RMA THIRD-PARTY/VENDOR RISK MANAGEMENT SURVEY

FINAL REPORT
SEPTEMBER 2014

Operational Risk

JOIN. ENGAGE. LEAD.

ACKNOWLEDGMENTS

The survey was conducted by The Risk Management Association between June and August 2014. The vast majority of the questions were multiple choice. A total of 114 responses were received covering a wide range of asset sizes and types of financial institutions, including community, regional, super-regional and money center banks, investment banks and insurance companies, headquartered in the United States, Canada, and Europe.

This RMA survey was designed with the help of the RMA Vendor Risk Management Steering Committee comprised of: Debbie Manos-McHenry (Huntington Bank), Brian Roche (RBS/Citizens Bank), Eric Sierka (TD Bank) and Linda Tuck-Chapman (Bank of Montreal). This RMA survey was intended 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 some of the key challenges that banks and other financial institutions are facing.

This survey was designed as an outcome of RMA Vendor Risk Management round table, which was planned to help institutions review changes mandated by the OCC in its revised vendor management guidance (OCC 2013-29, "Third-Party Relationships" which rescinded OCC Bulletin 2001-47 and OCC Advisory Letter 2000-9 and compare the revised OCC Guidance with the changes made by the Fed to their Guidance to Managing Outsourcing Risk (Fed- SR 13-19 / CA 13-21). **Key item addressed in the survey include definitions of the critical activity.**

Please note that the terms, "third party," "vendor," and "supplier" were used interchangeably throughout this survey.

The following areas were addressed:

- Vendor management framework.
- Vendor selection and monitoring process.
- Critical vendors and critical activities.
- Fourth-Party Suppliers.
- Tools and techniques.
- Contracts.
- Reporting.
- Regulatory and Compliance.

The final report presentation style shows the participants responses, while masking the identity of the participant of the reporting institution for protection. 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 **MetricStream** for sponsoring this survey.

Institutions that participated in the survey:

Adirondack Bank	Amarillo National Bank
American West Bank	Bank of New Hampshire
BB&T	BMO Financial Group
BOKF, NA	Broadway National Bank
Capital One	CenterState Bank
Charles Schwab & Co., Inc.	CIBC
Citizens Bank	City National Bank
Columbia Bank	Commerce Bank
Community National Bank	CommunityOne Bank, N.A.
Delta Bank, N.A.	EverBank
Farmers and Merchants Trust Company	Federal Home Loan Bank of Pittsburgh
First Commonwealth Bank	First Federal Lakewood
First Horizon National Corporation	First National Bank of Omaha
Fox Chase Bank	Great Western Bank
Home Savings and Loan Company	HSBC
Huntington National Bank	Jefferies LLC
LegacyTexas Bank	Manufacturers Bank
MidCountry Financial	North American Savings Bank
NYCB	Pacific Mercantile Bank
Park Sterling Bank	PENSCO Trust Company
PNC Bank	RBS
Revere Bank	S&T Bank
State Farm Bank	Susquehanna Bancshares Inc.
AIG	Amboy Bank
Bank of America	Bank of the West
BBVA Compass	BOFI Federal Bank
Bremer Bank	Brookline Bancorp
CapStar Bank	Central Pacific Bank
Chemung Canal Trust	CIT
Citizens Banking Company	CoBank, ACB
Comerica Bank	Community Bank NA
Community Resource Bank	Credit Agricole CIB
Discover Financial Services	Farmers & Merchants Bank of Long Beach
Federal Home Loan Bank of Chicago	Fidelity Homestead
First Farmers and Merchants Bank	First Guaranty Bank
First Midwest Bank	First Niagara
FIS Global	Goldman Sachs
Hanmi Bank	Home State Bank, N.A.
Hudson City Savings Bank	Iberia Bank
KeyBank	MainSource Bank
Meridian Bank, N.A.	MUFG-Union Bank
OneWest Bank	Park National Bank
Peapack-Gladstone Bank	People's United Bank
QNB	Republic Bank & Trust

Royal Bank of Canada	Scotiabank
SunTrust	Talmer Bank & Trust
TD Bank	The Bancorp
US Bank	Victory Capital Management
Wells Fargo	Western Alliance Bank
WSFS Bank	The American National Bank of Texas
The Home Savings and Loan Company	Union Community Bank
Webster Bank	WesBanco, Inc.
WestStar 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 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 16,000 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.

EXECUTIVE SUMMARY

This RMA survey was intended 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 some of the key challenges that banks and other financial institutions are facing. The questions in the survey were grouped into eight areas:

- Vendor management framework.
- Vendor selection and monitoring process.
- Critical vendors and critical activities.
- Fourth-Party Suppliers.
- Tools and techniques.
- Contracts.
- Reporting.
- Regulatory and Compliance.

The survey was conducted by The Risk Management Association between June and August 2014. The vast majority of the questions were multiple choice. A total of 114 responses were received covering a wide range of asset sizes and types of financial institutions, including community, regional, super-regional and money center banks, investment banks and insurance companies, headquartered in the United States, Canada, and Europe:

- Asset size below $10 billion: 61 responses.
- Asset size between $10-50 billion: 22 responses.
- Asset size between $50-100 billion: 11 responses.
- Asset size between over $100 billion: 20 responses.

When asked to rate the maturity level of the vendor management program within their institutions on a scale from 1-5 (where 1 is completely mature, and 5 is not mature at all), none of the participants selected "completely mature," and 58% responded "somewhat mature," ranging from 49.2% of respondents with asset sizes below $10 billion and 55% of respondents with assets over $100 billion.

According to the survey, for nearly 46% of the institutions, the team responsible for developing and maintaining the supplier risk management framework, policy, and standard is located within the enterprise risk management function, particularly for institutions with asset size below $10 billion (58%). For institutions with more than $50 billion in assets, the function resides in procurement or a combination of procurement, vendor management, and enterprise risk management (65-72%). Oversight of the vendor risk management function for almost 50% of respondents (including 60% of respondents with less than $10 billion in assets) is located at the risk management department and for almost 30% of respondents a variety of governance functions, including operational risk management committee, legal, and compliance. For nearly 45% of respondents (54% of respondents with less than $10 billion in assets), the oversight function is centralized, for 15% it is decentralized, and for

40% (50-55% of respondents with more than $10 billion in assets) it is a hybrid structure involving the business line, subject matter experts, and centers of excellence. For 70% of institutions across all asset sizes, business lines have primary responsibility when it comes to managing vendors, and 14.2% have some combination of central utility and business segments.

For OCC-regulated institutions, 84% have defined (77%) or partially defined (7%) third parties. In addition to traditional providers of goods and services, the institutions identified additional third parties that are in their program today, including: co-branded products and services (54%), agents (53%), channel and distribution agreements (52%), correspondent banking agreements (49%), agency agreements (47%), and debt buyers (19%).

Based on the institution's asset size, there is a wide range of practice when it comes to the number of suppliers that are currently in institutions' supplier risk management program. The overall results show that more than 40% of respondents have fewer than 250 suppliers in their program (67% for asset size of less than $10 billion). The second highest response (19%) has above 2,500 suppliers (50% for asset size of more than $100 billion). Institutions with asset size in the $10 to 50 billion range from <1,000 to <2,500 (50%). This range is also reflected in the responses showing how many "enterprise critical" suppliers are managed in the institution's program with 51% ranging from 3 to 15 (72% for asset size <$10 billion) and 29% over 25 (70% for asset size > $100 billion).

In driving the process to identify vendors covered under the program, 70% of institutions make this determination based on the product or service provided with 26% using some combination of product/service, spend, data access, and criticality to the operations of the institution. Seventy percent of institutions use 3 tiers (43%) or 4 (27%) tiers of risk.

Due diligence on fourth parties or subcontractors of third parties/vendors is performed by 33% of institutions, but with significant variation among asset size: 71% of asset size <$10 billion and those >$100 billion and 91% of $50-100 billion are not, whereas 59% of those $10-50 billion are conducting due diligence on fourth parties. In those cases where due diligence is taking place, it is occurring either when the contract is put in place with the primary supplier (20%), when the primary supplier notifies the institution of the use of a fourth party (13%), or some other combination of triggering events (10%).

While 50% of institutions have already defined what constitutes a "critical activity" within their institutions, 47% are in the process of defining it (65% for asset sizes over $100 billion and 73% for $50-$100 billion). **The detailed survey results include sample definitions of "critical activities."** When asked about segmenting the suppliers, answers revealed that for 61% of respondents "risk" is the main factor when deciding if the vendor is critical. For over 30% of respondents "risk and spend" is the deciding factor with another 8% further defining the elements of risk considered, including criticality, materiality, customer contact, and complexity. These responses were consistent across all ranges of asset size.

When it comes to the number of full time employees (FTEs) dedicated to third-party management within the centralized risk management oversight function, the survey shows that the number of FTEs dedicated varies widely based on the size of the institution, with

the highest concentrations between <3 and 10 FTEs (91% of respondents with <$10 billion in assets selected <3), increasing to ranges from 11 to 25 (40%), and >25 (25%) reported by institutions with asset size greater than $100 billion. In comparison, the number of dedicated FTEs increased across all ranges of asset size for the decentralized structure with 27% selecting over 25 FTEs (80% for asset size over $100 billion) and 41% less than 3 FTEs (59% for asset size under $10 billion).

According to the survey, each institution involves multiple areas of subject matter expertise when it comes to conducting due diligence and the vendor selection process. Information technology and information security are the most frequently included (91%), in addition to compliance (75%), legal (81%), business continuity management/planning (68%), and finance (61%).

For institutions that conduct secondary supplier risk assessments (in addition to questions asked in requests for proposal (RFPs), the most frequently selected secondary assessment was information security (79%), followed by information technology (57%), business continuity management (46%), and legal (32%). About 56% of respondents send additional questionnaires to vendors for risk assessment purposes beyond the RFP. This varied widely based on the size of the institution with less than 39% of those under $10 billion and 80-90% of those over $50 billion reporting sending questionnaires for risk assessment purposes.

Eighty percent of respondents reported sending questionnaires as part of ongoing monitoring with the frequency of re-assessments and triggers for conducting the re-assessment varying widely. In addition to due diligence questionnaires and monitoring, 73% of respondents conduct site visits for critical vendors, ranging from 61% for asset size under $10 billion to 85-90% for asset size over 10 billion. In addition, 78% of respondents report that once the contract is executed, risk is re-assessed on an annual basis for high-risk suppliers, and similarly for critical suppliers.

In addition, participants shared names of tools/technology they currently have in place for sourcing and supplier risk management. Institutions with asset size under $50 billion more frequently reported using Microsoft Excel and SharePoint applications with larger institutions using packaged tools, including RSA Archer, Hiperos, Ariba, and IBM Emptoris.

From the survey, we learned that 57% of institutions either use standard contracts (20%) or standard contracts "with exceptions" (37%) for their vendors. Eighty-six percent of those using standard contracts "with exceptions" reported an exception approval process beyond the line of business, with 14% reporting a designated "committee" for exceptions or some combination of additional stakeholders conferring with the business (67%), including legal, compliance, and an array of internal executive committees. When asked about the use of "Supplier Codes of Conducts" only 23% of participants currently require their use.

With respect to reporting and escalation of vendor risk issues, 72% of institutions escalate risk issues to the business line, the company's subject matter experts, and upper management, 67% escalate issues to the company's operational and management committees, 30% regularly report status of issues to the business, and 8% report periodically to the Board of Directors or a Committee of the Board. For respondents with more than

$100 billion in assets, in addition to reporting and escalation processes, 30% perform vendor trend-line analysis to evaluate overall risk the vendor relationship poses to the company and 40% report risk issues in real-time with reports always available to management, and procurement/sourcing. Sixty-seven percent of institutions don't formally identify concentration risk among their vendors and 23% report on concentration risk by manually extracting information from spend or risk management data.

Quality assurance processes are in place to validate the risk management activities and monitoring in the first line of defense (the business) in 43% of institutions ranging from 33% for asset size < $10 billion to 60-65% for asset size over $50 billion. Validation of regulatory compliance and effectiveness of the vendor risk management framework is conducted annually by 72% of the institutions responding. The majority of institutions have a designated person who tracks and communicates regulatory and compliance updates/changes related to third-party management. Independent reviews are conducted by a variety of functions with the highest concentration in the $10 to $100 billion asset size institutions reporting that this is done by internal audit (50–55%).

Based on the most recent regulatory examination, the areas of criticism included: monitoring (28%), reporting (20%) governance (17%), and due diligence (15%). Other (28%) includes safeguards against consumer harm, consistency in execution among business lines, and documentation of policies and procedures. The highest concentration among criticism options in this survey question was reported by institutions in the $50-$100 billion asset sizes with 55% reporting criticism in monitoring and 46% in reporting.

Please see the pages following for a detailed responses and examples of the range of practices these institutions employ in managing third-party/vendor risk and how they are responding to evolving regulatory guidance from the OCC, CFPB, Federal Reserve, SEC, OSFI, and other regulatory bodies.