were developed by members of the RMA Vendor/Third-Party Risk Management Round Table. These definitions are more commonly used.

How are Third Parties defined for purposes of this survey?	General Definition	Any person, including any entity, individual and/or affiliate of the institution, that has a business relationship with the institution or its customers, and is not itself a customer. Third-party relationships include: non-vendor and vendor third parties.
	Non-Vendor Third Party	"Non-vendor" third-party relationships are typically developed by a business line/segment directly not through a sourcing/procurement function. Financial remuneration, if applicable, is typically transacted outside of Accounts Payable processes. These relationships may be managed solely by a business line/segment, or managed in conjunction with a corporate risk management function.
	Vendor Third Party	"Vendor" third parties are service providers/vendors that provide a product or service to the institution. These relationships are typically sourced through a sourcing/procurement process. Payment is typically rendered by Accounts Payable.

Program scope, design, and maturity

"Vendor" third-party risk management programs are evolving quickly. In the 2014 survey 0% of respondents described their "vendor" third-party risk management program as fully mature. In the 2015 survey, between 25% and 40% of participating institutions, depending on asset size, reported that their program is fully mature. There is evidence that the level of clarity and sense of direction are improving. For example, definitions of "critical activities" were somewhat vague in the 2014 report and are more precise in the 2015 report. Seventeen participating institutions suggest that they have experienced "clean" regulatory examinations. There are still many areas of immaturity as evidenced by the responses to question 53: "Based on our most recent regulatory examination, in which areas did you receive criticism?" It is important that the sector continues to invest and evolve its program —an important indicator of "safety and soundness."

Expansion of "vendor" third-party risk management programs to include "non-vendor" relationships has occurred since the 2014 survey was conducted. In preparation for the survey, the RMA Third-Party/Vendor Risk Management Round Table Steering Committee members, with input from eleven member institutions, developed a profile of non-vendor third parties. Definitions were validated with RMA Third-Party/Vendor Risk Management Round Table member institutions.

The list of "non-vendor" relationships common in banks and insurance companies of all sizes consists of 19 categories and 53 subcategories. These categories were used to enable common language and consistent responses about current practices:

1. Specialized analysts and advisors to executive management
2. Agents
3. Affiliates
4. Affinity relationships
5. Alliance and partnerships
6. Brokers
7. Correspondent banks
8. Counterparties
9. Debt underwriters/securitization firms/ trustees
10. Financial product providers
11. Financial utilities
12. Government Special Purpose Entity (GSE)
13. Indirect lending
14. Joint marketing partners/co-branding partners
15. Rating agencies
16. Servicers
17. Tenants
18. Trade associations
19. Wholesale banking

When participants were asked to respond to the question, " 'Non-vendor' third-party management is a regulatory requirement and/or our institution is formally addressing risk (identify, assess, manage and control)" (question 22), institutions of all sizes responded positively as follows:

	All	< $10 bil	$10 – 50 bil	$50 – 100 bil	>$100 bil
Yes	50%	33.3%	37.5%	87.5%	78.9%
No	50%	66.7%	62.5%	12.5%	21.1%

Participants who responded "Yes" were asked which of the following "non-vendor" categories of relationships are addressed in their existing third-party program. For each covered category they were also asked to respond to four questions about:

a) Governance
b) Procurement
c) Contracting
d) Reporting

The majority of responding institutions anticipate that "vendor" and "non-vendor" third-party relationships will be covered by the same policy and standards (an average of 68.2%). Practices associated with "non-vendor" third-party risk management are still immature. The 2015 RMA survey will serve as a baseline for member institutions to measure their progress over time compared to peer institutions.

Key Stakeholder Roles and Responsibilities

The majority of institutions have a "center-led" or "hybrid" approach to supporting the 1st Line of Defense in execution of their responsibilities for both vendor and non-vendor third-party relationships. "Center-led" means that there is a matrixed organization operating in partnership with risk subject matter experts. In institutions with less than $10B in assets, 40% of institutions responded that they have a completely centralized organization.

In institutions of all asset sizes the number of FTE supporting related activities has grown since the 2014 RMA survey.

	How Many FTEs are dedicated to:	
	"vendor" third-party management	**"non-vendor" third-party management**
<3	55%	77.5%
3-5	15%	8.8%
6-10	8.8%	7.5%
11-15	3.8%	1.3%
16-25	3.8%	2.5%
>25	13.8%	2.5%

This is a significant change in common practices. In 2014, "non-vendor" third parties were a limited focus or not a focus for RMA Third-Party/Vendor Risk Management Round Table participants.

To date, program development has focused on the framework, standards, processes, and tools. Based on survey results, more effort is required to fully support the 1st Line of Defense and senior management in execution of their responsibilities.

Technology and Workload Management

Workload management is an increasing concern for Third-Party/Vendor Risk Management Round Table member institutions. In response, some institutions have developed new practices to streamline due diligence and governance for "vendor" and "non-vendor" third-party relationships.

For example, in response to the question, "Have you granted any blanket exceptions to specific categories of relationships/activities whereby they are exempt from due diligence

that would otherwise be mandatory? (e.g., shrink-wrap software, appraisers, law firms, government or quasi-government agencies)" (question 33), almost half of survey participants responded positively and shared some of their innovative practices.

Response	Percent
No, and no plans to do so	26.3%
Not yet	27.5%
Yes – Explain and give specific examples.	46.3%

Examples	
Law firms and corporate legal advice	Parking, food services, travel, florists, office supplies, equipment
Appraisers, title companies, repo's	
PR firms	Leases, building expenses
Facilities Maintenance	Utilities
[Quasi] government entities	Telecom
Corporate sponsorships, donations	Shrink wrap software
FMU's, rating agencies	M&A

Technology adoption is much higher than reported in responses to the 2014 RMA survey. As of the 2015 survey, only 28.8% of participating institutions are still using MS Access, Excel, or SharePoint to manage their third-party risk management programs, with higher numbers in smaller institutions. In smaller institutions, the majority use the same technology solution for third-party risk management and contract repository. This is a far less common practice in larger institutions.

Most institutions acquire data from third parties like Dunn and Bradstreet, LexisNexis and Moody's to support due diligence and monitoring activities. Automated data feeds, automated alerts, and independent due diligence are emerging practices, albeit slowly. The most common types of due diligence that are outsourced to a third party are (1) assessment of the third party's financial condition and (2) monitoring for adverse news.

Approximately 60% of participating institutions use standard contracts and risk control clauses for third-party relationships. This practice can provide assurance on compliance matters in addition to helping manage heavy workloads.

Recent Regulatory Criticism

17 participating institutions suggested they have achieved "clean" regulatory examinations.

The following information about regulatory criticism can be used as a guide for program evolution across the sector. Please refer to question 53 for additional information.

	<$10 bil	$10-50 bil	$50-100 bil	>$100 bil
Response	Percent	Percent	Percent	Percent
Completeness- full lifecycle of "vendors"	8.9%	25%	0%	26.3%
Completeness- includes all "non-vendor" relationships	4.4%	25%	12.5%	21.1%
Consistency- across all lines of business	8.9%	12.5%	12.5%	47.4%
Due diligence- quality and completeness, documentation	17.8%	37.5%	12.5%	21.1%
BCM (new Appendix J)	15.6%	37.5%	0%	10.5%
Governance and oversight	4.4%	12.5%	0%	36.8%
Effective challenge	0%	0%	0%	15.8%
Monitoring	20%	25%	0%	21.1%
Reporting	2.2%	0%	12.5%	15.8%
Other, please explain	46.7%	25%	62.5%	42.1%

Insight and Advice

Survey participants were very generous in sharing information, advice, and lessons learned. Thank you!

There are insightful comments throughout the survey. Where RMA asked for specific advice and information, we've provided the following list of question numbers for easy access to their golden nuggets:

Q15) Non-vendor program execution, excluding the 1st Line of Defense.
Q17) Definition of "critical non-vendors."
Q24) Greatest challenges in developing an effective "non-vendor" third-party risk management program.
Q25) Advice related to "non-vendor" third-party risk management.
Q28) Vendor program execution, excluding the 1st Line of Defense.
Q33) Blanket exceptions to due diligence, by category.
Q25) Site visits including frequency.
Q37) Definition of "critical vendors."
Q40) Definition of critical vendor "activities."

Conclusion

Institutions continue to invest in third-party risk management and practices continue to evolve and grow. In 2014 vendor third-party risk management practices were the focus of the survey, reflecting the focus of institutions and practitioners at that time. In the 2015 survey, it is clear that vendor-centric practices are rapidly maturing. Based on responses to the 2015 survey, people, processes, and technology are making measurable improvements and best practices have evolved significantly. Non-vendor third party risk management is a strong theme, but those practices are still immature.

There is a tremendous willingness to share knowledge and expertise across the sector, and a new professional discipline in third party risk management is emerging.

Thanks again to all Third-Party Risk Management Round Table members and member institutions that contributed to and completed the 2015 RMA Third-Party/Vendor Risk Management survey. We really appreciate and look forward to your continued support.

Please see the pages following for detailed responses and examples of range of practices institutions employ in managing third-party/vendor risk management.