2019 RMA THIRD-PARTY NON-VENDOR RISK MANAGEMENT SURVEY

EXECUTIVE SUMMARY

DATA COLLECTED: FEBRUARY-APRIL 2019
REPORT DATE: JUNE 2019

JOIN. ENGAGE. LEAD.

Operational Risk

ACKNOWLEDGMENTS

The survey was conducted by The Risk Management Association between February and April 2019. Most of the questions were multiple choice with many opportunities to provide comments. Some questions were open text and designed to provide information and insight about the current status and emerging practices for "non-vendor" third-party relationships, across a range of RMA member institutions.

A total of 74 responses was received, covering a wide range 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 future articles in *The RMA Journal*.

The first iteration of this survey was designed in 2015 by the RMA Third-Party/Vendor Risk Management Steering Committee. Updates to the 2019 survey were possible with the help of: Ron Ausemus (Texas Capital Bank), Matthew Buskard (Fifth Third Bank), Carol Haeberle (Prudential), Debbie Manos-McHenry (Huntington Bank), and Linda Tuck Chapman (ONTALA Performance Solutions Ltd). The definitions for "vendor" and "non-vendor," as well as a sample of 20 categories of non-vendors, have been developed by the Third-Party Risk Management Round Table Steering Committee with the help of the working group participants.

The 2014, 2015, 2017, and 2019 RMA Third-Party/Vendor Risk Management surveys were conducted at the request of RMA Third-Party/Vendor Risk Management Round Table members. The 2015 survey was designed as an update and expansion to similar content in the 2014 RMA survey. Practices are rapidly evolving due to increased regulation of the 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. The 2014 and 2017 surveys focused on the third-party programs, while the 2015 and 2019 surveys focused more on "non-vendor" practices.

Please note the use of the terms "vendor" and 'non-vendor" third party throughout this survey. This is an important distinction in identifying 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 following more commonly used definitions were developed by members of the RMA Vendor/Third-Party Risk Management Round Table.

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. Non-Vendor Third-Party Risk Management Program.
2. Governance, Procurement, Contracting, and Reporting.
3. Tools and Technology.
4. Insight and Advice.

The final report 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.

RMA would like to thank the institutions that contributed to this study. Credit for participation was given to all 74 institutions regardless if respondents skipped certain questions, yet we feel they provided valuable data to the majority of the questions.

We respectfully request that these materials not be shared with any consultants or service providers. The material contained in this document is exclusive to RMA and contributing members.

Institutions (74) that participated in the survey:

Anonymous (3)	AIG
Amarillo National Bank	American National Bank of Texas
Bank of America	Bank of America Merchant Services
Bank OZK	Bankers' Bank
BB&T	BBVA Compass Bank
BNY Mellon	BOK Financial
Bryn Mawr Trust Company	Capital One Bank
CenterState Bank	Citizens Bank
City National Bank	Commerce Bank
Credit Agricole Corporate and Investment Bank	Discover Financial Services
DTCC	E*TRADE Financial
Farmers & Merchants Bank of Long Beach	Federal Home Loan Bank Pittsburgh
Fifth Third Bank	First Citizens Bank
First National Bank of Omaha	First United Bank & Trust
First Volunteer Bank	Hancock Whitney Bank
The Huntington National Bank	Iberiabank
Industrial & Commercial Bank of China (USA) N.A.	Independent Bank
Investar	Investors Bank
Ion Bank	John Deere Financial
Key Bank	Limestone Bank
M&T Bank	Mountain America Credit Union
Midsouth Bank N.A.	Morgan Stanley
MUFG Securities	MUFG Union Bank
Mutual of Omaha	National Bank of Canada
Parkside Financial Bank & Trust	PNC Bank
Powell Valley National Bank	Prudential Financial
RBC Royal Bank	Republic Bank
Sandy Spring Bank	Shore United Bank
Signature Bank	Silvergate Bank
Simmons Bank	Societe Generale
State Farm Insurance Co.	State Street Bank
Stephenson National Bank & Trust	TD Ameritrade
Texas Capital Bank	U.S. Bank
Union Community Bank	USAA
Voya Financial	Wells Fargo Bank
Western State 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

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues. Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, more than 18,000 of these individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

Members actively participate in the RMA network of chapters. These chapters are run by RMA Associates on a volunteer basis and they provide our members with opportunities in their local communities for education, training, and networking throughout all stages of their financial services career. Chapters are located across the U.S. and Canada as well as in global financial centers.

RMA members also avail themselves of benefits offered through headquarters in Philadelphia, Pennsylvania. To assist members in advancing sound risk management principles, RMA keeps members informed and provides access to industry information at this site; publishes *The RMA Journal* and a variety of newsletters, books, and statistics; conducts workshops and seminars; holds conferences, including an annual convention (Annual Risk Management Conference); and has numerous committees working on a variety of projects.

Visit RMA at www.rmahq.org.
Note: As a not-for-profit, professional association, RMA does not lobby on behalf of the industry.

EXECUTIVE SUMMARY

The survey was conducted by The Risk Management Association between February and April 2019. 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 the current status and emerging practices for "non-vendor" third-party relationships, across a range of RMA member institutions.

A total of 74 responses was 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	24	32.4%
$10-50 billion	16	21.6%
$50-100 billion	11	14.9%
Greater than $100 billion	23	31.1%

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

1. Non-Vendor Third-Party Risk Management Program
2. Governance, Procurement, Contracting, and Reporting
3. Tools and Technology
4. Insight and Advice

Some questions were carried over from the 2015 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 more commonly used definitions were developed by members of the RMA Vendor/Third-Party Risk Management Round Table.

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

By looking at the data, there is evidence that the level of maturity has slightly improved. When it comes to maturity level for a "non-vendor" third-party risk management program, in the 2015 survey, close to 14% of respondents described their "vendor" third-party risk management program as fully mature, and 26% indicated that the non-vendor program will be fully mature in less than a year. In this year's survey, we see that 24% of participants consider their non-vendor third-party risk management program to be fully mature and 13% will become fully mature in less than a year. There is still a significant number of institutions where the non-vendor program is new/underway.

	2019 Survey		2015 Survey	
Response	Count	Percent	Count	Percent
Fully mature	16	24.2%	11	13.8%
Will be fully mature in less than a year	9	13.6%	21	26.3%
Doesn't address the full lifecycle yet	17	25.8%	16	20%
New or underway	24	36.4%	32	40%
Total Responses	*66 out of 74*		*80 out of 80*	

Expansion of "vendor" third-party risk management programs to include "non-vendor" relationships has occurred since the 2015 survey was conducted. In preparation for this year's survey, the RMA Third-Party/Vendor Risk Management Round Table Steering Committee members developed a profile of non-vendor third parties.

The list of "non-vendor" relationships common in banks and insurance companies of all sizes consists of 20 categories. These categories were used to enable common language and consistent responses about current practices. The detailed list of categories and subcategories was shared with those who participated in the survey:

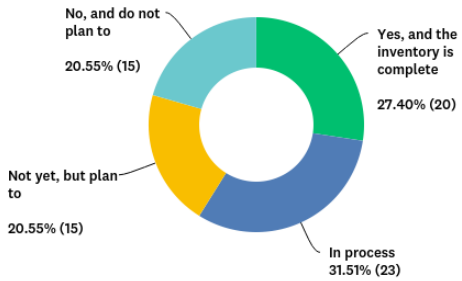
2019 Survey (20 categories)	2015 Survey (19 categories)
Affiliate	Affiliates
Affinity Relationships	Affinity Relationships
Agents	Agents
Alliances and Partnerships	Alliance and Partnerships
Brokers	Brokers
Correspondent Banks, Lenders, Brokers and Wholesale Banking	Correspondent Banks
Counterparties	Counterparties
Debt Underwriters/Securitization Firms/Trustees	Debt Underwriters/Securitization Firms/ Trustees
Facilities Providers	Financial Product Providers
Financial Utilities (e.g. SWIFT, DTCC, ACH)	Financial Utilities
Government-Sponsored Entities/ Government Special Purpose Entities	Government Special Purpose Entity (GSE)
Indirect Lending Third Parties	Indirect Lending
Insurance Third Parties	
Joint Marketing Providers	Joint Marketing Partners/Co-Branding Partners
Law Firms	
Rating Agencies	Rating Agencies
Real Estate Lessors/Lessees	
Servicers	Servicers
Specialized Analysts and Advisors to Executive Management	Specialized Analysts and Advisors to Executive Management
	Tenants
Trade Associations	Trade Associations
	Wholesale Banking

In the 2015 survey, 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)," there was an even split (50%) between yes and no.

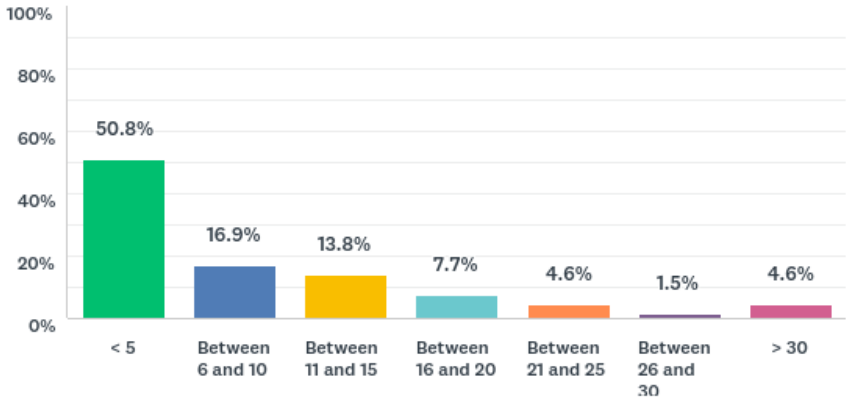
In the 2019 survey, we asked if participating institutions have a regulatory requirement to implement a "non-vendor" third-party risk policy, framework, and/or standards. 54% of respondents said "yes," 23% said "no," and 23% were "unsure."

42% of respondents confirmed that their institution developed a "non-vendor" third-party risk management policy, program framework, and/or standards (45% in 2015). About 24% are in the process of developing those (21% in 2015). Out of those who selected "yes" and "in process" for that question, 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 66.7%) For comparison, the percentage of institutions that planned on having their vendor and non-vendor third-party relationships covered by the same policy and standards was 68.2%.

In anticipation for more detailed questions of non-vendor relationships, we asked if institutions conducted an inventory of all "non-vendor" relationships. We had revised the answers for this question in 2019 from the 2015 survey, and for the purposes of the executive summary will focus only on participants who responded "yes," and "in-process." In the most recent survey those numbers looked as follow: 27%, and 31%. In contrast the approximately 42% of respondents answered "yes" and 29% answered "in process" in the 2015 survey.

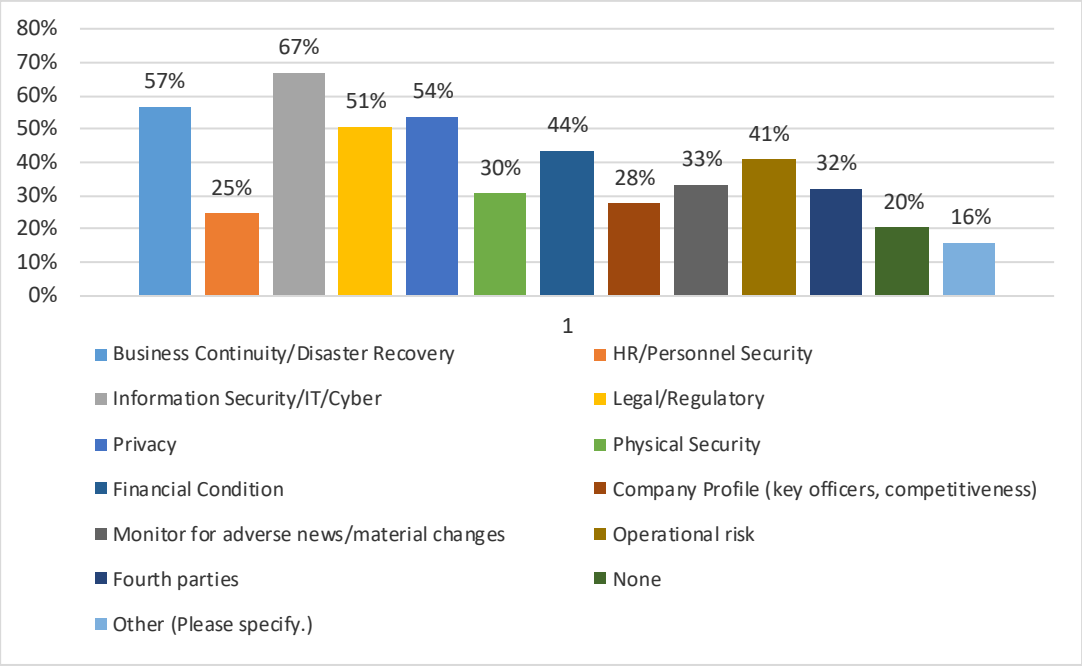


We have learned that in most cases (51%) institutions have less than five non-vendor third-party categories in their risk management program, 17% have between 6 and 10 categories in place, and 14% have between 11 and 15 categories. Approximately 31% of institutions do not segment non-vendors. Those who follow that practice indicated that non-vendor third parties are segmented/tiered based on risk assessment (50%), and criticality/materiality reliance (29%).



The following due diligence assessments or risk areas are evaluated regarding third-party non-vendors (listed in the order of highest to lowest response rate):

- Information Security/IT/Cyber
- Business Continuity/Disaster Recovery
- Privacy
- Legal/Regulatory
- Financial Condition
- Operational Risk
- Monitor for Adverse News/Material Changes
- Fourth Parties
- Physical Security



For 35% of institutions, business units are required to have documented contingency plans and exit strategies in place for their critical "non-vendor" third parties. That number is down from 44% in 2015.

The table below shows information about how many "non-vendor" third-party relationships are currently in respondents' third-party risk management programs.

	2019 Survey		2015 Survey	
Response	Count	Percent	Count	Percent
<250	42	65.6%	56	70%
251-500	5	7.8%	8	15%
501-1,000	3	4.7%	4	5%
1,001-1,500	0	0%	4	5%
1,501-2,000	4	6.3%	1	1.3%
2,001-2,500	1	1.6%	1	1.3%
>2,500	9	14.1%	6	7.5%
Total Responses	*64*		*80*	

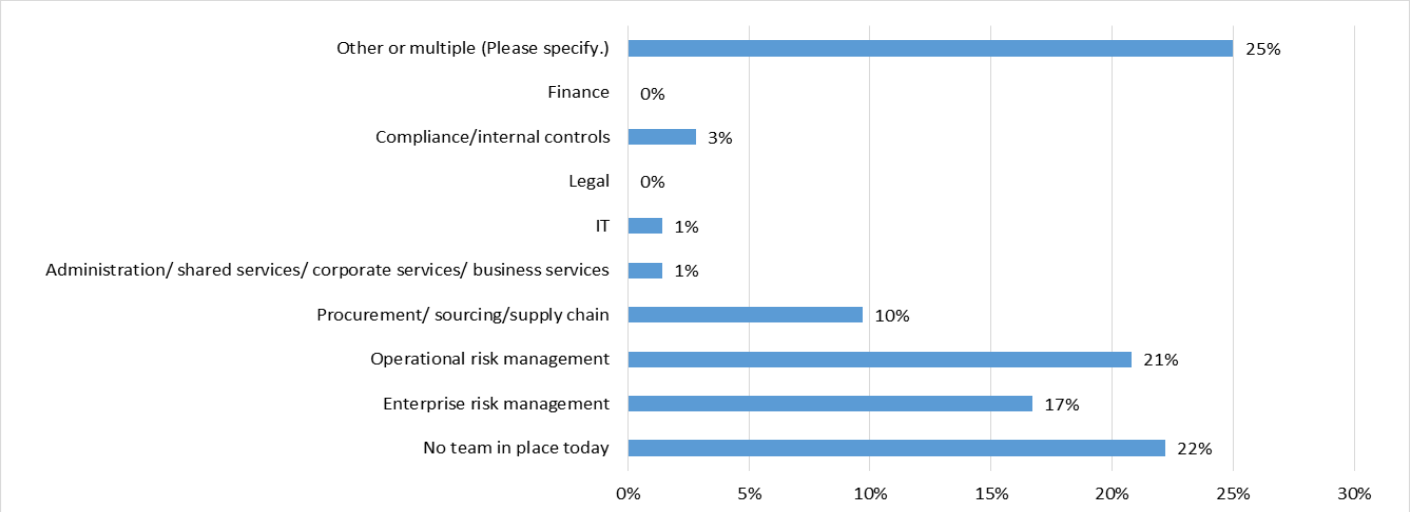
Participants were asked to identify from the list of 20 non-vendor categories, how each of those is formally addressed in their institution (as vendor, non-vendor, or N/A). After establishing their non-vendors, the participants were asked to respond to four questions about Governance (Q.21), Procurement (Q.22), Contracting (Q.23), and Reporting (Q.24). There is a range of practices when it comes to treating various categories. Some of those are treated by majority as vendors (financial utilities, facilities providers, servicers, law firms, specialized analysts, and advisors to executive management). Those with the highest count for treatment as non-vendors were: correspondent banks, lenders, brokers and wholesale banking; brokers; counterparties; and agents. Leading in the N/A category were: affinity relationships; trade associations; indirect lending third parties; and real estate lessors/lessees.

Key Stakeholder Roles and Responsibilities

In institutions of all asset sizes the number of FTEs dedicated to "non-vendor" third-party risk management in the oversight department has grown since the 2015 RMA survey.

	How Many FTEs are dedicated to "non-vendor" third-party risk management?	
	2019 Survey	2015 Survey
<3	75.4%	77.5%
3-5	4.6%	8.8%
6-10	6.2%	7.5%
11-15	4.6%	1.3%
16-25	0%	2.5%
>25	9.2%	2.5%

22% of respondents said that they currently do not have a team in place, which would be responsible for design, oversight, framework, policy/standards, and processes for "non-vendor" third-party risk management. Those who have a team in place identified it as part of the following functional areas:



Technology and Workload Management

Workload management is an increasing concern for member institutions at the Third-Party/Vendor Risk Management Round Table. 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 29), 40% of survey participants responded positively and shared some of their innovative practices.

Response	2019 Survey	2015 Survey
No, and no plans to do so	22.7%	26.3%
Not yet	36.4%	27.5%
Yes – Explain and give specific examples.	40.9%	46.3%

Technology adoption is much higher in the 2019 survey than reported in responses to the 2015 RMA survey. Results from the 2015 survey showed that 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. In the current survey, use

of MS Office programs declined to 11% from 2015. Depending on the asset size, institutions rely on various vendors.

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:

Q11) Definition of "critical non-vendor activities."
Q20) Additional categories/subcategories classified by institutions as "non-vendors" that were not included on the initial RMA list of 20 categories.
Q22) Details regarding procurement practices for "non-vendors."
Q23) Details regarding contracting practices for "non-vendors."
Q24) Details regarding reporting practices for "non-vendors."
Q27) Storing vendor and non-vendor contracts.
Q29) Blanket exceptions to due diligence, by category.
Q29) Greatest challenges in developing an effective "non-vendor" third-party risk management program.
Q31) Advice related to "non-vendor" third-party risk management.

Conclusion

Institutions continue to invest in third-party risk management and practices continue to evolve and grow. Based on responses to the 2019 survey, non-vendor third-party risk management is a strong theme, but there is still a range of practices depending on the maturity level of the institution. Technology is making measurable improvements and best practices are starting to evolve slowly.

Thanks again to all Third-Party Risk Management Round Table members as well as other RMA institutions that contributed to and completed the 2019 RMA Third-Party Non-Vendor Risk Management survey. We really appreciate it and look forward to your continued support.

Thank you to the RMA member banks for contributing to this benchmarking study. The full report is available to those institutions that contributed to the study.