2017 RMA MID-TIER BANKS: ASSET SIZE: $10 – 50 BILLION THIRD-PARTY RISK MANAGEMENT SURVEY- EXECUTIVE SUMMARY

FINAL REPORT
OCTOBER 2017

JOIN. ENGAGE. LEAD.

Operational Risk

ACKNOWLEDGMENTS

The 2017 survey was designed with the help of RMA's Vendor Risk Management Steering Committee, comprised of Debbie Manos-McHenry (Huntington Bank), John Klapmust (Bank of the West), Linda Quong (Charles Schwab), and Linda Tuck Chapman (ONTALA Performance Solutions Ltd).

The purpose of the survey was to capture the range of practices in third-party 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 risk management.

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.

The RMA staff member contributing to the study was Sylwia M. Czajkowska.

Institutions that participated in the survey:

Banc of California, NA
Bremer Bank
DTCC
EverBank
First National Bank of Omaha
Frost Bank
Investors Bank
NYCB
People's United Bank
Signature Bank
Sterling National Bank
Synovus Bank
Texas Capital Bank
UMB Financial Corporation
Webster Bank
Whitney Bank

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 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.

RMA welcomes all personnel involved in lending and risk management in member organizations to become RMA Associates. 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 (RMA) between June and August 2017. Most of the questions were multiple choice with opportunities to provide comments. Some questions were open text, designed to provide information and insight about best and current practices.

A total of 16 responses from mid-tier size banks were received, covering a range of asset sizes between $10-50 billion. This year, RMA decided to conduct separate surveys for mid-tier banks, large and regional banks, and community banks.

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, and FDIC.

The following areas were addressed in the survey:

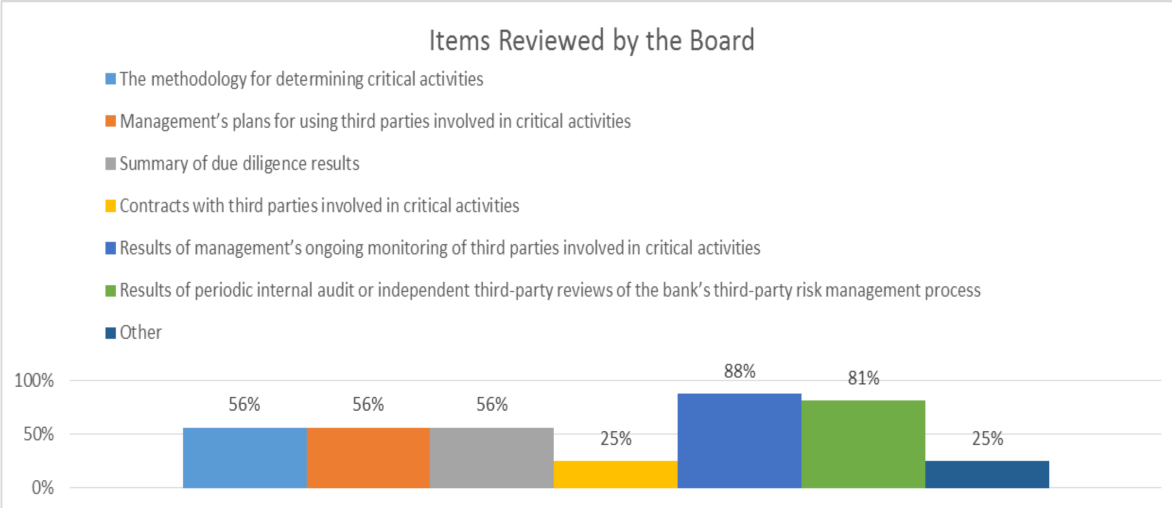
1. Third-Party Risk Management Framework.
2. Third-Party Selection and Monitoring Process.
3. Critical Third-Parties and Critical Activities.
4. Tools and Technology.
5. Contracts.
6. Regulatory and Compliance.
7. Fourth Parties.

Some questions were repeated from the 2014 and 2015 baseline surveys. This will help financial services companies track their progress and evolution of practices.

Third-Party Risk Management Framework

When asked about the Board of Directors' involvement with third-party risk management, a majority of institutions (>60%) confirmed that their Board ensures that strategies related to the bank's core competencies appropriately address which services to retain and which services to outsource to third parties. Key items reviewed by the Board include:

- The methodology for determining critical activities.
- Management's plans for using third parties involved in critical activities.
- Summary of due diligence reports.
- Results of management's ongoing monitoring of third parties involved in critical activities.
- Results of periodic internal audit or independent third-party reviews of the bank's third-party risk management process.

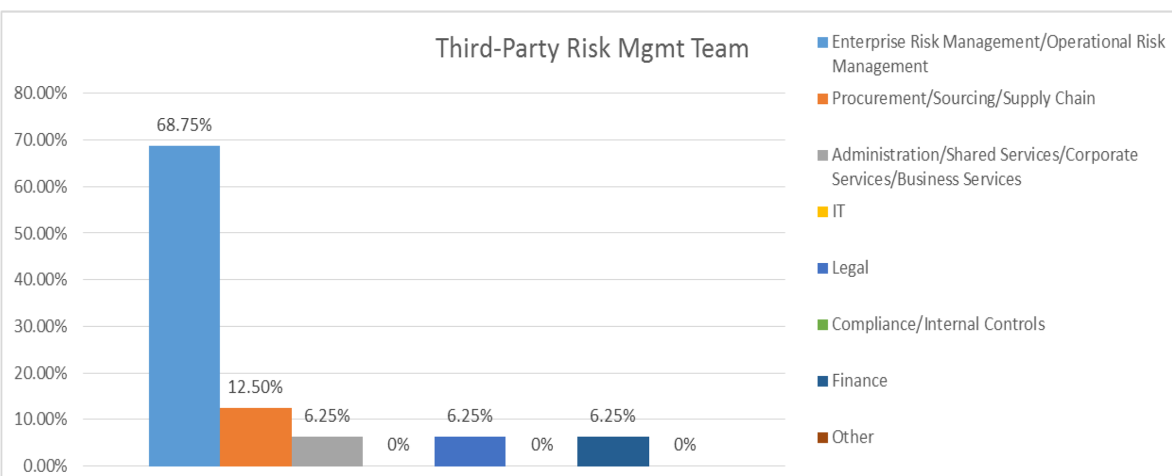


For 62% of respondents, the institution's overall strategy for third-party risk is well understood and fully aligned with the institution's overall risk appetite.

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. In this years' data, we see that over 60% of participants consider their third-party risk management program to be fully mature (32%) or will become fully mature in less than a year (32%).

Since 2014, there has been a shift in how the vendors are managed. About 75% of vendors are managed in the business, compared to 59% in the 2014 survey for the same asset size category.

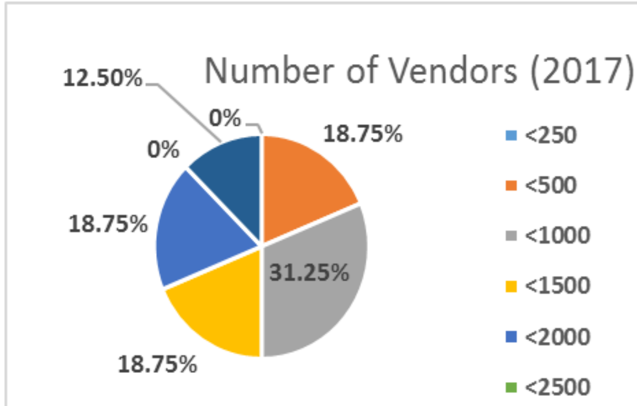
Similarly, as in the 2015 report, the team responsible for design, framework, policy/standards, and processes for third-party is primarily located in the Enterprise Risk Management/Operational Risk Management function.



The oversight function resides in the 2nd line of defense and is part of the same risk oversight area.

The composition of the number of vendors within the scope of the program has shifted since our last survey. About 50% of respondents predict that the current number of third parties will increase in the next two to three years.

# of Vendors	2017	2015	2014
<250	0%	25%	22.70%
<500	18.75%	0%	4.50%
<1000	31.25%	37.50%	18.20%
<1500	18.75%	25%	4.50%
<2000	18.75%	0%	13.60%
<2500	0%	0%	13.60%
>2500	12.50%	12.50%	22.70%



For institutions with asset size between $10-50 billion, the number of FTEs supporting related activities has changed from the 2015 survey.

Total # of FTEs	FTEs dedicated to:		
	"vendor" third-parties (2017)	"vendor" third-parties (2015)	"non-vendor" third-parties (2015)
<3	25%	25%	75%
3-5	50%	37.5%	25%
6-10	18.75%	25%	0%
11-15	6.25%	12.5%	0%
16-25	0%	0%	0%
>25	0%	0%	0%

Third-Party Selection and Monitoring

The main factor driving the process to identify the third parties that will be actively managed within an institution's third-party risk management program is determined by a risk profile calculator/algorithm built into the third-party risk assessment questionnaire (50% of responses). This is consistent with the 2015 report.

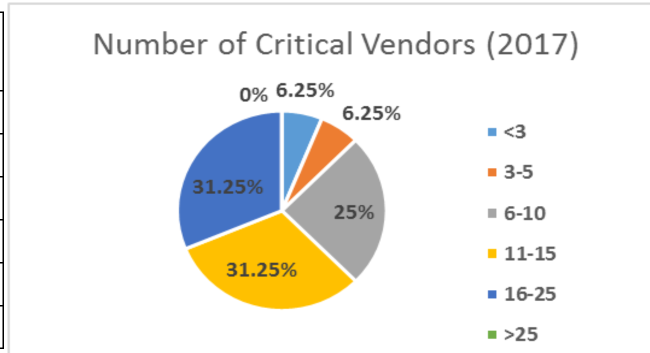
All of the participants indicated they send due diligence questionnaires for risk assessment purposes, in addition to the RFP questions. The preferred alternatives to these questionnaires include: SOC (Types 1, 2, and 3), SSAE16 (Types 1 and 2) reports, and ISO27001 certification.

Taking into consideration the amount of work required to review a vendor, 87% of respondents would be willing to consider using a shared assessment provided by a third party.

Critical Third Parties and Critical Activities

Over the years, the number of "enterprise critical" third parties has shifted. The figures show that the majority of institutions have between 11 and 25 "enterprise critical" vendors – vendors that have the potential to bring the bank to its knees - in their programs.

# of Critical Vendors	2017	2015	2014
<3	6.25%	0%	4.50%
3-5	6.25%	0%	9.10%
6-10	25%	12.50%	9.10%
11-15	31.25%	37.50%	13.60%
16-25	31.25%	50%	13.60%
>25	0%	0%	50%



About 87% of respondents conduct site visits for their most and/or high risk critical third parties, while 43% of those who conduct site visits do so on an annual basis. Out of the 87% who conduct site visits, about 57% do not have resources dedicated to this task.

There is evidence that institutions are gaining clarity around third-party management requirements. For example, definitions of "critical activities" provided in the 2014 report were somewhat vague. The definitions are much more precise in this year's report. Furthermore, in this year's report the definition of "critical activity" is fully defined for 60% of the institutions who contributed to the study. The remaining 40% are in the process of defining it.

The data also shows an upward trend related to requiring an exit strategy for critical supplier, likely in response to FFIEC's Appendix J on business continuity management. For years 2014, 2015, and 2017, the percentage of institutions requiring exit strategies was 73%, 87%, and 87%, respectively.

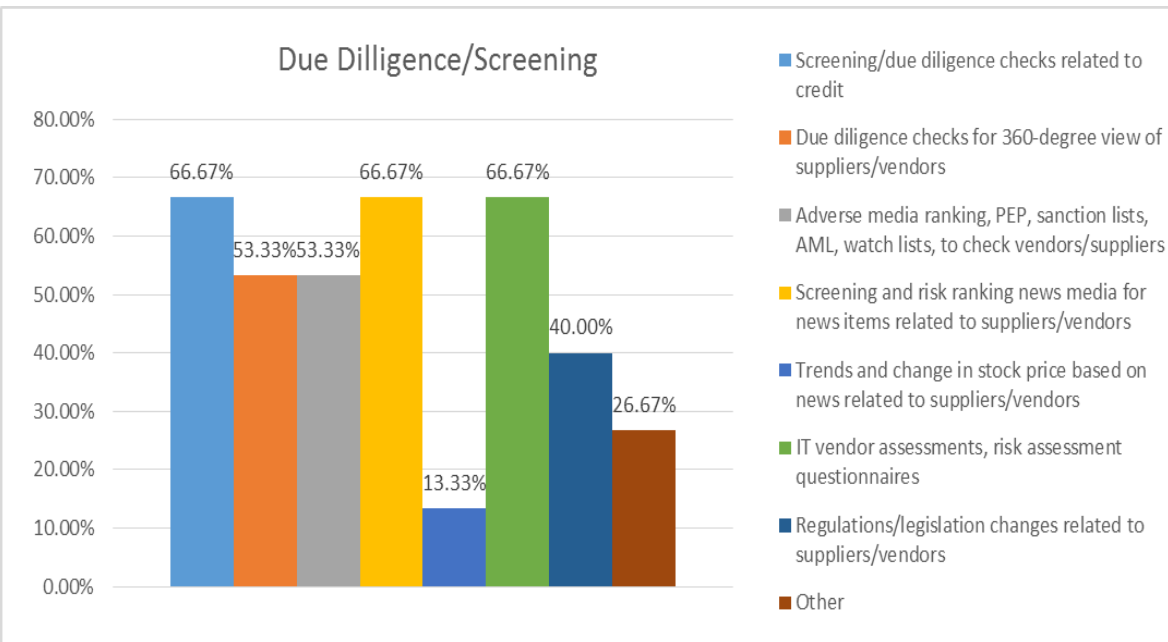
Workload management is an increasing concern for third-party risk management professionals. For example, in response to the question, "Have you granted any blanket exceptions to specific categories of relationships/activities whereby they are exempt from due diligence that would otherwise be mandatory? (e.g., shrink-wrap software, appraisers, law firms, and government or quasi-government agencies)" (question 36), over 50% of survey participants responded positively and shared some of their practices.

Tools and Technology

Technology adoption varies across institutions. There is no dominant third-party solution provider. Some of the commonly used programs include: Archer, Hiperos, and MetricStream. We have noticed a spike in supplementing use of commercial providers with using MS Office programs. In the 2015 survey, only 25% of participating institutions were using MS Access, Excel, or SharePoint to manage their third-party risk management programs, with higher numbers in smaller institutions. In 2017, that number increased to 37%. When asked if institutions use the same primary technology to manage activities, documentation, and reporting for non-vendor third-party risk management programs, 56% of respondents selected "Yes."

Most institutions acquire data from third parties like Dunn and Bradstreet, LexisNexis and Moody's to support due diligence and monitoring activities. The use of automated data feeds, automated alerts, and independent due diligence is an emerging practice, and most of the data comes from common sources.

The most common types of due diligence that institutions use and/or are interested in obtaining are (1) screening/due diligence checks related to credit, (2) screening and risk rating for relevant news media for news items related to vendors/suppliers, and (3) IT vendor assessments/risk assessment questionnaires.



About 56% of respondents require cyber liability insurance from third parties that have access to personal and private information.

Contracts

About 50% of institutions use standard contract and risk control clauses for third-party relationships. This number is down from 2015 where 62% of respondents indicated they've implemented these standards. .

Internal audit continues to play a key role in terms of conducting independent reviews of a third-party risk management program.

When it comes to the "Supplier Code of Conduct," 56% of respondents do not have one in place. This is down from the 72% threshold noted in the 2014 data.

Once the contract is executed, 81% of institutions reassess risks for higher risk third parties on an annual basis. This number increased from 59% in 2014, likely in response to regulatory requirements for "continuous monitoring" throughout the lifecycle of relationships.

When asked about managing and reporting on third-party risk incidents and issues, consistently across the years, the top three responses were:

1. Escalates risk incidents and issues to the business line, the company's risk subject matter experts, and upper management.
2. Reports risk incidents and issues to the company's operational and management committees.
3. Regularly reports status of risk incidents and issues to the business.

We asked our members about outsourcing. Currently, 87% of institutions do not outsource any part of sourcing, procurement, or supplier risk management. About 64% answered that none of their due diligence assessments have been outsourced to third-party providers.

Regulatory and Compliance

In most cases, enterprise/operational risk management is responsible for identifying, tracking, and communicating regulatory and compliance updates/changes related to third-party risk management.

Approximately 75% of institutions have a risk oversight committee, formed specifically to oversee third-party risks. This is an increase from 62% noted in 2015.

The following information about regulatory criticism can be used as a guide for program evolution across the sector. Please refer to question 58 for additional information.

Response	Percent
Completeness: program doesn't address full lifecycle of "vendor" third-party relationships	8.33%
Completeness: program doesn't include all critical "vendor" third-party	8.33%

Response	Percent
relationships and activities	
Due diligence: quality and completeness, documentation	16.67%
Business continuity/resilience (new Appendix J to FFIEC guidance)	8.33%
Governance and oversight	8.33%
Data quality	8.33%
Quality Assurance	8.33%
Effective Challenge	8.33%
Monitoring	16.67%
Reporting	33.33%
Independent reviews	8.33%
Sales Practices (e.g., horizontal Fed/OCC sales practices review post Sept. 2016 incident)	8.33%
Other (please specify)	33.33%

Fourth Parties

The final section of the survey was dedicated to fourth parties. There is a range of practices when it comes to how **material** fourth parties are identified.

- 25% require their third party to identify fourth parties during RFP process.
- 37% indicated that material fourth parties are identified in the contract.
- 25% require their third party to update the list of material fourth parties annually.

In 2014, 59% of those surveyed confirmed that they perform due diligence on fourth parties. That number declined to 13% in 2017. The change may be impacted by the additional option to allow respondents to answer the question "partially" which accounts for 47% of this year's responses.

Insights

Please see the pages following for detailed responses and examples of the range of practices institutions with asset sizes of $10- 50 billion employ for third-party/vendor risk management.

Thank you to RMA member banks for contributing to this benchmarking study. The full report is available to participating institutions.