



Operational Risk Sails into the Mainstream

Stephan Salvador
Director, Risk and Compliance Consulting

Table of Contents

Centralized Risk Management Oversight 3
Areas of Risk Responsibility 3
Completed and Planned Operational Risk Assessments..... 4
ORM Expenditures 6
Summary 6
For More Information 7

It seems like only yesterday that the financial services industry was scrambling to define Operational Risk Management (ORM) and pondering how to integrate it into its workflows. But recent research conducted on behalf of Metavante indicates a new era has dawned, one marked by banks making significant progress toward leveraging ORM on behalf of their organizations. Especially heartening is the willingness of mid-tier, regional, and community banks to embrace the discipline and move forward -- banks with assets ranging from \$500 million to \$50 billion, which were the focus of this study.

Centralized Risk Management Oversight

The progress made by this segment of the financial services industry is spotlighted by what our survey revealed regarding the adoption of centralized risk management oversight. Placing risk management squarely at the center of the banking enterprise makes standardization and consistency possible across the institution, creating accountability for managing risks that impact all business units across the enterprise, but that may not be the responsibility of one specified function. Creating a core focal point promotes a common understanding of risk that leads to meaningful analysis in the shortest possible period of time. Indeed, centralized governance forms the foundation of ORM; the discipline's effectiveness flows directly out of it.

Our research indicates that a vast majority of banks understand this. More than eight in 10 of those polled indicated they had implemented centralized risk management oversight, and 64.7% of those that had not completely implemented it indicated they were moving in that direction. Only 5.9% of respondents lacked any formal risk management structure.

Adoption of the approach wasn't limited to the larger banks surveyed. While it is true that banks with over \$1 billion in assets led the pack with an 87% adoption rate, smaller banks -- those with \$500 - \$999 million in assets -- weren't far behind with an 80% adoption rate.

An essential part of the organization's ORM nucleus is a specific position or positions to manage the risk function: someone who functions as a Chief Risk Officer (CRO) with related staff (depending on the size of the bank and its requirements). Our research shows that while the "CRO" nomenclature may not yet be commonly accepted parlance for the job -- titles like "compliance officer" and "operations manager" were cited approximately half the time -- the consolidation of risk functions under specific personnel has definitely begun to coalesce.

In fact, the majority of those polled hold such titles, with over three-fourths indicating they have a position in place that handles *both* operational risk and compliance issues. Conjoining the two makes sense, since compliance is evolving to become a subset of ORM in some banks. For smaller banks, where salary resources may become an issue, it is an efficient way to proceed.

Areas of Risk Responsibility

The broader perspective required for ORM influences the types of risk for which the central risk governing body bears responsibility. Our research uncovered the following breakdown:

	Primary Responsibility	Minor Responsibility	Not a Responsibility	Primary Responsibility	
				Large Bank	Smaller Bank
Fraud prevention	58.4%	33.7%	7.9%	42%	71%
Data privacy	56.4%	30.7%	11.9%	49%	63%
Business continuity planning	47.5%	35.6%	16.8%	44%	50%
Vendor management	38.6%	49.5%	11.9%	27%	48%
Internet banking security	26.7%	46.5%	26.7%	18%	34%
Network security	17.8%	45.5%	36.6%	9%	25%

Figure 1. Types of operational risk addressed by banks.

Risk officers rate fraud prevention, data privacy, and business continuity high as concerns. This is to be expected, as these risk types fall across the board and are difficult to contain under the jurisdiction of a single function. Those cited lower on the list -- vendor management, Internet banking security, and network security -- are risk types for which there is by and large a tradition of risk management in place. Internet banking and network security are typically the domain of the IT department; the finance department has historically handled vendor management (more procurement than risk assessments). Rank of importance did not vary much between small and large banks, although concern over fraud was particularly acute for community banks, perhaps displaying the awareness that fraudsters are moving away from larger banks that they consider "hard targets," toward those they feel may be less equipped to detect the schemes they put into play.

Completed and Planned Operational Risk Assessments

It is interesting to note that although fraud prevention tops the list of operational risk responsibilities as shown in Figure 1, the practice of completing fraud-centric risk assessments falls behind in comparison to risk assessments being conducted in other areas.

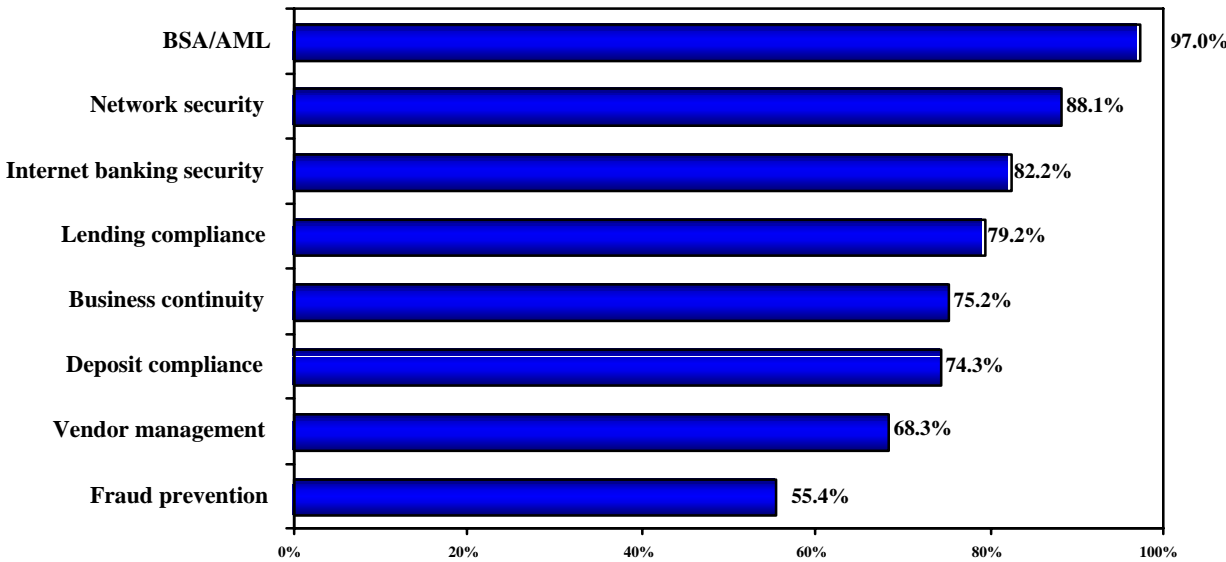


Figure 2. Risk assessments performed in the past year.

The priorities illustrated in Figure 2 are not evidence of misdirected energy and efforts; they simply provide a snapshot of ORM at this point in its development. Compliance issues, because of the "heat" they generate from regulating bodies, have been driving risk management over the past few years. From that standpoint it is easy to see why, especially in the wake of 9/11, anti-money laundering (AML) and the Bank Secrecy Act top the list, with technology-related security not far behind.

Regulators have been most demanding of banks in these areas. The lower incidence of fraud-related assessments looks more severe than it is when compared to these categories. In truth, the fact that 55.4% of surveyed banks have undertaken them is heartening, especially considering that fraudulent activity generates high visibility in the local and national news. The same positive view can be taken for the remainder of the risk assessments in the lower part of the list, including business continuity and vendor management. We can only expect that these numbers will rise in the years to come, an assertion borne out in part by the risk assessments our respondents have planned for 2007:

	Definitely Planning	Possibly	Not Planning	DK/NA	Definitely	
					Large Banks	Smaller Banks
BSA/AML	98.0%	1.0%	1.0%	0.0%	100%	96%
Network security	88.1%	11.9%	0.0%	0.0%	84%	91%
Business continuity	80.2%	13.9%	3.0%	3.0%	89%	73%
Internet banking security	79.2%	17.8%	3.0%	0.0%	76%	82%
Lending compliance	73.3%	18.8%	5.0%	3.0%	71%	75%
Deposit compliance	68.3%	16.8%	12.9%	2.0%	73%	64%
Vendor management	65.3%	23.8%	7.9%	3.0%	62%	68%
Fraud prevention	54.5%	36.6%	5.9%	3.0%	53%	55%

Figure 3. Risk assessments respondents are planning for 2007.

It is reassuring to discover that smaller banks, despite misgivings of this type, are doing a decent job of keeping up with their larger counterparts when it comes to risk assessment. In the areas of fraud, as well as network and Internet security, they are actually doing a better job:

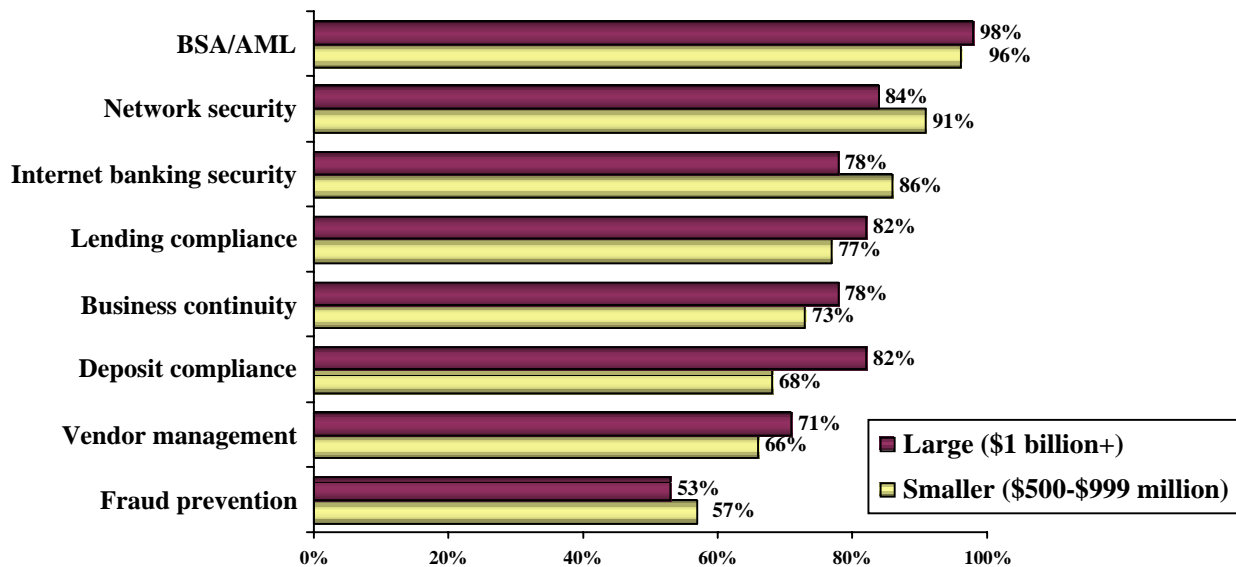


Figure 4. Bank risk assessments by bank size.

This isn't to say that banks perform risk assessments *only* on the categories mentioned so far. Our findings showed that nearly six in 10 had performed at least one of 13 other types of risk assessment, those most often cited being privacy, audit risk, and compliance risk. This scattering of types is indicative of a methodology that is in its adolescent stages, with consolidation of risk management likely to take place in the future. The important thing to remember here is that banks are getting a foothold in the practice of making risk assessments, which readies them to apply what they have learned to other relevant categories as they broaden their scope, making their job easier and more likely to succeed.

ORM Expenditures

Just what kind of expenditures are banks making in ORM to ensure they get up to speed and stay there? The largest portion of expenditures, 37%, is directed toward technology. No surprise there, given the range of tools that are needed to knit together the plethora of components and cross-dependencies that define ORM. Among these are AML transaction monitoring, network intrusion, fraud monitoring, Internet banking security, and risk assessment systems, to name some of the most important.

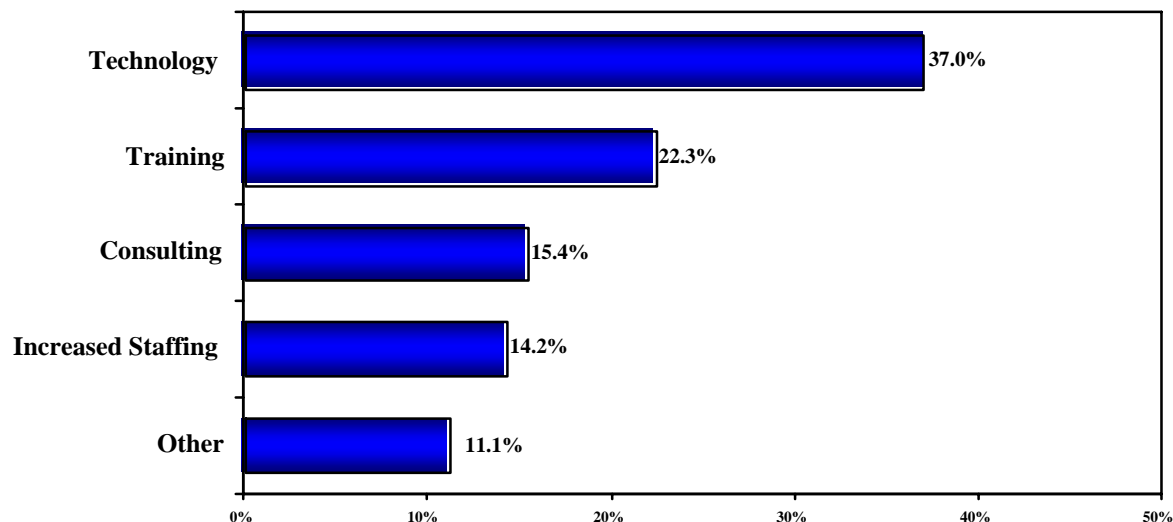


Figure 5. Allocation of expenditures for risk management.

Despite their heavy investment in technology, savvy financial institutions understand technology alone does not guarantee success and that a best practices ORM program consists of a fully integrated system of people, processes, and technology. This knowledge likely contributes to the high ranking attributed to training and consulting, the number-one and number-two runners-up to technology in ORM investments.

Training, in this case, refers to those educational efforts carried out by the bank, or someone hired by the bank, mainly to get staff up to speed on integrating the aspects of ORM affecting their position into their daily workflows. This occurs once the groundwork and the bank's culture are "readied" for the introduction of ORM.

By contrast, *consulting* pertains to the people and resources that help the bank lay out this groundwork, which can include establishing formal organizational structures and governance; redefining supporting roles for technology, operations, internal audit, compliance, and business unit managers; providing for ongoing operational risk self-assessments and monitoring at the business unit level; and leveraging existing risk and Sarbanes-Oxley data into new enterprise risk systems. A natural outgrowth of such planning is staff growth, which likely explains the number-four position on the expenditure list.

Summary

We believe the information in this study helps support Metavante's belief that the banks best positioned to succeed in the future will move to conjoin their operational risk and compliance management functions. Such consolidation promotes a strong risk framework, productive leverage of risk assessments and audits, and a common language that can exceed minimum compliance requirements. Given the increased regulatory presence within the financial services industry and the predisposition of regulators to require formal risk assessments in all areas of the enterprise as part of their ongoing examination process, we believe there really are no viable alternatives to this type of ORM model for banks.

This reality has forced an epiphany upon banks, clearly reflected in the facts and information summarized in this article. The new regulatory climate is driving the systems, technologies, and organizational designs banks are putting in place, and while it may be premature to proclaim ORM an industry standard, it appears to be well on its way to being one.

This development bodes well for the future health of the financial services industry, but it raises a flag of caution for banks that have not yet significantly integrated the discipline into their enterprise. These institutions will likely remain unable to move beyond traditional consumer compliance and financial controls, and because they have not transformed their business accordingly, they may find themselves less and less a viable option to existing customers and prospects, not positioned well to compete with financial institutions that have embraced ORM best standards and practices and as a result are more likely to enjoy improved customer service, greater efficiency, better technology utilization, increased speed to market of new products, and lower risk.

Using this survey data as supporting evidence for a business case, we recommend these banks force themselves to take a proactive approach to build a sustainable risk management program, and do it in the next few years before they fall farther behind, making it more difficult to catch up.

For More Information

Metavante Corporation's team of risk management specialists comprises practitioners in financial services, operations, technology, compliance, and risk management.

Our operational risk expertise is focused specifically on the areas of fraud prevention, compliance, information security, privacy, business continuity, IT recovery, physical security, and vendor management.

We deliver measurable results that help prepare your institution for the current competitive and regulatory environment.

To learn more, call 1-800-822-6758 and talk with one of our consulting professionals, or visit us at metavante.com.

A note on the methodology supporting this article:

Telephone interviews were conducted with 101 financial institutions. Targeted respondents were those responsible for operational or enterprise risk management at their bank. The breakdown of the sampling quota was as follows:

Bank Assets	Population (based on Metavante list)	Final Study Sample	
		N	Percent
\$10 billion or higher	6.7%	5	5.0%
\$2 billion to \$9.99 billion	18.4%	16	15.8%
\$1 billion to \$1.99 billion	24.1%	24	23.8%
\$600 million to \$999 million	34.0%	39	38.6%
\$500 million to \$599 million	16.9%	17	16.8%

Note that the assets of the final sample matched the population reasonably well, so the data was not weighed in the analysis presented in this report.

