

Designing an Operational Risk Program for a Community Bank

Stephan Salvador

Managing Director, Risk Management Consulting

Table of Contents

Is your institution as prepared as it needs to be?.....	3
Defining operational risk	4
Advancing your operational risk program - why do it?	4
<i>Mandated investment in risk management</i>	4
<i>Proactively investing in risk management</i>	5
<i>Investing in risk management to create value</i>	5
<i>Establishing your goals</i>	5
Identifying program components.....	7
1. <i>Options for organizational structure</i>	8
2. <i>Sharing risk management responsibilities</i>	9
Business and support units	9
Operational risk management.....	9
Internal audit	10
3. <i>Leveraging risk and controls assessments</i>	10
The time is now for an operational risk program.	11
For more information	11

Introduction

We live in a time of enormous uncertainty, brought about by technological change, escalating threats, unstable political climates, and an increased blurring of international borders that demands we all play in the same economic sandbox.

No financial institution, regardless of size or geography, is immune to the effects of industry risks and regulatory pressures. In fact, operational risk management has become a prerequisite for strong performance in today's community bank marketplace.

So, more than ever before, community banks, from the board of directors through all levels of management, need to be in a well-informed, documented, and advanced position regarding how they manage their risk.

Regulators are examining operational and compliance risks under the Bank Secrecy Act, USA Patriot Act, Gramm-Leach-Bliley Act, Basel II Accord, Sarbanes-Oxley, and FFIEC guidelines, and the outcome will affect your examination rating and, possibly, your continued viability.

Is your institution as prepared as it needs to be?

If you're hearing comments like those that follow, they should serve as a warning that your organization needs to develop a comprehensive operational risk management program:

“The board has directed us to formalize risk management functions.”

“We're getting unfavorable comments from regulators on our inconsistent risk assessment management reporting.”

“It seems like all we do is go through risk assessments by the examiners, external auditors, internal auditors, and consultants, and the overlapping work effort is burdensome and inefficient.”

I'm not sure we're using the latest and greatest tools in information security to protect our customers' data and privacy.”

“We have too many number one priorities and we won't be able to recover all mission-critical business units and their systems to meet the needs of the business units.”

“We've had some recent teller fraud losses that could have been prevented.”

A community bank can manage these operational risks more strategically, efficiently, and effectively with a well-designed risk management program.

Defining operational risk

A recent and generally accepted definition of operational risk is “the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.” It also can include legal and compliance-related risks.

Management of operations risk is not a new practice in banking – it’s always been essential to prevent fraud, maintain internal controls, and reduce errors in transaction processing. But in the past, banks relied upon internal controls within business lines, supplemented by the audit function, to manage operational risk.

Operational risk management as a comprehensive discipline is now at the same level of importance as credit and market risks. Recent regulations, industry trends, new types of threats and exposures, and a growing number of high-profile operational losses are dictating that banks and examiners view operational risk management as a separate discipline.

It is important that a bank’s definition of an operational risk program includes a full range of operational risks, and captures the most significant causes of operational losses, such as: internal and external fraud; compliance with AML, BSA, SAR, and CTRs regulations; vandalism; customer information security and privacy; physical security; business disruption and system failures; process-level risk within wire transfers, ACH, deposit operations, and loan operations; and vendor management.

Advancing your operational risk program – why do it?

There are three excellent reasons for a community bank to advance its operational risk program: regulators are going to require you to do so over time; taking a proactive stance means doing it on your own timelines and on your own terms; and your shareholders expect you to add value to your bank.

Mandated investment in risk management

There are a number of regulatory and legislative mandates for banks to create and/or enhance an operational risk management program.

- FDICIA and Sarbanes-Oxley Section 404 both require internal controls review across most departments, which are a subset of the bankwide risk assessment process.
- The Bank Secrecy Act and the USA Patriot Act require programs to be in place for anti-money-laundering, suspicious activity reporting, large cash transactions, customer identification, and more.
- The Gramm-Leach-Bliley Act requires safeguards for customer information, privacy, and information security.
- FFIEC IT Handbooks direct senior management and the board of directors to manage IT risks, including information security, business continuity, disaster recovery, and vendors.
- Boards of directors can be held criminally liable for failures to control risk

Proactively investing in risk management

There are a number of reasons why taking a proactive approach to operational risk management is just good business.

- Beyond the expense of regulatory penalties and fines, the loss in business momentum and revenue growth after formal agreements, memoranda of understanding, and cease and desist orders could be considerable.
- Banks need to strengthen defenses to avoid losses from fraudsters, hackers, identify thieves, and natural disasters.
- Avoiding C1 risk – the new street term for reputational risk – which occurs when your bank appears on the front page of section C of The Wall Street Journal.
- Allocate capital based on business unit risk profile to encourage business unit ownership and management of their risks.

Investing in risk management to create value

Developing an operational risk management program ultimately will add value to your bank as it:

- Enables your bank to meet commitments to customers, employees, and shareholders
- Differentiates your bank favorably to the marketplace during uncertain times when security is a top concern of consumers and the business community

Don't become a victim of "Regulatory Duress," which will require you to invest quickly and heavily to remedy your program. Rather, start planning today and you will benefit by building sustainability into your operational risk management program, which leads to strengthening the operational resiliency of your bank.

Establishing your goals

As you begin to develop your operational risk program, you'll want to articulate the goals of that program.

The overarching goal is to have a unified view of operational risks and controls across all business units and processes; to have three-pronged: a common risk assessment and measurement system; and to have sound policies governing the risk management process.

Ultimately, an integrated operational risk management program with robust analytics will lead to more efficient use of capital and personnel.

Specifically, you will want to:

- Promote a risk culture throughout the bank that proactively manages risk.
- Move your future position on an operational risk management spectrum beyond basic requirements, to one that is more advanced.
- Undergo needed organizational change, while ensuring that the new operational risk management program fits within your existing structure, and does not disrupt activities that are functioning well.
- Leverage existing operational risk disciplines, processes, tools, systems, and resources that do not add to costs.
- Communicate and coordinate between the executive, operational risk, and business functions, while maintaining segregation of responsibilities, controls, and oversight.
- Conduct in-depth operational risk self-assessments in all business units.
- Have your internal audit serve as an independent reviewer of the operational risk management program.
- Give strategic feedback to the board and to senior management on the overall level, trends, and necessary allocation of resources.
- Consistently evaluate the risk/return of businesses through capital allocations.

Identifying program components

Operational risk management can be modeled after credit risk management. Just as banks have been managing their lending activities, analyzing portfolios, monitoring allowance for loan losses, and varying loan concentrations, a similar structure should be wrapped around the various aspects of operations and technology.

A community bank would not think of moving forward without a loan review or credit risk committee, established lending policies, or metrics to follow charge-offs. Operational risk is no different.

In fact, with such a broad scope, one would think that coordination and consistency would be our industry standard, yet we all know that these disciplines are managed separately, and thus the risks are not aggregated.

The eight program components identified in the graphic above are the key ingredients for a successful operational risk program.

Three of these eight elements must be addressed first as you move forward, since they are typically what is lacking most in community banks:

- Establish formal organizational structure and governance, including an operational risk committee equipped with a charter, guiding principles, and operating mode.
- Redefine supporting roles for your technology, operations, internal audit, compliance, and business unit managers.
- Provide for ongoing operational risk self-assessments and monitoring at the business unit level, and at the same time, leverage existing risk information from internal audit, compliance, business units, FDICIA, and Sarbanes-Oxley.



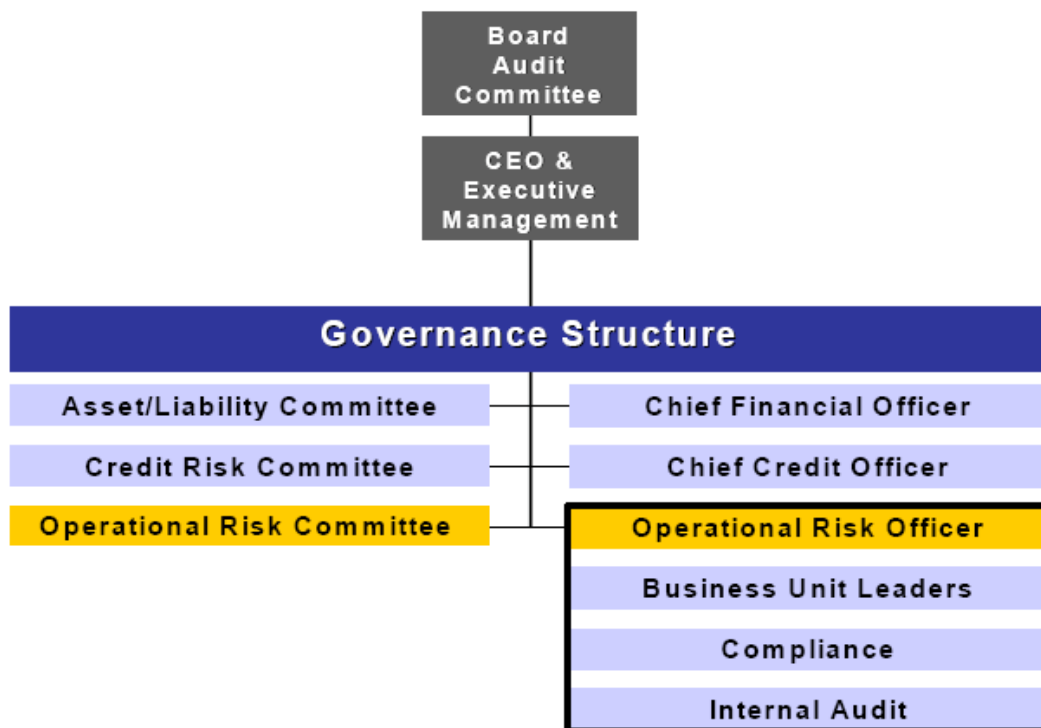
1. Options for organizational structure

The first issue to address is how a community bank should organize its governance for an operational risk program.

The chart below illustrates a suggested governance structure based on typical functions within community banks.

The board audit committee should provide guidance on strategies, how much risk the bank is willing to take, ensure that risks are managed within tolerance, and approve all major changes to risk policies.

The CEO and executive management team should review the governance of operational risk management activities, and delegate policy formulation and day-to-day oversight to committees and risk managers.



Advantages of this functional alignment include:

- Stronger, coordinated roles for business unit leaders, compliance, and internal audit via a new operational risk committee
- An integrated approach to and consistent framework for managing operational, market, and credit risk
- Cultural and process changes can be driven from the top
- Regional risk management efforts can be linked into a corporate committee and risk office
- Builds upon, streamlines, and eliminates redundant risk management and compliance efforts

The operational risk officer should focus on building the risk assessment process across all departments, which is the most underdeveloped in community banks. In addition, this position should not disrupt existing reporting relationships of credit and market risk managers, should remain independent from production duties, and should coordinate with all other risk management and compliance activities.

Underlying this functional alignment is an intersection between traditional compliance and this new concept of centralized risk management. A comprehensive risk management program must address laws and regulations with compliance implications.

Conversely, managing compliance with consumer regulations is a critical component of a comprehensive risk management program. A solution is to join the compliance function with the risk management function. Some larger banks also join the internal audit function with the risk management function.

2. Sharing risk management responsibilities

In support of the above governance structure, the following are the major functional roles for effective alignment of risk management responsibilities:

BUSINESS AND SUPPORT UNITS

- Own operational risk
 - Assign coordinator who links the business unit to risk management
 - Conduct risk self-assessments using tools from risk manager
 - Respond to changes in risk metrics
 - Work with other units on cross-functional projects to prevent silos
 - Implement corrective actions and new risk solutions (policies, technology, process change, personnel)

OPERATIONAL RISK MANAGEMENT

- Define and manage the program
 - Build awareness
 - Partner with business and support units
 - Provide tools and consultation
 - Ensure consistency in risk assessment process
 - Aggregate and evaluate data by risk category and department
 - Maintain risk model and loss event database

INTERNAL AUDIT

- Validate the program
 - • Leverage risk assessment information as input to audit plan
 - • Identify and report operational risk trends that require resolution
 - • Independent link to the board audit committee

With these new roles in place, you should be able to reach your goals and successfully implement the program.

3. Leveraging risk and controls assessments

As operational risk management evolves into a unique discipline, advanced analytics and reporting are required to quantify risk levels with departments, and to focus mitigation efforts. As banks deal with FDICIA, Sarbanes-Oxley 404, and internal and external risk assessments, the need to organize and report risk data more efficiently becomes imperative.

The purpose of a Risk and Control Model is to provide a new level of organization and presentation of risk assessment and internal control information. For each department included in your risk assessment, you should be able to record risk criteria, control objectives, findings, and recommendations in a model with assignment of risk type, inherent and residual risk scoring, evaluation of control effectiveness, direction of risk, final disposition, and key metrics.

The quantification of risk should be based on inherent and residual risk scores, with residual risk being most important because it is the remaining risk in the department after the assessment of the effectiveness of controls and risk solutions. It is at this level that you should decide to accept a risk position within a department, or work towards a more effective control.

Regarding additional leverage points, with the approval of your external auditors, you may want to convert your FDICIA or SOX 404 controls information into your model, and through cooperation with internal audit and compliance, add their assessments and corrective actions, as well.

As an output, the risk model should produce heat maps by department that track the number and severity of inherent risks and residual risks after controls are applied, and allow for aggregation across departments.

The same logic that brought the industry to a single book of record for the bank's financial statements (general ledger), and then to customer activity (CRM), now leads us to a similar position with risk; over time, your risk assessment model should evolve into the single book of record for your risk profile.

The time is now for an operational risk program

Operational risks are present throughout the scope of your organization, either internally through people, processes, and systems, or through external events, like computer hackers, or even natural disasters.

When not offset with a solid plan, these risks can be potentially devastating to your organization; however, with an ongoing operational risk program, your bank increases value to shareowners.

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 prepare your institution for the current competitive and regulatory environment.

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

