Risk Management Association

Advance Your World.

2023 RMA THIRD-PARTY NON-VENDOR RISK MANAGEMENT SURVEY

FINAL REPORT

DATA COLLECTED: *OCTOBER-NOVEMBER 2023*
REPORT DATE: MARCH 2024

ACKNOWLEDGMENTS

The survey was conducted by The Risk Management Association between October and November 2023. 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 status and emerging practices for "non-vendor" third-party relationships, across a range of RMA member institutions.

A total of 46 responses was received, covering a wide range of financial institutions from four asset sizes: less than $10 billion, between $10 billion and $50 billion, $50 billion to $250 billion, and over $250 billion, including community, regional, super-regional, and money center banks, and investment banks headquartered in the United States, Canada, and Europe.

The first iteration of this survey was designed in 2015 by the RMA Third-Party/Vendor Risk Management Steering Committee. The survey was updated in 2019. Updates to the 2023 survey were possible with the help of: Matthew Buskard (Fifth Third Bank), Heather Hendershott (Ally Bank), and Linda Tuck Chapman (Third Party Risk Institute).

The following commonly used definitions for "vendor" and "non-vendor," as well as a sample of categories of non-vendors were developed by members of the RMA Vendor/Third-Party Risk Management Roundtable Steering Committee with the help of the working group participants.

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 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 (sczajkowska@rmahq.org). The final report was written by RMA.

About Risk Management Association (RMA)

For more than 100 years, RMA has been laser focused on one thing: helping its members in the world's financial institutions better understand and address risk.

As a trusted partner, RMA has weathered the many economic ups and downs of the last century alongside its members, which now number 1,600+ financial institutions of all sizes, from multi-nationals to local community banks. These institutions are represented by over 51,000 individual RMA members located throughout North America, Europe, Australia, and Asia.

Our members rely on us to keep them abreast of important industry trends and prepare them to face new challenges head-on. Our sound risk management principles are developed for members, by members, and help to build safer, stronger financial institutions, impacting local communities and the global economy.

All of this makes RMA unique - we are the only comprehensive source of risk management tools and education that has spanned the last 100 years. And we look forward to the next 100 as we help the industry come together on the transformative issues of climate, cyber, culture, technology, and more.

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

RMA would like to thank the institutions that contributed to this study. Credit for participation was given to all 46 institutions regardless of whether respondents skipped certain questions. In every case, they provided valuable data to the majority of the questions.

Institutions (46) that participated in the survey:

Anonymous (6)	Ally Bank
Avidia Bank	Bank OZK
BNP Paribas	Capital One
CIBC	Citi
Citizens Business Bank	Credit Agricole CIB
CrossFirst Bank	Deere Credit Services/John Deere Financial
Discover Financial Services	Enterprise Bank & Trust
Fifth Third Bank	First Citizens Bank
First National Bank of Omaha	Flagstar
HSBC	HTLF
KeyBank	Lakeland Bank
Mechanics Bank	Mizuho
MUFG	Nano Banc
National Bank of Canada	New Hampshire Mutual Bancorp
Old National Bank	Pinnacle Financial Partners
PNC Bank	Raymond James
State Street	Sterling Bank & Trust F.S.B.
TD Bank	Trustmark Bank
U.S. Bank	UMBFS
Veritex Community Bank	Webster Bank
Zions Bancorporation	

Disclaimer

EXECUTIVE SUMMARY

As noted, 46 financial institutions contributed to this survey. The breakdown of participation is below.

Asset Size	Number of Institutions	Percent
Less than $10 billion	9	20.0%
$10-50 billion	14	31.1%
$50-100 billion	4	8.9%
$100-250 billion	10	22.2%
$250-500 billion	3	6.7%
Greater than $500 billion	5	11.1%

To ensure participants' anonymity, we grouped the analysis into the following tiers:
(Note: One respondent did not provide information about their asset size)

Asset Size	Number of Institutions	Percent
Less than $10 billion	8	17.4%
$10-50 billion	14	30.4%
$50-250 billion	14	30.4%
Greater than $250 billion	9	19.6%

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

1. Non-Vendor Third-Party Risk Management Program
2. Key Stakeholders: Roles and Responsibilities
3. Technology
4. Insight and Advice

Some questions were carried over from the 2015 and 2019 baseline survey. When available we added the historical data to this report. When looking at the historical data, please note that the asset size grouping for the past years was different from 2023. We hope that presenting the historical data will show trends and will help financial companies track their progress and the evolution of their practices.

Participants were asked to respond to questions about current practices for "vendor" and "non-vendor" third-party relationships. It was apparent in RMA roundtable discussions that this is an important distinction due to different practices for 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.
- Provide risk reporting.

The latest survey provided clarity on current differences in practices. The timing of the survey was associated with the release of "Third-Party Relationships: Interagency Guidance on Risk Management" (OCC Bulletin 2023-17).

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

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

In 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 program as fully mature, and 26% indicated that their non-vendor program will be fully mature in less than a year. In 2019, the number of institutions feeling mature increased to 24%. In the new survey, we see that close to 28% of participants consider their non-vendor third-party risk management program to be fully mature and 35% believe it 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. It is encouraging to see, though, that the number of institutions that don't address the full maturity lifecycle has declined over the years.

	2023 Survey		2019 Survey		2015 Survey	
Response	Count	Percent	Count	Percent	Count	Percent
Fully mature	12	27.9%	16	24.2%	11	13.8%
Will be fully mature in less than a year	15	34.9%	9	13.6%	21	26.3%
Doesn't address the full lifecycle yet	7	16.3%	17	25.8%	16	20%
New or underway	9	20.9%	24	36.4%	32	40%
Total Responses	*43 out of 46*		*66 out of 74*		*80 out of 80*	

There has been expansion of "vendor" third-party risk management programs to include "non-vendor" relationships since the 2015 survey. In preparation for the most recent survey, the RMA Third-Party/Vendor Risk Management Roundtable 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 has grown over the history of the survey. These categories are 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.

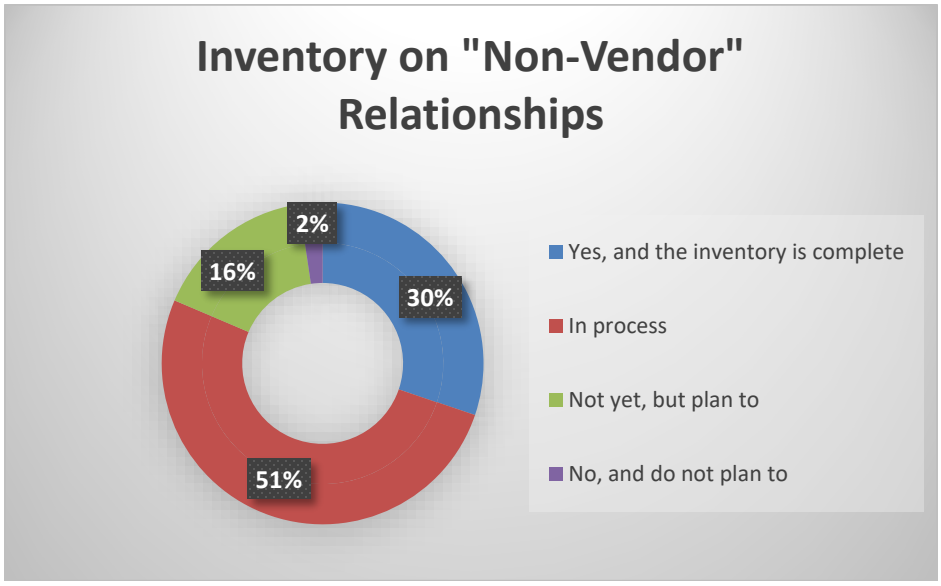
The number of non-vendor categories now stands at 25 with 107 subcategories. The full list of categories and subcategories is presented in question 18.

2023 Survey (25 categories)	2019 Survey (20 categories)	2015 Survey (19 categories)
	Affiliates	Affiliates
Affinity Relationships	Affinity Relationships	Affinity Relationships
Agents	Agents	Agents
Alliances and Partnerships	Alliances and Partnerships	Alliance and Partnerships
Brokers	Brokers	Brokers
	Correspondent Banks, Lenders, Brokers and Wholesale Banking	Correspondent Banks
Commercial Equipment		
Counterparties	Counterparties	Counterparties
	Debt Underwriters/Securitization Firms/Trustees	Debt Underwriters/Securitization Firms/ Trustees
Facilities Providers		
Financial Product Providers	Facilities Providers	Financial Product Providers
Financial Utilities (e.g. SWIFT, DTCC, ACH)	Financial Utilities (e.g. SWIFT, DTCC, ACH)	Financial Utilities
Government-Sponsored Entities / Government Special Purpose Entities	Government-Sponsored Entities/ Government Special Purpose Entities	Government Special Purpose Entity (GSE)
	Indirect Lending Third Parties	Indirect Lending
Insurance	Insurance Third Parties	
Intercompany Relationships		
	Joint Marketing Providers	Joint Marketing Partners/Co-Branding Partners
Law Firms	Law Firms	
Lending		
Marketing		
Memberships		

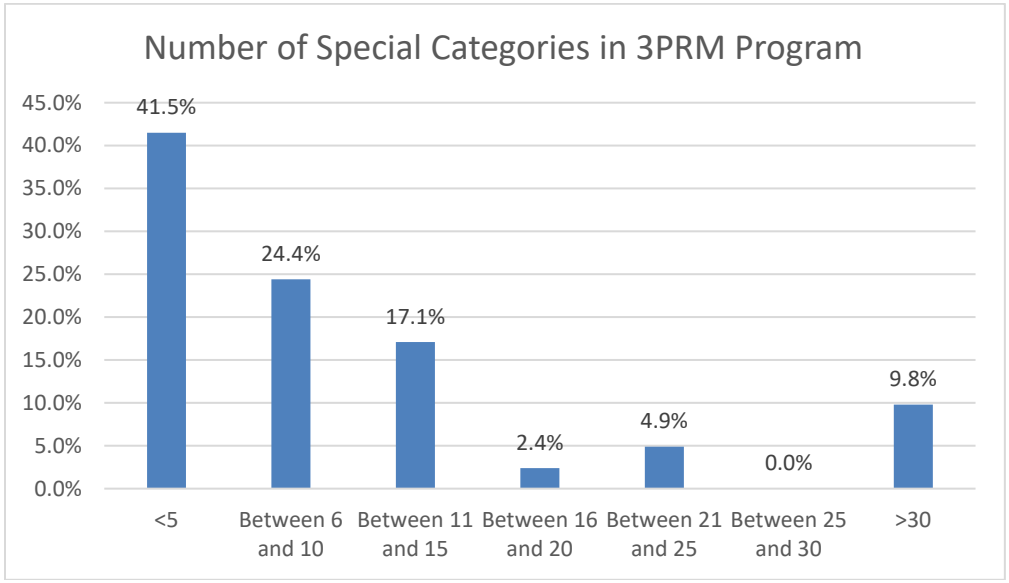
Payments		
Rating Agencies	Rating Agencies	Rating Agencies
Real Estate Lessors / Lessees	Real Estate Lessors/Lessees	
Servicers	Servicers	Servicers
Specialized Analysts and Advisors to Executive Management	Specialized Analysts and Advisors to Executive Management	Specialized Analysts and Advisors to Executive Management
Subscriptions		
		Tenants
	Trade Associations	Trade Associations
Trust Services		
Underwriters/ Securitization/ Trustees and Custody		
		Wholesale Banking
Other		

As in earlier surveys, the most recent one asked if institutions developed a "special category" third party risk management policy, program framework, and/or standards. We can note that 60% of institutions answered yes, and close to 27% are in the process of developing one. Only 9% plan to continue without a distinction between non-vendor and vendor programs. This is marks significant progress from 2019, when 18% did not anticipate making that distinction.

The survey also asked if institutions conducted an inventory of all "non-vendor" relationships. We had revised the form of the question in 2019 from the 2015 survey, so for the purposes of this executive summary we will focus only on participants who responded "yes" and "in-process." In the most recent survey those answers were, respectively, 30% and 51% . By comparison, the numbers in 2019 were 27% and 31%. It is encouraging to see that over 80% of respondents are now focusing their efforts on an inventory. Meanwhile, there has been a significant decline in the percentage of institutions that do not plan to conduct an inventory. It was 2% in the recent survey, down from 20% in 2019.



The survey found that 41% of institutions have fewer than five non-vendor third-party categories in their risk management program, 24% have between 6 and 10 categories in place, and 17% have between 11 and 15 categories.

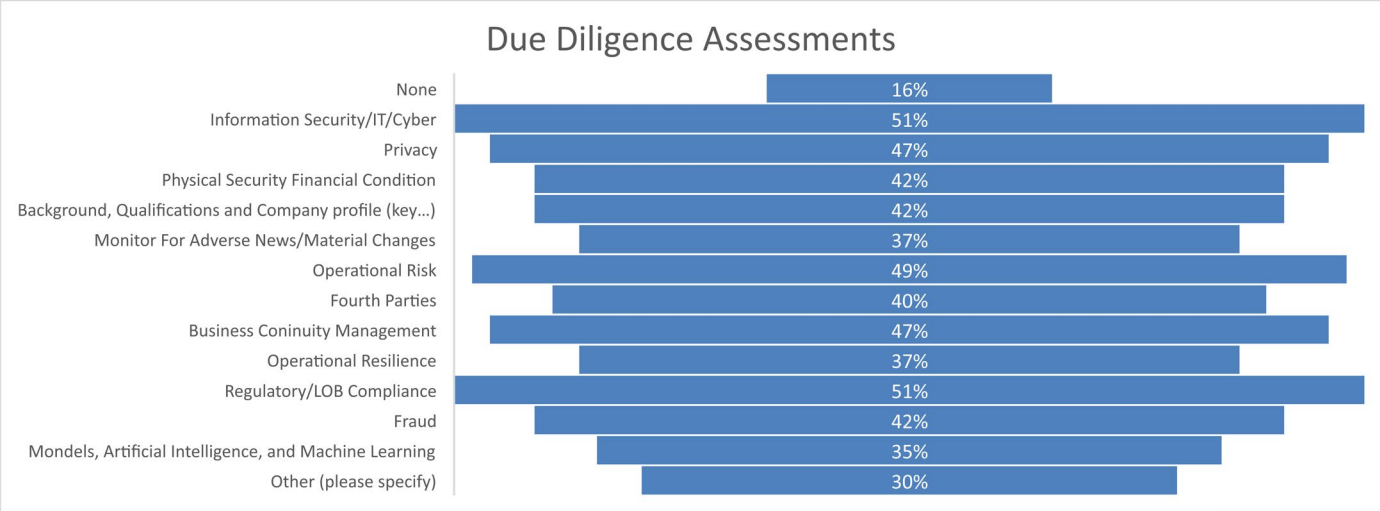


Approximately 7% of institutions do not segment non-vendors (down from 31% in 2019). Those who do say they segment/tier them based on: criticality/materiality (52%), line of business (43%), and risk assessments (7%). This is a change from 2019, when the majority said they segmented based on risk assessment (50%) or criticality/materiality reliance (39%).

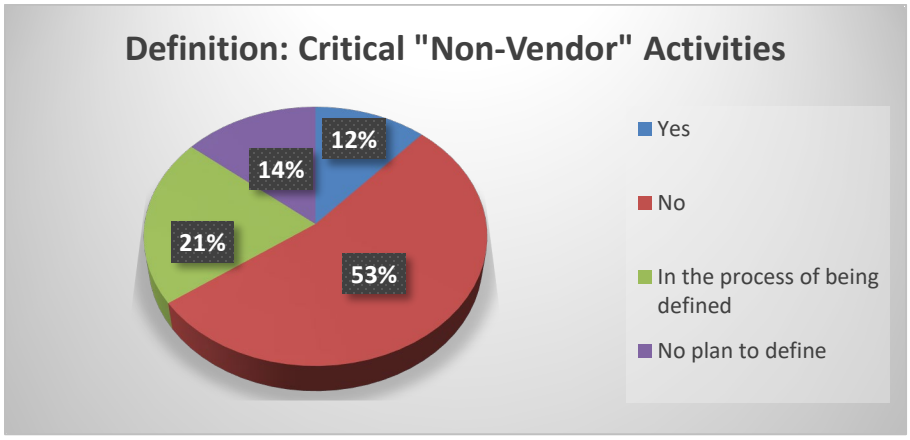
According to the data, the risk assessments of special category third parties are performed by third party product/service (49%) or by category (44%).

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):

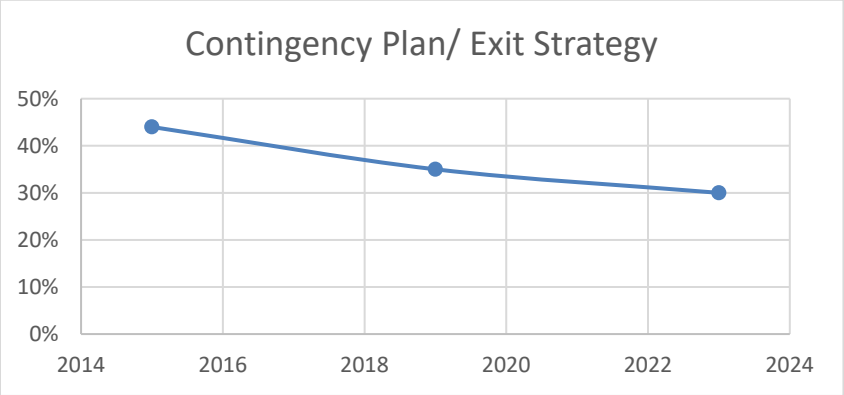
- Information Security/IT/Cyber
- Regulatory/ LOB Compliance
- Operational Risk
- Business Continuity/Disaster Recovery
- Privacy
- Fraud
- Physical Security
- Background Qualifications and Company Profile



When it comes to having a separate definition for critical non-vendor activities, close to 53% don't have one in place, 14% are not planning to have one, and 21% are currently in the process of developing one. Banks below $10 billion in assets are the most likely of all the respondents to be in the process of defining critical non-vendor activities. The detailed section of the report provides some examples of definitions.



In this survey, we continued to see a decline in institutions that require business units to have a documented contingency plan and exit strategies in place for critical special category third parties. Only 30% said it was a requirement, down from 44% in 2015.



The following table shows how many "non-vendor" third-party relationships are currently in respondents' third-party risk management programs. As in past years, more than half of institutions have fewer than 250 non-vendor third party relationships (52%). In looking at previous surveys, we can see that the number has declined from 70% in 2015. The category with 501-1000 non vendors rose to 14% from the 5% at the survey starting point in 2015.

	2023 Survey		2019 Survey		2015 Survey	
Response	Count	Percent	Count	Percent	Count	Percent
<250	22	52.4%	42	65.6%	56	70%
251-500	3	7.1%	5	7.8%	8	15%
501-1,000	6	14.3%	3	4.7%	4	5%
1,001-1,500	1	2.4%	0	0%	4	5%
1,501-2,000	2	4.8%	4	6.3%	1	1.3%
2,001-2,500	1	2.4%	1	1.6%	1	1.3%
>2,500	7	16.7%	9	14.1%	6	7.5%
Total Responses	*42*		*64*		*80*	

Key Stakeholder Roles and Responsibilities

The survey found that teams responsible for design, oversight, and the framework, policy/standards and processes are largely split between Third-Party Risk Management/2nd Line of Defense (40%), Enterprise Risk Management/2nd Line of Defense (19%), and Third-Party Risk Management/1st Line of Defense (19%).

In institutions of all asset sizes the number of FTEs dedicated to "non-vendor" third-party risk management in the oversight department has grown slightly in comparison to past years. Regardless

of asset size, the majority of respondents said they had fewer than three (<3) FTEs dedicated to special category third party risk management.

	2023 Survey		2019 Survey		2015 Survey	
Response	Count	Percent	Count	Percent	Count	Percent
<3	34	79.1%	49	75.4%	62	77.5%
3-5	4	9.3%	3	4.6%	7	8.8%
6-10	1	2.3%	4	6.2%	6	7.5%
11-15	1	2.3%	3	4.6%	1	1.3%
16-25	2	4.7%	0	0%	2	2.5%
>25	1	2.3%	6	9.2%	2	2.5%
Total Responses	*43*		*65*		*80*	

The line of defense of the team that provides direct, day-to-day support and oversight to "special category" relationship owners varies. The survey found that it broke down in this way: Third-Party Risk Management/1st Line of Defense (30%), Third-Party Risk Management/2nd Line of Defense (20%), Enterprise Risk Management/2nd Line of Defense (14%). The FTE composition for departments identified above was as follows:

	2023 Survey		2019 Survey		2015 Survey	
Response	Count	Percent	Count	Percent	Count	Percent
<3	29	67.4%	46	74.2%	62	77.5%
3-5	5	11.6%	3	4.8%	8	10%
6-10	4	9.3%	3	4.8%	6	7.5%
11-15	0	0.0%	5	8.1%	2	2.5%
16-25	0	0.0%	0	0%	0	0%
>25	5	11.6%	5	8.1%	2	2.5%
Total Responses	*43*		*62*		*80*	

Technology and Workload Management

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

The survey asked, "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)." Fifty-six percent of participants responded positively (and shared some of their innovative practices). That is an increase from 41% when we last asked that question.

Response	2023 Survey	2019 Survey	2015 Survey
No, and no plans to do so	19.5%	22.7%	26.3%
Not yet	24.4%	36.4%	27.5%
Yes – Explain and give specific examples.	56.1%	40.9%	46.3%

Technology adoption remains a challenge. Our data shows that 50% use the same technology to manage activities and reporting for both their vendor and special category third party risk management program. There is a range of practices based on asset sizes: The smaller institutions use the same system in 80% of cases and partially do so in 20% of cases.

Participants were asked to share whether they store both third party "vendor" and "special category" contracts in the same system. There has been no change since 2019: Fifty-five percent responded "Yes", while 45% responded "No".

Insight and Advice

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

There are insightful comments throughout the survey. The following is a list of the question numbers for easy access to them.

Q19) Storing vendor and non-vendor contracts.
Q20) Use of primary technology to manage activities, documentation and reporting.
Q21) Blanket exceptions to due diligence or ongoing monitoring.
Q22) Greatest challenges in developing an effective "non-vendor" third-party risk management program.
Q23) 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 2023 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. Following the recent Interagency Guidance, many institutions are reviewing and revamping their practices and RMA will continue to provide resources to help them in this journey.

Thanks again to all Third-Party Risk Management Roundtable members as well as other RMA institutions that contributed to and completed the 2023 RMA Third-Party Non-Vendor Risk Management survey. We greatly appreciate your participation and look forward to your continued support and dialogue at upcoming in-person peer sharing events.

Please see the following pages for detailed responses and examples of the range of practices institutions employ in 2023 in managing third-party/vendor risk management. For questions that were included in both the 2015 and 2019 surveys, we have included responses from both survey iterations for easy comparison. This full report is available only to participating institutions.