Common Breakdowns in Risk Management

Recognizing and managing key risks have never been more challenging for large financial institutions, and the job seems only to get more difficult. Risk managers are responsible for a daunting range of products and activities, and handling 99% of the risks still leaves 1% that threatens the entire enterprise.

The Dodd-Frank Act added to risk managers’ already considerable compliance responsibilities through new standards for business lines ranging from swap dealing to mortgage lending. Firms face increased liability for noncompliance, as regulators are armed with greater powers to sanction companies, impose penalties, and seek redress for harmed parties.

For the risk-management, compliance, and internal-audit functions at large financial institutions, being good is no longer good enough. Learning from mistakes — preferably those of others — aids the pursuit of excellence in these disciplines, and the many breakdowns that have fed headlines in recent years are a rich opportunity to explore common risk-management mistakes.

PUT RISK MANAGEMENT IN A POSITION OF AUTHORITY

Firms court a risk-management breakdown when business lines dominate risk-management, compliance, or audit functions, and when risk managers lack the stature they need to criticize and challenge a business unit. Firms that view risk management as an obstacle to profitability undermine

COMMON RISK-MANAGEMENT MISTAKES

- Failing to regard risk management as a top-tier discipline
- Inadequate staffing in risk-management functions
- Weak and inadequate risk data and information
- Ignoring warnings about potential problems
- Inattention to potential risk accretion at high-volume businesses perceived as low risk
- Inadequate due diligence on vendors and third parties
- Disregarding lessons that can be learned from peers’ experiences
- Not holding all employees responsible for ethical behavior
these functions and put managers at a disadvantage in sustaining a conversation with business-line executives about balancing risk and reward. A popular and practical solution is to make sure business lines own the risks they take, but organizations should be careful about turning risk managers into business partners who view their role more as enabling profitability than ensuring strong controls.

Risk inevitably catches up with those who ignore it. The initial costs associated with a breakdown are followed by back-end expenses in rebuilding risk controls and restoring a diminished reputation with clients, regulators, the media, and the public. But institutions can break the cycle by emphasizing vigilance and by communicating the lasting importance of the risk-management function — even when external conditions seem benign.

RECRUIT TALENTED MANAGERS, AND STAFF RISK FUNCTIONS APPROPRIATELY

Having talented professionals dedicated to risk management is essential. A firm must devote the human resources to risk management that the importance of the function demands. Senior risk managers must have the requisite skills and have risk-management experience commensurate with the challenges faced by a large financial institution.

The best risk managers also accommodate changing risk profiles, and recognize that techniques that work today may come up short only a few months later. Organizations should have risk-management processes that are flexible and able to meet challenges that arise from circumstances beyond firms’ control.

The common perception of risk management as just an expense has fed a reluctance to spend money on it, but companies need trained, adequately staffed functions to cover the size and nature of their businesses. Staff turnover can add to this challenge, and adroit competitors poach risk-management talent just as they poach talent in business lines. Firms should build in redundancies and avoid key-person dependencies so that the departure of valued risk managers doesn’t leave gaps. Planning for talent flight helps companies find replacements quickly.

THE RIGHT BALANCE OF RISK INFORMATION

Getting the right information into the right peoples’ hands is one of the trickiest risk-management challenges large institutions face, and plenty of recent failures can be traced to communications breakdowns in which senior risk managers and board members did not get the data they needed — either because the information simply did not reach them, or was not gathered in the first place.

Large financial institutions must make sure they gather usable and relevant information on subjects as varied as credit exposure, counterparty risk, and even the public’s views about the firms’ products and practices. The entire picture is important, and firms should not hesitate to deliver it to senior risk managers and the board for fear of causing offense.

The larger and more complex the firm, generally the more varied types of risk, including — and perhaps especially — those that are hard to identify. Size and complexity increase the distance between risk creators and those who need to receive, make sense of, and react to information on risk. A bank of large size and high complexity can be tempted to look past risks from small functions, and miss that they could inflict substantial losses on the entire enterprise. A good rule of thumb: If an activity is so complicated that very few people can understand it, managing the associated risks may be impossible. Firms may wish to reconsider whether to engage in the activity.
The amount of information delivered to senior risk managers and the board is as important as the type of information. An overabundance of information might draw attention away from the risks that matter. Too little information might leave out essential details and make the information conveyed unclear and unusable. When a board is not getting the right amount of usable data, it cannot effectively challenge a firm’s management and give direction on risk tolerance.

Technological challenges also lead to breakdowns in the flow of vital information. After mergers and acquisitions, companies may be left with multiple risk-management programs and incompatible technology platforms. Procedures for IT and platform integration should include risk management.

**FOLLOW UP ON WHAT YOUR INFORMATION IS TELLING YOU**

The failure to recognize and respond quickly to warnings about potential problems is another type of risk-management breakdown. Internal audits underpin strong risk management, but firms may ignore concerns identified in internal audits — often to their extreme detriment. Some warnings come from outside the firm. Consumer-advocacy groups, for instance, can serve as valuable critics of a firm’s retail practices. Activities that generate high volumes of customer complaints also merit additional monitoring.

Banks must take their examiners’ warnings especially seriously. The bank supervision process is designed to identify and fix problems early. The goal of supervision is sound banking, not to be merely punitive. When bank examiners flag matters requiring attention — “MRAs” — it is often a firm’s best chance to fix a problem before it evolves into an enforcement matter. Banks that use the examination process constructively — to identify operational weaknesses and promptly rectify them — improve their odds of avoiding serious risk-management lapses.

**PAY ATTENTION TO SEEMINGLY LOW-RISK FUNCTIONS**

Simple, small errors can have outsized consequences if they are repeated frequently enough — witness problems with mortgage-foreclosure documentation. Supervisors have begun to ask
whether large banks have other, similar processes for other types of products. Firms with relatively straightforward but high-volume businesses of any sort should be mindful that the marginal risk of each transaction over time can accrete, eventually constituting a messy problem. Institutions should probe these businesses for the fault lines, which often require unconventional thinking to spot.

KEEP AN EYE ON VENDORS
Banks have never been more liable than they are today for the practices of the vendors they select to carry out important functions. Prudential regulators and the Consumer Financial Protection Bureau have recently taken actions against banks and thrifts for products and services provided to their customers by third parties, as well as for due-diligence failures in selecting and monitoring those third parties. The CFPB also told companies in a bulletin last spring that they can be held liable for the actions of firms with which they contract.

A firm that “deconstructs” its operations — that is, it uses a third party to perform a function that the institution might otherwise have performed — must think of those operations as if the firm itself carried them out. Due diligence must not end with vendor selection; in the eyes of regulators, vendor due diligence is a matter of continuously managing risk and verifying that the third party’s practices meet the institution’s standards.

MONITOR AND LEARN FROM YOUR PEERS
Banks that recognize and promptly correct their own lapses can also benefit from understanding other firms’ lapses. When an industry peer suffers a high-profile breakdown in risk management, banks should assess their own risk management and controls for similar operations. Risk managers and audit committees should constantly watch peers for signs of trouble and ask whether their own company is prone to the same risks — and if so, whether it has a process in place to gauge the type of risk that led to the problem.

DOING THE RIGHT THING
Perhaps the best safeguard against risk-management lapses is a firmwide culture that encourages employees always to make a good-faith effort to do the right thing. Many of the recent high-profile enforcement actions against U.S. and global financial institutions resulted from actions by employees who lost sight of this principle. Countless individual careers, several major institutions, and the banking industry have suffered severe reputational and financial damage as a result.

Responsibility for a firm’s culture resides at the top of the organization. It is up to management and the board — through personnel and compensation decisions, the handling and use of consumer complaints, and other means — to instill sound ethics and create a sustainable enterprise. Subcultures within a firm lacking that commitment need to be identified, monitored, controlled, and ultimately, corrected. Risk managers play a role here, but their best efforts must be coupled with a firmwide commitment to fair conduct.

CONCLUSION
Financial institutions serve their clients by accepting risk, and the past few years have offered constant reminders about the consequences of failing to manage it. Policymakers are naturally focused on risk management, compliance, and internal audit given the repeated breakdowns of recent years, but it’s up to the companies to make sure that their own vigilance isn’t cyclical. Perceptions of risk priorities are variable; the principles that guide its management are constant.
Contact Promontory

For more information, please call or email your usual Promontory contact, or one of those listed below:

**Konrad Alt**  
Managing Director, San Francisco  
kalt@promontory.com  
+1 415 986 4160

**Michael Dawson**  
Managing Director, Washington, D.C.  
mdawson@promontory.com  
+1 202 384 1080

**Kathy Dick**  
Managing Director, Washington, D.C.  
kdick@promontory.com  
+1 202 384 1092

**David Gibbons**  
Managing Director, Washington, D.C.  
dgibbons@promontory.com  
+1 847 707 4279

**Susan Krause Bell**  
Managing Director, Washington, D.C.  
skrausebell@promontory.com  
+1 202 384 1151

**Patrick Parkinson**  
Managing Director, Washington, D.C.  
pparkinson@promontory.com  
+1 202 384 1052

**Wayne Rushton**  
Managing Director, Washington, D.C.  
wrushton@promontory.com  
+1 202 384 1015

**William Rutledge**  
Managing Director, New York  
rutledge@promontory.com  
+1 212 365 6984

**Julie Williams**  
Managing Director and Director of Domestic Advisory Practice, Washington, D.C.  
juwilliams@promontory.com  
+1 202 384 1087

To subscribe to Promontory’s publications, please visit promontory.com/subscribe2.aspx

Follow Promontory on Twitter @PromontoryFG

Promontory is a leading strategy, risk management, and regulatory compliance consulting firm for the financial services industry. Promontory’s professionals have deep and varied expertise gained through decades of experience as senior leaders of regulatory bodies and financial institutions. Promontory assists clients in meeting regulatory requirements and in enhancing governance, risk management, strategic plans, and compliance programs.
Goals for the Session

1. Operational Risk 101 - gain working knowledge of the language and tools of Operational Risk
2. Operational Risk 201 - understand a few critical components of an effective Operational Risk Management Program
3. Operational Risk 301 - be aware of hot topics, discuss emerging risks, “fat” tail losses, 10X Risk, and future of Operational Risk Management disciple
101

• **Operational Risk 101**, gain working knowledge
  • History of Operational Risk as a risk discipline
  • Supervisory guidance, key sources
  • Definitions, event type categories, and four data elements
  • Approaches to quantification of capital

Basel II

• It all starts with Basel Committee on Banking Supervision
  • Published Basel II in June 2004 to create an international standard to determine how much capital banks need
  • Rule of thumb: the greater the risk taken, the higher the capital
  • Final version separated Operational Risk from Credit Risk
  • BCBS introduced in 2004 a capital charge for Operational Risk as part of the new capital adequacy framework
  • Basel has periodically updated Operational Risk guidance
Why did BCBS Add a Capital Charge Operational Risk?

Probably...

• Barings (1995: $1.4 billion Nikkei Futures)
• National Australia Bank (2004: A$360 million foreign currency trading)
• 9/11/2001
• Globalization
• Deregulation
• Technology

Basel Committee Definition

Definition of Operational Risk

• Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

• This definition includes legal risk, but excludes strategic and reputational risk.

• Legal risk includes, but is not limited to, exposure to damages, fines, penalties, or punitive damages resulting from civil cases and supervisory actions.
Methods of Operational Risk Capital Measurement

• Basel II has given guidance to 3 broad methods of capital calculation for Operational Risk

• Basic Indicator Approach - based on annual revenue of the Financial Institution

• Standardized Approach - based on annual revenue of each of the broad business lines of the Financial Institution

• Advanced Measurement Approaches - based on the internally developed risk measurement framework of the bank adhering to the standards prescribed (methods include IMA, LDA, Scenario-based, Scorecard etc.)

Basel II Event Type Categories

• Internal Fraud - misappropriation of assets, tax evasion, intentional mismarking of positions, bribery

• External Fraud - theft of information, hacking damage, third-party theft and forgery

• Employment Practices and Workplace Safety - discrimination, workers compensation, employee health and safety

• Clients, Products, & Business Practice - market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning

• Damage to Physical Assets - natural disasters, terrorism, vandalism

• Business Disruption & Systems Failures - utility disruptions, software failures, hardware failures

• Execution, Delivery, & Process Management - data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets, and failure to adhere to internal policies and limits.
AMA: Four Fundamental Elements

1. Internal (Loss) Data
2. External (Loss) Data
3. Scenario Planning
4. Business Environment and Internal Control Factors

Insurance

• BCBS stipulates a number of requirements before insurance can be counted as a mitigant, for example:
  • The insurance company must have a rating of A (or equivalent).
  • The policy must be no less than one year in duration
  • Cancellation requires 90 days notice
  • Must not have exclusions triggered by bank failure of regulator action
### 201

**Operational Risk 201**, discuss five drivers of effective Operational Risk Management

- Clear **Roles** and Responsibilities, with emphasis on Governance
- The role of the **Board** of Directors
- The right **KRI**s
- **Scenario Analysis**
- **Emerging External Risk** management process

---


Detailed descriptions of **roles** for:

- Board of Directors
- Senior Management

Detailed descriptions for **processes**:

- Risk Management Environment
- Monitoring and Reporting
Basel Committee -- June 2011
First Four Principles

1. The Board should take the lead
2. Banks should develop a framework
3. Board shall review the framework periodically
4. Board should approve a risk appetite and have tolerance statement

Operational 301, discuss macro US and global issues related to the management of banks

• “Fat” Tail Losses

• “10X Risk”
The Big Risks

- Form Over Substance
- Failing to Focus on Critical Few Activities
- Making ORM a Quantitative Exercise

ORX 2011 Operational Loss Analysis

Events: 36,259

Total Losses: € 25.1 billion

Average: € 620 million
ORX Reported OpLoss Events 2011

Loss Categories in Euros

ORX Losses 2011
25.1 MM Euros

Loss Categories in Euros
What is “10X Risk”? 

- Origin 
- Definition 
- Implications 

10X Risk in the U.S. 

- 6 Bank Panics in 19th century 
  Panic of 1907 
- 9000 bank failures Great Depression 
- 3000 failures Banking Crisis of 1985-1992 
  -- 2008 in 11 states 
- 460 + bank failures since 2008 
  -- 72% in 10 states
Why do banks fail?

Years of Regulators’ Material Loss Reviews reveal:

- **Board** governance weak - directors lack bank skills
- **Management** lacks skill IMMR risks
- **Controls** are inadequate
- **Strategy**: Bank lacks strategic plan, or if it has one, it is inadequate

Bank Failures are Operational Risk Failures

- **Board** = People and Processes
- **Management** = People and Processes
- **Controls** = Processes and Systems
- **Strategy** = People and Processes
The Future of Bank Risk Management?
10X Risk vs. X Risk

• Focus on Operational Risk?

• Common Sense: Major in the Majors
  • 10X
  • Fat Tail

A Shameless Plug

Broke: America’s Banking System: Common Sense Ideas to Fix Banking in America

About basic banking in the U.S.

Published by The Risk Management Association

Available March 20, 2013
at www.rmahq.org and www.amazon.com