

**booz&co.**

---

Bringing Back Best  
Practices in Risk  
Management  
*Banks' Three Lines  
Of Defense*



---

---

Booz & Company is a leading global management consulting firm, helping the world's top businesses, governments, and organizations.

Our founder, Edwin Booz, defined the profession when he established the first management consulting firm in 1914.

Today, with more than 3,300 people in 58 offices around the world, we bring foresight and

knowledge, deep functional expertise, and a practical approach to building capabilities and delivering real impact. We work closely with our clients to create and deliver essential advantage.

For our management magazine *strategy+business*, visit [www.strategy-business.com](http://www.strategy-business.com).

Visit [www.booz.com](http://www.booz.com) to learn more about Booz & Company.

---

## CONTACT INFORMATION

### Beirut

#### Peter Vayanos

Partner  
+961-1-336433  
[peter.vayanos@booz.com](mailto:peter.vayanos@booz.com)

### Frankfurt

#### Thorsten Liebert

Principal  
+49-69-97167-864  
[thorsten.liebert@booz.com](mailto:thorsten.liebert@booz.com)

### Hong Kong

#### Giles Brennand

Senior Executive  
+852-3650-6100  
[giles.brennand@booz.com](mailto:giles.brennand@booz.com)

### London

#### Alan Gemes

Partner  
+44-20-7393-3290  
[alan.gemes@booz.com](mailto:alan.gemes@booz.com)

#### Charles Teschner

Partner  
+44-20-7393-3792  
[charles.teschner@booz.com](mailto:charles.teschner@booz.com)

#### Dr. Peter Golder

Principal  
+44-20-7393-3234  
[peter.golder@booz.com](mailto:peter.golder@booz.com)

### Moscow

#### Steffen Leistner

Partner  
+7-495-980-9962  
[steffen.leistner@booz.com](mailto:steffen.leistner@booz.com)

### Munich

#### Dr. Johannes Bussmann

Partner  
+49-89-54525-535  
[johannes.bussmann@booz.com](mailto:johannes.bussmann@booz.com)

### New York

#### Paul Hyde

Partner  
+1-212-551-6069  
[paul.hyde@booz.com](mailto:paul.hyde@booz.com)

### São Paulo

#### Ivan de Souza

Partner  
+55-11-5501-6368  
[ivan.de.souza@booz.com](mailto:ivan.de.souza@booz.com)

### Shanghai

#### Andrew Caine

Senior Executive Advisor  
+852-3650-6100  
[andrew.caine@booz.com](mailto:andrew.caine@booz.com)

### Sydney

#### Peter Burns

Partner  
+61-2-9321-1974  
[peter.burns@booz.com](mailto:peter.burns@booz.com)

### Tokyo

#### Yoshiyuki Kishimoto

Senior Executive Advisor  
+81-3-3436-8609  
[yoshiyuki.kishimoto@booz.com](mailto:yoshiyuki.kishimoto@booz.com)

*Nick Donovan and Hussein Sefian also contributed to this Perspective.*

---

# BRINGING BACK BEST PRACTICES IN RISK MANAGEMENT

## *Banks' Three Lines Of Defense*

### **Executive Summary**

Many financial institutions have had horrific losses over the past 18 months. A variety of largely exogenous factors have been blamed for the losses, such as ownership structures and incentives, rating agencies, and the absence of effective market pricing for some products. However, we contend that at a small number of banks, a focus on basics actually prevented many losses. In particular, they benefited from a strong risk culture combined with a sharp focus on three effective lines of defense: top management and the front office, the risk management function, and audit. These lines of defense, staffed with capable individuals imbued with a strong sense of risk awareness, are at the heart of effective risk management.

### **The Root of the Problem**

The current downturn originated largely in the U.S. financial markets. Cheap credit from the Federal Reserve fueled an extraordinary leveraging of the U.S. economy—with a particular focus on consumer debt, especially mortgage debt. The original sin was not in the lack of regulation but in the expansion of credit to the non-creditworthy on outrageous terms—as in the case of 105 percent loan-to-value loans being given without credit checks. Underwriting banks, large and small, packaged and resold this debt to investors, including other banks, as collateralized debt obligations and mortgage- or asset-backed securities; this freed up their balance sheets and allowed them to go at it again. The latter step was predicated on the notion that the purchase of the debt would bring a perpetual stream of repayment income against “secure” collateral—and, of course, this notion depended on the idea that the real estate market would keep rising. Globally, many institutions, assured by ratings, believed this to be the case.

Cheap debt also contributed to the explosive growth in banks' balance sheets. These purchases of assets resulted in irresponsible leverage, rising at some banks to debt-equity ratios of 30:1, 40:1, and even 100:1. However,

---

based on recent interviews with leading financial institutions, our hypothesis is that neither cheap central bank money nor inadequate regulation nor even the “complexity” of risk was the culprit behind this overleveraging. The job of financial institutions is to collect, price, disaggregate, de-correlate, reaggregate, and price risk. To blame complexity is to seek a barter economy. The real culprits were bad governance, bad incentive systems, and astonishingly poor risk management at some major banks.

With the inevitable decline of the U.S. real estate market, the leverage-powered engine of growth went into reverse. For primary originators (or the resold obligation owners), asset values sank below loan values. Moreover, a major goal of “packaging and aggregation” had been to create pools of lower or more diversified risk. However, this was built on the premise that the underlying assets were not correlated, which, of course, was not the case given that many of the bets were based on one super bet: the prospects of the U.S. housing market.

What we are now observing is an almost Darwinian process of selection, in which the strong or fast vanquish the weak or slow. As the pressure for growth became greater and greater over the past few years, almost all banks became more focused on returns, in absolute or relative terms, and less on risk. However, not all banks began with equal capabilities in terms of managing risk—particularly in terms of level of funding and human resources. As a result, we have seen the near-death of weaker business models—namely, the stand-alone integrated investment bank. We have also seen and will continue to see distress among banks whose appetite for growth and risk exceeded their ability to handle it. Losses at other players—

medium-size insurance companies, for instance—may yet surface.

### **Risk Governance Failures**

The enormous losses we have seen have resulted in many top management casualties. However, while chief executives and investment banking directors are falling on their swords, postmortem evaluations and industry commentators are pointing fingers at a bewildering variety of underlying external causes. These include moral hazards arising from public ownership and compensation structures; a “herd” mentality across the industry; rating agencies’ compensation schemes and models; opaque reporting and illusory off-balance-sheet transfers; and inadequate market pricing infrastructure for some products. Surely, all these factors were at work. However, in many respects, losses stemmed from a failure of one of the core functions of banks: risk management. By this, we do not mean simply the risk management function. Rather, we are speaking of risk management in a holistic sense.

Banks have invested heavily in risk management tools and processes over the years, conducting a number of large and complex projects. Although such initiatives made banks compliant with regulations, often they failed to address more fundamental issues. For instance, few banks have focused sufficiently on addressing the root causes of poor data integrity and quality, resulting in systems that have proved ineffective at producing timely, relevant, decision-oriented information. When this information is available, too few managers have the experience, authority, and oversight to make actionable decisions. In addition, overreliance on complex models that were understood by too few people within the bank (let alone

the regulators) created a false sense of comfort.

However, the more serious gaps within companies are related not to technology and models but to the role of individual people and general decision-making processes. Good tools and processes provide the basis for a solid risk management framework, but the human aspects of decision making must not be underestimated. For a number of institutions, the strong drive for profit in the seemingly benign pre-crisis environment led to veiled but intense pressures on risk departments to approve increasingly risky transactions. In turn, these assaults on the institutional risk culture have weakened the stature and prominence of the risk discipline.

Banks that want to see their way successfully out of the downturn will need to address this issue. The key to strong risk management in complex, turbulent markets is a renewed focus on the basic concept of effective lines of defense, working in conjunction with a pervasive risk culture. The three major lines of defense are top management and the front office, the risk management function, and audit (see Exhibit 1).

### **Enabling a Strong Risk Culture**

The risk culture of an organization stems from its leadership. If the board is to understand, define, and actively manage its organization’s risk appetite, it needs a core of executive directors with solid business and risk expertise. The board must be able to appreciate the risks being run. In practice, this means board members must not only be informed but also understand the risk—return drivers inherent in major product innovations and concentrations. Additionally, they must understand and accept the consequences of major

## Exhibit 1

### Best Practices in Risk Management Governance



Source: Booz & Company

implementation decisions. Most boards of investment banks did not, for example, discuss the consequences of the huge increase in absolute leverage or the unintended consequences of some bankers’ almost unlimited earning power. Actively shaping and agreeing to a risk profile is the first step in building a culture in which risk management is seen as an enabler of the front office rather than an obstacle to be circumvented.

The second step in building an appropriate risk culture is to encourage constant communication. A company’s culture should make it easy to get the right people engaged on potential risk issues, as well as hold individuals accountable for their own decisions and actions. Where clear accountability exists, no one can assume that risk is not their responsibility;

risk issues are everyone’s concern. Modern investment banking products involve multiple asset classes with reinforcing risks; at a portfolio level, dangerous correlations can exist not only between a firm’s positions but also between the firm’s positions and counterparties’ positions. No individual—whether a specialist in a certain asset class, product, or function—can be solely responsible for identifying and mitigating against all possible causes of unacceptable losses. Steps to improve communication can be as simple as requiring risk managers to sit on the trading floor, and encouraging, rather than silencing, a variety of opinions on portfolios.

The third step in strengthening risk culture is to raise the profile of the risk teams, particularly in the front office areas, and to increase the extent to which risk

professionals are represented on executive committees and boards of directors. While the risk management function has grown in size over time, it is typically short on top talent. How many former traders actually work on risk teams? How many risk managers combine both strong quantitative skills and a deep understanding of the business? How many board members have worked on a trading floor? Establishing the credibility of the risk function through a deep knowledge of the business and its ever-evolving product requirements would go a long way toward entrenching a culture in which risk professionals are perceived to be on equal footing with the front office, rather than merely support professionals. Risk management must be pervasive to the culture, not the responsibility of the risk function alone.

## Back to Basics: The Three Lines of Defense

*Top Management and the Front Office:* Football (or soccer) coaches sometimes say that for the goalie to miss a save, 10 other players must have missed it before him. Fixed-income traders and desk heads at some banks obviously missed some goal-line saves. They also took unnecessary risks, as if they were shortsightedly playing to win a single game and build their individual reputations rather than looking toward winning the tournament as a team (that is, ensuring the long-term success of their firm).

Various entities—rating agencies, in particular—could be and have been made scapegoats in the wake of the credit crisis. Investors thought they could rely on the agencies to provide reliable ratings information. However, greater scrutiny by top management on the part of both buyers and sellers would have played a large role in preventing some of the problems. For example, one product that has received public scrutiny was the GSAMP Trust 2006-S3, a Goldman Sachs second-mortgage securitization in which the average loan-to-value of these second properties was 99.29 percent, where 58 percent of the loans were no- or low-documentation, and where GSAMP could not effectively foreclose.<sup>1</sup> Of this issue, 93 percent was rated as investment grade. No sophisticated model is necessary to raise questions about the logic of selling or buying such an instrument.

There are three characteristics of a healthy first line of defense: sustainable risk–return thinking; usable, up-to-date risk-related information; and respect for limits and other basic controls.

Sustainable risk–return thinking is a corollary of a communicative

risk culture. Discussions about new products, existing and new positions, and other issues must be broad and not limited to meeting quarterly targets or other short-term goals. Both the front office and top management must have reliable and consistent information with respect to the positions and the risks they are taking. Finally, limits and other basic controls must be respected. For example, limit setting and limit monitoring must be done by mechanisms with teeth, traders must be forced to take holidays, and segregation of duties should be clear and enforced.

*The Risk Management Function:* Alongside a farsighted and responsible front office, banks need an effective, respected risk management function. Risk managers need to go beyond the traditional role of “limit cop”: Not only do they need to understand and challenge the front office; they also need to develop a deep understanding of concentrations, correlations, and early warnings. Finance must develop a more critical understanding of the underlying risk–return drivers of profitability.

If the secret of best-in-class risk management lies in the risk culture of an institution, that culture is enabled by the capabilities of the risk managers. For risk managers to engage with the front office on equal footing, and for the front office to respect the disciplines imposed by risk, high-caliber risk managers are required. Not only do these managers need to have a clear understanding of the business and the risks being taken on, they also need to keep pace with a rapidly evolving and increasingly complex array of products.

However, highly skilled risk managers are not enough on their own. A supporting organi-

zational structure, infrastructure, and internal processes are also required. Risk managers need timely, accurate data, as well as the authority to enforce actions and impose rapid sanctioning mechanisms when appropriate. Roles and responsibilities must be clearly allocated.

Traditional risk-type separation will not suffice when it comes to products that cross the divide, such as structured products, or in assessing correlations or concentrations that involve multiple risk classes. We are observing the formation of more “traded risk” teams that deal both with market risk and with the counterparty and issuer risks arising from traded products. To get a wider view across risk types, portfolio oversight and strategic risk management units perform stress tests and concentration analysis on the macro level, with the authority to force change where necessary.

However, sophisticated risk analysis must be underpinned by reliable marking to market of illiquid assets. Despite the noise in the system about the deleterious impact of marking to market, a lack of this discipline would impair the functioning of those markets that have largely been spared by the credit crisis to date. The role of the finance organization independently validating “marks” is also of critical importance.

This is an important final point: The effectiveness of the second line of defense requires that the control functions—finance, risk, compliance—work hand in hand. For instance, all too often, finance has critically challenged negative swings in performance while paying less attention to the causes of peaks in performance. A focus on decomposing the drivers of profit, good or bad, needs to be the mentality prevailing in the future.

<sup>1</sup> Washington Post, Tuesday, October 16, 2007, “An Unsavory Slice of Subprime.”

---

*Audit:* The third line of defense—audit—has arguably failed in its role of providing independent and objective assurance of the effectiveness of the first two lines of defense.

For the third line of defense to act as an effective steward of the policies and procedures approved by the board, it needs to have not only a good understanding of the business—how the front office makes money—but also a deep understanding of risk management discipline. In best-in-class organizations, audit and finance teams have the ability to blend their strong process and IT know-how with their understanding of the business and risk. For example, audit teams should investigate and validate mark-to-market positions, ensuring the integrity of information as it passes from one system to the next.

Moreover, the third line of defense must develop a strong critical approach to each functional disci-

pline, performing more than just a “checking the checkers” role. It is not inconceivable, for example, that after reviewing the securitization process, the internal audit team could identify and bring to the board’s attention potential flaws, such as overreliance on rating agencies. All too often, auditors document processes as a box-ticking exercise to ensure compliance, with limited critical review of potential weaknesses.

Finally, the third line of defense must be empowered to enforce its findings. Audit items often remain open quarter after quarter, with no consequences for the executive who fails to act. A more disciplined approach is required, with senior leaders taking a leading role.

### Conclusion

Short-term memory is a persistent problem in financial markets. After the failure of Barings PLC in 1995 and the bailout of Long

Term Capital Management hedge fund in 1998, leading industry experts and regulatory bodies a series of recommendations to prevent similar losses in the future. In retrospect, a great deal of progress has subsequently been made along the scientific and technical aspects of risk management. But at a more fundamental level—in terms of good governance, strong lines of defense, and a healthy risk culture—much remains to be done.

Bank managers should act to establish a strong risk management culture now, while the front office has been humbled and there is strong consensus in the organization. As John F. Kennedy said, “In the Chinese language, the word ‘crisis’ is composed of two characters—one representing danger, and one representing opportunity.”

---

## BOOZ & COMPANY WORLDWIDE OFFICES

### Asia

Beijing  
Hong Kong  
Mumbai  
Seoul  
Shanghai  
Taipei  
Tokyo

### Australia, New Zealand, and Southeast Asia

Adelaide  
Auckland  
Bangkok  
Brisbane  
Canberra  
Jakarta  
Kuala Lumpur  
Melbourne  
Sydney

### Europe

Amsterdam  
Berlin  
Copenhagen  
Dublin  
Düsseldorf  
Frankfurt  
Helsinki  
London  
Madrid  
Milan  
Moscow  
Munich  
Oslo  
Paris  
Rome  
Stockholm  
Stuttgart  
Vienna  
Warsaw  
Zurich

### Middle East

Abu Dhabi  
Beirut  
Cairo  
Dubai  
Riyadh

### North America

Atlanta  
Chicago  
Cleveland  
Dallas  
Detroit  
Florham Park  
Houston  
Los Angeles  
McLean  
Mexico City  
New York City  
Parsippany  
San Francisco

### South America

Buenos Aires  
Rio de Janeiro  
Santiago  
São Paulo