

# Operational Risk Management

*Too Important to Fail*

**Pierre Pourquery and Johan De Mulder**

## TABLE OF CONTENTS

Preface .....	2
The Banking Industry: Fertile Ground for Operational Risk.....	3
A Strong Appetite for Growth, Innovation, and Risk.....	3
Incentive Schemes that Undermine a Bank’s Risk Culture .....	5
A Fragmented Control Environment.....	7
Impact of Back and Middle Office Staffing and Regulatory Pressure .....	7
Operational Risk Management: A Need for Radical Change.....	9
The Limitations of Operational Risk Frameworks .....	9
Five Factors that Undermine Operational Risk Frameworks.....	10
Call to Action: A New Paradigm for Operational Risk Management .....	13
Fewer Controls Can Be Better.....	13
Be Proactive, Not Reactive .....	14
Integrate, Don’t Segregate.....	15
Make Individuals Responsible.....	17
Support the Business.....	18
Recent BCG papers in risk management: .....	19
Authors.....	19

## Preface

---

The crisis has raised critical questions about the way banks manage their credit and market risks. And although the spotlight is on risk management in general, there has been much less attention paid to operational risk and the role it has played in the crisis. It is a vastly underrated discipline.

Operational failures have led to many of the losses associated with the crisis. Some of the more conspicuous failures include the flawed evaluation of subprime assets, ineffective operating models that prioritized innovation over the industrialization of processes, poor governance and risk management practices, inadequate information systems (concerns over potential exposure to toxic assets still persist), and incentive schemes that rewarded short-term results with no regard to a bank's long-term stability.

Banks and regulators should be alarmed by the consequences of underestimating the importance of operational risks. The recent spike in operational failures has highlighted several weaknesses in the control environment of most banks:

- The imposition of too many controls has created a fragmented environment hampered by duplication, poor connectivity, unclear roles and responsibilities, and the obfuscation of an integrated view of risk. The proliferation of controls has also created a false sense of protection in many banks, which has led to a lack of risk awareness across the organization.
- The frameworks for managing operational risk, which were inspired for the most part by Basel II, cannot protect banks from events as extreme and complex as the global financial crisis. Most of these frameworks, while capable of measuring economic and regulatory capital, tend to be more reactive than proactive when dealing with emerging risks.
- The precrisis surge of growth and innovation put enormous pressure on these flaws, turning small cracks into major fissures. Banks were deploying and integrating highly sophisticated business processes, organizational structures, and technology infrastructure. Additional stress came from record volumes of activity in both retail banking and capital markets. Vulnerable risk-management frameworks were simply overwhelmed.

Banks must improve their operational risk management to restore the confidence of shareholders, customers, and regulators, and to assuage concerns that their business models are too risky—and perhaps not even sustainable in the long term. Banks also need to learn from recent operational risk failures and determine whether their risk management approaches are equipped to manage these threats.

At the same time, banks must look beyond restoring confidence, complying with tougher regulations, and heading off operational failures. They need to change their perspective on operational risk, recognizing that this discipline is not only critical to ensuring sustainable growth, but is also essential to creating competitive advantage.

Such radical change should include the creation of a “control of controls” function and a new detection system that converts weak signals into strong ones, the implementation of operational risk limits, the creation of an Extreme Stress Team that pinpoints the vulnerabilities of operations, and a radical cultural shift that recognises the importance of managing operational risk.

## The Banking Industry: Fertile Ground for Operational Risk

Historically, banks have been fertile ground for significant operational risks. Prior to the crisis, they tended to have a strong appetite for growth, innovation, and risk. To make matters worse, many banks had incentive schemes that undermined a risk culture, along with control environments that were extremely fragmented.

### *A Strong Appetite for Growth, Innovation, and Risk*

Prior to the crisis, three factors led to a significant increase in banks' operational risks: the growth of retail banking, the growth of capital markets, and the proliferation of innovation and complexity in capital markets.

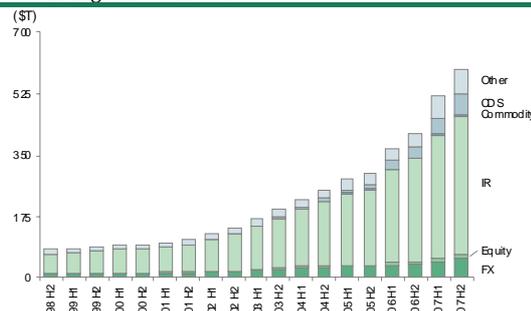
**The Growth of Retail Banking.** Especially in the UK and the US, the volume of mortgages soared over the past ten years, fuelled by rising house prices, low interest rates, and lax lending standards. Many banks lacked sufficient processing capacity to deal with the explosion of deals. In smaller, younger financial institutions, in particular, the risk management and governance structures took much longer to catch up with the growth in mortgages. The stress on processes increased the likelihood of bad deals going through and led to a range of errors and poor decisions:

- **Upstream:** Apart from unintentional mis-selling, file mismanagement was common.
- **Midstream:** Due diligence teams often missed or ignored mistakes made in the underwriting process. Loan officers were overwhelmed by the huge volume of loans. Moreover, the realization that these loans would not be on a bank's book very long—they would soon be sold or securitized—made loan officers less vigilant.
- **Downstream:** Few people in collections and recovery had the experience to identify which cases should be worked out with the customer, as opposed to encouraging the borrower to sell the house.

**The Growth of Capital Markets.** Market volume increased significantly over the past ten years. The OTC derivatives market has had spectacular growth. (See Exhibit 1.) The \$62 trillion CDS segment continued to expand in the first half of 2008, as investors sought further credit protection in the aftermath of the subprime crisis.

Exhibit 1: The volume of OTC derivatives has soared

Outstanding OTC derivatives



Source: OTC derivatives market activity reports, Monetary and Economic department, BIS

This growth strained a system that was already burdened by customization, a lack of automation, and bilateral agreements. Because of the special nature of OTC transactions, confirming trades between counterparties takes much longer than it does for exchange-traded products, which can be confirmed quickly via straight-through processing. The delay can lead to losses due to payment or collateral breaks or litigation, which can arise due to disagreements about the precise terms.

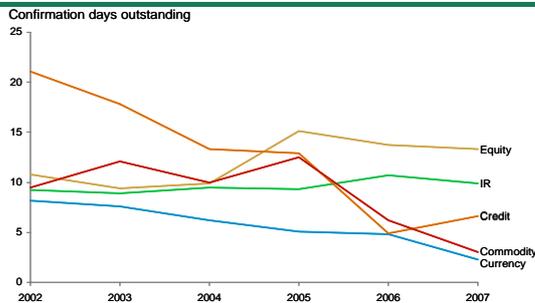
Regulatory pressure has reduced some of the risk associated with the growth of capital markets, but more action is needed. In 2002, the OTC confirmation days outstanding—a good measure of operational risk in OTC transactions—was extremely high for credit derivatives<sup>1</sup>. It was 21 business days compared to only 9 for interest rate derivatives. It was lower still for currency derivatives. Since then, regulatory pressure has led to a dramatic reduction in the number of confirmation days outstanding, particularly for credit derivatives. This is a critical improvement, given the exponential growth in trade volumes, but further improvements are still needed.

As late as July 2008, Ben Bernanke, the chairman of the US Federal Reserve, attacked the weak infrastructure of the OTC derivatives market, which strains the ability of market participants to settle transactions in a timely and efficient manner. The weak infrastructure can be strained by critical events such as a major bank failure—like the unravelling of Bear Stearns—or ratings downgrade.

<sup>1</sup> OTC confirmation days outstanding, or day's worth of OTC business, is defined as the number of confirmations outstanding times 22 divided by the monthly number of OTC trades.

The OTC infrastructure still seems vulnerable to sudden surges in trading volumes. There was a marked increase in confirmation backlogs for credit derivatives when the volume of CDS trading surged in 2007. (See Exhibit 2.)

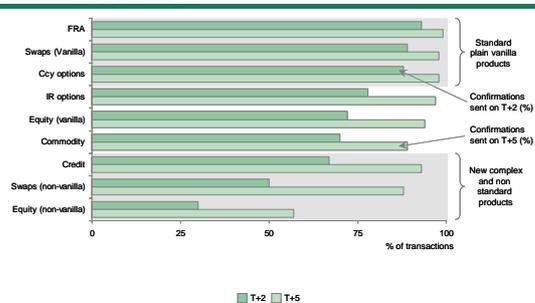
Exhibit 2: Confirmation backlogs for credit derivatives increased in 2007



Source: ISDA operations benchmark study, ISDA

**Increased Innovation and Complexity in Capital Markets.** Banks have relied on product innovation to create competitive advantage, but the introduction of new products—and in particular, complex structured products—inevitably leads to greater operational risk. Non-standard products do not lend themselves to automation. The lack of automation can lead to operational failures, especially when volumes surge.

Exhibit 3: Complex products lead to longer confirmation times

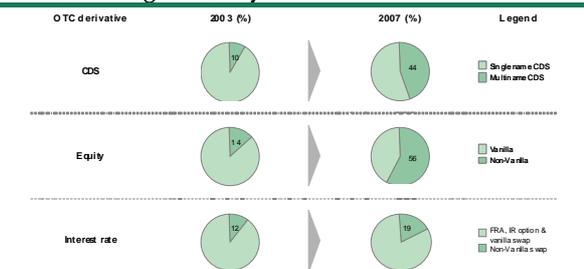


Source: ISDA operations benchmark survey 2006, ISDA

The link between product complexity and confirmation times is clear. FRAs, Vanilla Swaps and currency options are standardized contracts that are largely automated. In 2006, all confirmations for these products were sent out by T+5. (See Exhibit 3.) For complex products, by contrast, less than 70 percent of confirmations were sent out by T+2. Some were not sent out by T+5. Non-vanilla equity derivatives were the worst offenders, with 43 percent of confirmations not sent out by T+5.

Among OTC derivatives, the proportion of complex products has increased significantly. (See Exhibit 4.) The increase is especially noticeable for equity derivatives, where the proportion of non-vanilla products increased from 14 percent in 2003 to 56 percent in 2007. The proportion of multi-name credit default swaps, which have a portfolio or basket of CDSs or a CDS index, increased from 10 percent of all CDSs in 2003 to 44 percent in 2007.

Exhibit 4: The proportion of complex products has increased significantly



Source: ISDA operations benchmark survey, ISDA and OTC derivatives market activity reports, Monetary and Economic department, BIS

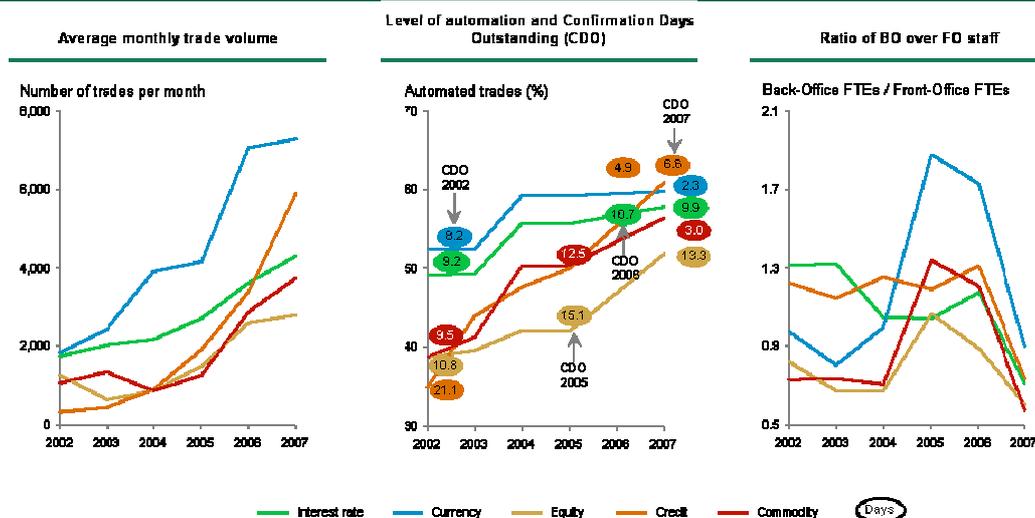
Improving automation is critical. The growth of complex OTC products creates a challenge for banks, but it does not mean that increased confirmation backlogs and operational risks are unavoidable.

We analyzed the impact of trade volume, level of automation, and back and middle office staffing on confirmation backlogs over the last six years, and found that:

- Automation has the largest impact on reducing confirmation backlogs, even as trade volume grows exponentially.
- Automation is possible for complex products, given the right regulatory incentives and market structure.
- Tight back and middle office staffing levels, coupled with low levels of automation, will aggravate the impact of volume increases.

The middle graph of Exhibit 5 shows the relationship between increased automation and confirmation backlogs. For currency, credit, and commodity OTC products, increased automation led to significant reductions in confirmation backlogs from 2002 to 2007 despite exponential growth in trade volume as well as under-resourced back and middle offices. In addition, automation helped banks reduce large backlogs in commodities, equities, and interest rates.

Exhibit 5: Automation generally leads to lower confirmation times



Source: BCG analysis of ISDA operations benchmark survey results

### *Incentive Schemes that Undermine a Bank's Risk Culture*

The financial industry has been compromised by a system of asymmetric incentives, whereby the people who benefit the most from increasing the bank's risk profile do not bear the losses when the bets backfire. The agency problem is acute in financial institutions where compensation practices do not align employees' interests with the interests of shareholders, depositors, or debt holders.

Bad incentives drive bad behaviour, and thus increase operational risks. It comes as no surprise that of the ten largest operational risk losses reported in the first quarter of 2008, six were related to inappropriate behaviour. These were due to internal fraud or theft, unauthorized activity, improper business practices, a lack of disclosure, or some combination of these factors. The problems associated with incentive schemes take different forms in retail banking and capital markets.

**Incentive Schemes in Retail Banking.** Under the originate-to-distribute model, which took hold in the retail banking industry prior to the crisis, several layers of securitization separated the eventual holders of the credit risk from the actual origination of the loans. The credit rating agencies gave investors confidence in the underlying assets, but in many cases they failed to provide sufficient transparency or perform adequate due diligence. They were under the illusion that sufficient levels of credit enhancement and guarantees would

offset any deterioration in the portfolio. This created a perilous misalignment of incentives along the value chain<sup>2</sup>. The people reaping the rewards were not the ones bearing the risks. Asymmetric incentives led to operational failures stemming from mis-selling, fraud, and poor execution:

- Incentivized by volume targets or sales commissions, unscrupulous lenders sold subprime loans to customers who actually could have qualified for a prime mortgage<sup>3</sup>.
- Through incompetence or bad intent, brokers or subprime lenders failed to disclose the specific characteristics of the mortgage, especially for adjustable rate mortgages, which had low—but temporary—"honeymoon" rates.
- Brokers colluded with clients to exaggerate their incomes or lie about their employment records to allow them to qualify for loans<sup>4</sup>.
- Clients funded the deposit for a loan by going to another lender—the silent second. This arrangement, which was

<sup>2</sup> This is more relevant in the US where the transaction undertaken by the broker may be limited to a sales job; advising the borrower to choose an appropriate lender and collecting the commission for the sale. It is less relevant in UK where brokers are held financially liable if the advice is later shown to be defective. In the rest of Europe, few use retail brokers.

<sup>3</sup> In 2006, The Wall Street Journal reported that 61 percent of borrowers who received subprime loans had credit scores that were high

<sup>4</sup> An FBI investigation in 2005 found rampant fraud in stated employment histories and claimed income on mortgage applications.

- not disclosed to the first lender, reduced the collateral value of the house<sup>5</sup>.
- Even before the loan was granted, there was another conflict of interest. In order to consummate the loan, the lender required an “independent” valuation of the property by an appraiser. Eager for follow-on business from the lender, the appraiser often worked towards justifying the value of the house, as already agreed by the lender and client.
  - The lack of end-to-end ownership of the loan process, coupled with various conflicts of interest, led to a relaxation of underwriting controls. It gave rise to low documentation loans (no verification of income or employment history).
  - Aggressive volume incentives encouraged underwriters to sell with little regard to the suitability of the loan for a given client or its performance beyond the near term. Managers made little effort to impose the few controls that were in place or to re-enforce the risk management structure. Conscientious underwriters were often pushed by their employer to approve questionable mortgage applications.

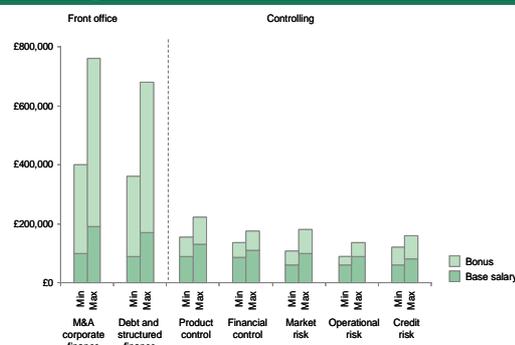
**Incentive Schemes in Capital Markets.** The financial crisis has once again underscored the dangers associated with excessive risk-taking by banks. It has also provided the impetus for revising compensation incentives, which influenced the risk-taking activities that led to the market disruptions. In his speech at the Global Association of Risk Management Professionals Annual Risk Convention, on February 25, 2008, Randall Kroszner, a member of the Board of Governors of the Federal Reserve, stressed the importance of providing managers and traders with the right incentives to ensure sound risk management. He noted that “Since the fortunes of even the most technically sophisticated financial institutions ultimately depend on the decisions and judgments of individual managers and traders, senior management must ensure that the right incentives are in place so that risk taking is appropriately captured in business-line

performance evaluation and employee compensation.”

Despite good intentions, banks and regulators have made moderate progress in dealing with the compensation issue<sup>6</sup>. Competition for talent is intense in the banking world, and the best talent is known to gravitate toward less restrictive, more lucrative environments. Moreover, the compensation issue is multifaceted, and involves a range of issues:

- Front office compensation packages are mostly based on short-term volume targets.
- Bonuses are paid in cash, shares and options, but star performers usually negotiate more cash upfront.
- Many compensation schemes have asymmetric rewards. Employees receive massive bonuses when earnings are high but suffer disproportionately less when losses occur. There are also massive differences in compensation for front office and controlling staff. (See **Exhibit 6.**)

Exhibit 6: There are vast differences in compensation between front office and controlling staff



If, indeed, compensation remains a difficult issue to address—even in the wake of an unprecedented crisis—then it becomes all the more important for financial institutions to develop a strong risk culture that relies on other types of levers (e.g. based on long term view, better sharing of the risks, change of behaviours, etc..).

<sup>5</sup> The proportion of silent second mortgages shot up from 6.8 percent in 2003 to 33 percent in 2006.

<sup>6</sup> The French Bankers Association (FBF) has published recently a set of recommendations on variable pay that banks will have to implement by 2010 while the UK government is currently working on a report on the management of banks and their remuneration schemes.

### *A Fragmented Control Environment*

The demands imposed by Sarbanes Oxley, Basel II, MiFID and a multitude of local regulations have led to a proliferation of controls. The imposition of too many controls has created a fragmented environment hampered by duplication, poor connectivity, unclear roles and responsibilities, and an inability to generate an integrated view of risk. It has also created a false sense of protection, which dampens risk awareness across the organization.

Many rogue-trading incidents can be traced back to weak risk controls rather than to the outright absence of such defences. Banks tend to focus more on the quantity—rather than the quality—of risk controls. Consequently, they end up with a complex and costly control architecture that is sufficient for day-to-day issues but vulnerable to extreme stress. Often, the failure to adequately apply controls stems from systemic issues, including IT security, IT outages, or intimidation of back-office staff by traders. Other contributing factors include a lack of formalization, accountability, and governance structures for key control activities.

The crisis has placed enormous pressure on these flaws, turning small cracks into major fissures. The problems became critical in banks that were deploying and integrating highly sophisticated business processes, organizational structures, and technology infrastructure, or were experiencing record volumes of trading activity.

Further problems have come from the normalization of the deviance of controls. This concept, which has been described by Diane Vaughan, is characterized by the fact that insiders, when repeatedly faced with evidence that something is wrong, normalized the deviance so that it became acceptable to them. In many cases of fraud or execution-related losses, managers and controlling functions decided not to act even though that had ample warning and clear indications that something was wrong.

In an environment characterized by a strong risk appetite, it is easy to imagine how investment banks would tolerate small deviations from the norm. But this is a slippery slope. A bank can become gradually tolerant of increasingly large (and dangerous) deviations from the norm. Only a strong risk culture and a healthy sense of

scepticism can effectively address this phenomenon.

### *Impact of Back and Middle Office Staffing and Regulatory Pressure*

Regulatory pressure and staffing levels play decisive roles in operational risk management. Increased regulatory focus helps reduce confirmation backlogs, but backlogs can rise if a bank reduces the number of back and middle office staff (which it often does in conjunction with an effort to automate processes, but staffing levels are sometimes reduced before automation is operating at full capacity).

**Regulatory Pressure.** The industry will focus on areas where regulatory pressure is highest. This includes market segments with complex products that would otherwise be considered too difficult to automate or standardize.

The surge in CDS volume in the second half of 2007 raised backlogs to 6.6 days and set regulatory alarm bells ringing once again. Further regulatory pressure will ensure that more progress will be made in this area to keep operational risk at bay.

Equity derivatives backlogs, at 13.3 days, were the highest among all OTC products in 2007. They have become the new focus of regulatory pressure. The operational risk associated with this product was partially mitigated by flat trading volumes in 2008, but much work needs to be done to increase automation. At the end of 2007, only 23 percent of equity derivatives had an automatic confirmation match on DTCC's Deriv Serv, compared to 62 percent for credit derivatives. Replicating the success in automating CDSs for equity derivatives may prove challenging. The CDS market is highly concentrated among a handful of dealers who trade frequently, which facilitates investments in sophisticated trade-processing systems. By contrast, one-third of equity derivatives deals are spread across 55 dealers, while the other two-thirds are dispersed over many counterparties. Equity derivatives will be the most threatening source of operational risk if the industry fails to standardize and move clients to automated platforms.

The problem with equity derivatives underscores the fact that reducing confirmation backlogs will require action on the part of all OTC market participants. This is the only way to ensure

standardization and to bring more trades onto electronic platforms. New regulatory guidelines are aimed at building an OTC industry infrastructure that is as reliable as those for mature markets such as exchange traded futures and options. These guidelines include:

- Increased standardization and use of FpML (financial products mark-up language), which is a standard for electronic communications of financial derivatives.
  - Increased automation and use of electronic confirmation and affirmation platforms such as DTCC for more OTC products. These central information depositories (CID) also allow multilateral netting and can link into other electronic systems that manage trade lifecycle events such as payments and settlements. CIDs stop short of functioning as a central counterparty.
  - Use of multilateral terminations that replace original positions among counterparties with a reduced set of bilateral contracts that represent the same net exposure but significantly lower gross exposure, thus reducing counterparty risk. The Trioptima service for CDS tear-ups shaved 11 percent of the growth of CDS outstanding volume in the first half of 2007.
  - Establishment of a central counterparty clearinghouse coupled with an exchange for OTC derivatives. The Federal Reserve Bank of NY is exploring possibilities in this area.
- *Currency Derivatives.* These are standardized OTC products characterized by frequent trading and a high level of automation. Automation has kept up with the spectacular growth in currency derivative trading volumes, resulting in a reduced backlog of confirmations. The volume spike in 2006 and the tightening of operations in 2007 have not hindered the fall in confirmation backlogs, which declined to 2.3 days. As a result, the processing of currency derivatives accounts for a small amount of operational risk in most banks.
  - *Interest Rate Derivatives.* Interest rate derivatives consist mainly of plain vanilla FRAs, vanilla swaps, and standardized interest-rate options. The share of complex non-vanilla swaps increased from 12 percent in 2003 to 19 percent in 2007—a small increase compared to rise of complex products for CDS and equity derivatives. In addition, central counterparties (CCP) such as Swap clear provide clearing services for certain types of interest rate derivatives, taking over 40 percent of interdealer positions in these products. Nonetheless, we did not find a significant reduction in confirmation backlogs from 2002 to 2007. The average backlog over this period was 9 days, and backlogs actually increased in 2006, to 10.7 days.
  - Changes in back and middle office staffing may have played a role in the recent increase in backlogs. While volumes picked up slowly between 2002 and 2004, automation levels increased significantly. At the same time, however, the ratio of back office staff to front office staff declined from 1.30 in 2002 to 0.70 in 2007, perhaps as a result of automation.
  - *Commodity Contracts.* These are less standardized than most interest rate options, yet they have been automated at a faster pace. The spike in 2005 appeared to mark the end of a volatile period, with volumes going up and down and backlogs following a similar pattern. Strong improvements in automation and high levels of back and middle office staffing led to a reduction

In the coming months, regulators will have to be much more active in setting standards for OTC markets.

**Back and Middle Office Staffing.** Automation has been instrumental to the reduction of confirmation backlogs, but its absence or underdevelopment cannot fully explain the backlog spikes that occurred for commodities and equities in 2005, interest rates in 2006, and credit derivatives last year. The data in Exhibit 6 suggest that spikes in backlogs are due to a combination of the level of automation, the share of complex products, and the level of back and middle office staffing when volumes rise. The interplay between these factors has led to different outcomes across a range of products:

backlogs from 2005 to 2007, even as volumes increased.

- *Credit derivatives.* Credit derivatives have seen major improvements since their massive confirmation backlogs—21 days in 2002—triggered regulatory action. The remedy included increased back and middle office staffing, a drive for standardization of many CDS contracts, a new novation protocol, and a push for further automation thanks to the establishment of the Depository Trust & Clearing Corp's (DTCC) Deriv-Serv, which is an electronic confirmation and affirmation platform for OTC participants. Backlogs plummeted to 4.9 days in 2006, despite enormous volume growth.

## Operational Risk Management: A Need for Radical Change

Operational risk management is a relatively new discipline. It emerged at the end of the 1990s, when the Basel Committee decided to integrate operational risk into its measurement of regulatory capital. But it has been around long enough for us to draw important lessons from what does and does not work, and to develop a fresh perspective on the best approach.

### *The Limitations of Operational Risk Frameworks*

Most banks have designed their operational risk frameworks to meet a range of objectives. Their first priority was to reinforce their control framework and establish operational risk processes that comply with regulatory regimes, such as Sarbanes-Oxley 404 reporting requirements. Their other priorities were to:

- Track operational risk losses and events.
- Develop metrics and standards for assessing operational risks.
- Determine mitigation strategies to reduce operational risks.
- Measure the economic/regulatory capital that is due to operational risk.

Banks want their operational risk frameworks to do more than comply with regulations. They want them to protect their reputations, minimize the cost of capital due to operational risks, protect their enterprises against adverse events, and reduce their operational losses.

Although many banks have established operational risk frameworks that satisfy many of these goals, these frameworks have proven their limited ability to:

- *Detect areas at risks.* Current metrics and risk measures are backward-looking. They are not designed to detect emerging threats. Banks need to link different types of information and knowledge in order to convert weak signals into strong ones. With many risk departments fragmented and silo-based, such links could significantly improve a bank's ability to manage risk.
- *Develop an effective management framework.* A bank's framework of controls is often a patchwork of different regulatory requirements, and may therefore be both incoherent and incomplete. In addition, regulators and auditors have pushed banks to establish multiple lines of defence to better control risk. This model, unfortunately, has created a lack of accountability. An integrated framework of controls would make it easier to detect a pattern of suspicious behaviour and would replace the false sense of protection with a clear perspective of the bank's ability to detect and manage risk.
- *Spread a risk culture and ensure clear accountability for risks.* Some banks compensate for deficiencies in the risk framework by instilling a culture of risk awareness. In many cases, however, a results-oriented culture simply outpaces a bank's capacity to monitor and control risk. It is imperative that banks extend the practice of managing risk well beyond rigid standards and processes. It has to permeate the culture in the same way that a results-oriented mindset might drive a bank's priorities.
- *Enforce structural changes to reduce operational risk.* Banks tend to focus on the superficial symptoms of operational risk, rather than identifying and addressing the root causes. To mitigate operational risk, banks need to take a much deeper look at structural changes—for example, improvements to processes or infrastructure.

### *Five Factors that Undermine Operational Risk Frameworks*

There are five main reasons why operational risk frameworks have struggled to meet their objectives:

- An overemphasis on measurement at the expense of detection
- A false sense of protection stemming from an abundance of controls
- The lack of a risk culture
- Inadequate integration with the business
- Limited mandate and low profile

**An overemphasis on measurement at the expense of detection.** The mantra of risk management remains the same: “If you can’t measure it, you can’t manage it.” Much analytical creativity and energy goes into trying to invent complex risk metrics, such as OpVaR, in order to estimate operational risk.

By forcing banks to calculate the regulatory capital due to operational risk, however, regulators have distracted banks from their real mission: to protect their infrastructure, people, and businesses by *anticipating* potentially adverse events—detecting the problem is more important than measuring it after the fact. Moreover, the “measurement mentality” misses the fact that people are remarkably well-equipped to judge complex things—most operational risk failures are the result of a series of failures—and can form a more accurate picture of what is going on by looking, talking, and interacting.

Although banks have recently developed mechanisms for detecting specific risks, mainly around anti-money laundering, these approaches have not been extended to other types of operational risks. They are relatively expensive to implement and operate, requiring a massive amount of data and people. Banks need a pragmatic approach to detection—one that requires less data, generates simpler output, and integrates more judgment and human expertise into the analysis.

**A false sense of protection stemming from an abundance of controls.** The amount of controls imposed on banks has increased significantly, creating a false sense of protection. A great deal of operational risk management activity focuses on routine system errors and malfunctions. It is as if the industry, faced with the task of inventing a

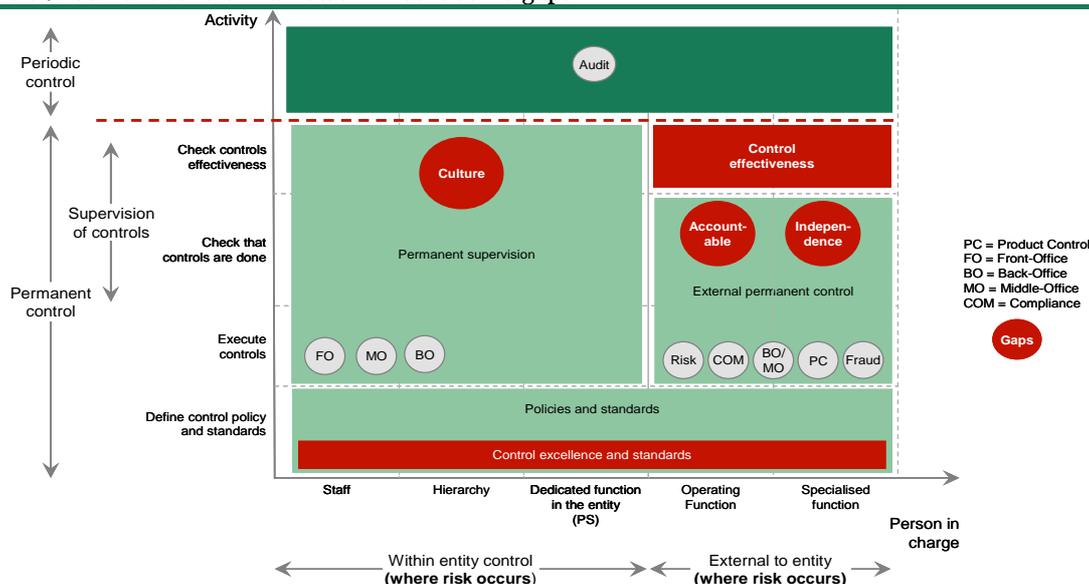
new risk management practice, has chosen to collect data that is accessible but not necessarily relevant. The burden of managing unknowable risks—risks that can trigger systemic failure or massive losses—has been passed over. Banks are focusing instead on risks that can be more easily measured and reported.

It is important to note that banks have little room to manoeuvre, given the number of requirements imposed by regulators and auditors. Recent events, however, provide a unique opportunity for banks to transform the model into one that is more realistic and does not aim to control everything.

The abundance of controls also masks gaps in the control framework. In most institutions, the control framework consists of two levels: permanent controls and periodic controls (See **Exhibit 7.**)

- *Permanent controls* comprise permanent supervision, which is done by the front line, and an external permanent control, which is performed by middle-office, risk and compliance functions. Permanent supervision consists of: internal day-to-day controls embedded in processes; controls imposed by managers on their own team; and controls imposed by a dedicated team within the entity—for example, within the COO function—which ensures that all expected controls are done properly.
- External permanent control can include: middle-office controls for front-office operations; risk-function controls related to market, credit and operational risk; compliance-function controls related to market abuse, KYC, and insider trading; finance-function controls on P&L attribution and integrity; and IT controls on information security.
- *Periodic controls* are mainly performed by internal and external audit functions as well as regulators. Their focus is to ensure the effectiveness of the controls in place and their compliance with regulatory requirements and control plans. Their actions are coordinated to ensure maximum coverage and depth of their controls.

Exhibit 7: Current control framework masks some gaps



This framework is not effective for a number of reasons. First and foremost, it is not clear who is in charge of what. Unclear accountability means that some responsibilities are overlooked or neglected. A fragmented control environment also precludes an integrated view of risks. These frameworks generally have a number of other shortcomings, as well:

- There is no one charged with reviewing the coverage, effectiveness, and efficiency of the controls on a frequent basis.
- People in charge of controls often lack the right incentives, the proper empowerment, and adequate profile within the organization.
- There are no tools that connect and analyze operational risk and compliance-related information.

**The lack of a risk culture.** There is a clear need to formalize roles and responsibilities to eliminate duplication and reinforce a strong sense of accountability. In addition, banks should develop and nurture a risk-aware philosophy across the organization. A risk culture would have a permanency that even the most solid processes and rules lack. Without a broad-based recognition of the importance of operational risk, a bank's best efforts to craft a sound framework for managing operational risk could be undone.

**Inadequate integration with the business.** The operational risk function needs to play a role in maintaining and improving a bank's competitive standing. To this end, the operational risk function should develop a new value proposition based on the following business-oriented goals:

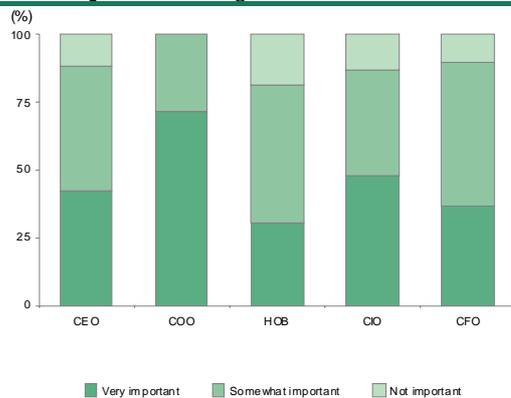
- Provide greater transparency on operational risks and support businesses in managing them. Operational risk data could be combined with other types of data to identify new insights for the business. Specifically, any combination of operational risk, operational effectiveness, and cost-related data will help the business understand trade-offs and take appropriate decisions.
- Optimize cost management by shedding light on the trade-offs among risk tolerance, revenue opportunities, and cost to the business.
- Enable growth by providing tools, methodologies, and competencies to the business in order to highlight and manage areas at risk.

More generally, the operational risk function can play an important, business-oriented role by providing better information about operational risk failures and losses, along with remediation measures and investments. It can also grade operational risks for specific processes and business lines, to optimize pricing and resource

allocation, and can assess the robustness of the bank's overall operating model.

**Limited mandate and low profile.** Operational risk management is often not recognized as a critical activity within banks. Market and credit risk management have historically had a much bigger role and attracted the attention of top management. The value and impact of operational risk management is not well understood.

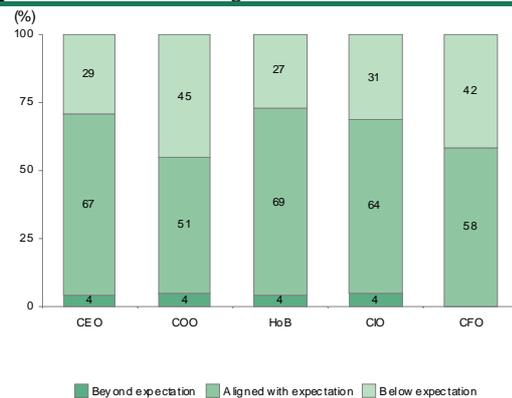
**Exhibit 8: Operational risk management lacks sufficient profile among heads of business**



Source: BCG OpsRisk survey 2008

A recent BCG survey found that operational risk management has yet to gain widespread acceptance as an essential component of the business. (See Exhibit 8.) The survey covered 60 banks from around the world; the mix of participants included retail, wholesale, and universal banks. About 70 percent of COOs viewed operational risk management as "very important," compared with only 30 percent of heads of business. This is particularly concerning, since business units have primary responsibility for managing operational risk on a day-to-day basis. Their support is essential to establishing a risk culture that permeates the bank and is effective at identifying, assessing, and managing operational risk.

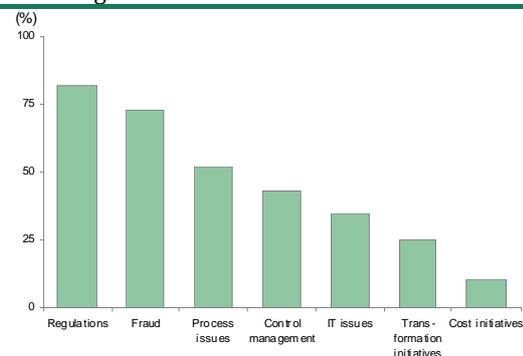
**Exhibit 9: COOs tend to be less satisfied with operational risk management**



Source: BCG OpsRisk survey 2008

Interestingly, about 70 percent of CEOs and heads of business said that operational risk management is aligned with or exceeds their expectations. (See Exhibit 9.) This result may owe more to low expectations or a narrowly defined view of operational risk, rather than to banks' actual capabilities for managing operational risk. In fact, the survey found that regulatory compliance and fraud are seen as the top priorities for operational risk management. (See Exhibit 10.) Few senior managers see operational risk management playing a role in transformation and cost initiatives. It is likely that senior managers view money spent on operational risk management as the cost of regulatory compliance, rather than an investment in a value-adding function that could help reduce costs, improve processes, or ensure the bank's survival.

**Exhibit 10: Regulatory compliance and fraud are seen as top priorities for operational risk management**



Source: BCG OpsRisk survey 2008

The narrow view of operational risk management is reflected in the resources allocated to this area. In a survey by *OpRisk & Compliance* magazine,

more than 50 percent of respondents said that their firms spent less than \$1 million on operational risk matters. This is a fraction of the money spent on market and credit risk. The bulk of this money is usually spent on increased reporting, staff, and training. Consequently, operational risk teams are small—they often have, at most, five people. With an extensive regulatory mandate and limited resources, it is no wonder that operational risk management has failed to make a more valuable—and visible—contribution to the business. To enable operational risk management to make an impact beyond regulatory compliance, banks will need to give this function greater resources and a higher profile. Operational risk executives should have the same stature as market and credit risk executives.

### Call to Action: A New Paradigm for Operational Risk Management

We have identified five guidelines for developing a more effective, business-oriented framework for operational risk management:

- **Fewer controls can be better—quality, not quantity, is what matters most.** The creation of a “control of controls” function will eliminate duplication and ensure the effectiveness of controls.
- **Be proactive, not reactive—focus on detection not on measurement.** It is important to detect problems before they spin out of control. New methods of detection are required to amplify weak signals into strong ones. Performing “real-life” stress test on your operations (process, IT, people) on a continuous basis will reveal vulnerabilities embedded in operations. Implementing and monitoring limits on operations will help prevent crises that might otherwise arise due to lack of capacity or aggressive innovation.
- **Integrate, don’t segregate—re-organise operational risk management.** Operational risk management activities should be organized by activities, not labels. This will help create an integrated operations information infrastructure.
- **Make individuals responsible—eliminate the duplication of responsibilities.** Operational risk management is often encumbered by a lack of clarity about the roles and responsibilities associated with functions such as the Control Department, Middle Office, Compliance, and Legal.
- **Support the business—assist the bank to optimize their resources sustainable.** The operational risk manager needs to become a credible partner to the business and a driving force to ensure the proper level of automation, effectiveness, resilience, agility, and efficiency of the operations.

#### *Fewer Controls Can Be Better*

The proliferation of control structures has resulted in considerable inefficiencies. Multiple audits are not uncommon. A department in one bank was audited seven times in one year: once for SOX, once by the control division, once by the compliance division, twice by internal audit, once by an external audit, and once by the regulators. All of these audits were focused on the same types of controls, and the objectives of each audit varied only slightly.

*Create a new function to control the controls.* The role of a “control of controls” function is to frequently review the effectiveness and the efficiency of controls. It should also ensure that the controls in place actually matter. Among other things, the function should:

- Assess the quality of controls, conduct in-house stress tests on controls, and enforce a plan for optimizing current controls, creating new ones, or even suppressing non-necessary ones.
- Implement a structured process for identifying over-controlled areas and optimizing both the number and cost of controls in a given business area.
- Set up and maintain a repository of all controls and procedures; collect and store all processes, procedures and control plans and any useful data (for example, dashboards, statistics, audit reports); and ensure transversal consistency of controls across the front, middle, and back office and any other support functions.
- Foster awareness of operational risk — and fraud in particular — and conduct training.

- Collect and share best practices among activities; identify the main weaknesses in processes and launch appropriate on-the-ground deep-dives; and check that control plans are updated to reflect process evolution.
- Act as the main interface with auditors and external regulators on control-related issues.

*Improve the competence of the team.* The ability of the new function to challenge the status quo and provide sound recommendations will be commensurate with its level of expertise and the seniority of its team. The right mix of resources has to be found and should include people who have the requisite business expertise and the courage to confront individuals if necessary. Its position in the organization should also ensure its full independence and empowerment.

#### *Be Proactive, Not Reactive*

Most controls are reactive—that is, they identify symptoms as they emerge. In the long run, however, it would be more effective to have controls that are preventative, which would allow the business to head off specific risks. Instead of simply providing information about operational losses, the risk function should develop capabilities for detecting patterns and anticipating extreme events.

*Set up a Risk Detection Team to convert weak signals into strong ones.* Banks should create a new function that is dedicated to detecting risks and developing immediate responses. This approach is already being followed for anti-money laundering activities. It should be extended to fraud risk, execution risk, IT risk, legal risk, regulatory risk, and damage to physical assets. The Risk Detection Team would be tasked with converting weak signals into strong indicators about particular events.

Large operational failures, such as rogue trading events, are often preceded by a series of warning signs. In most cases, however, these signs were too weak to attract the attention of risk teams. In the case of a rogue trading event, the signs might include dubious explanations from a trader about a particular event, a transaction that has been cancelled, the lack of vacations over an extended period, or a radical change of P&L that cannot be explained clearly. The signs might be small deviations from the norm, and are therefore not

considered serious. These signals can be difficult to interpret for several other reasons:

- The proliferation of controls, alerts, and risk-related information creates too much noise. The problem stems not from a lack of information, but from an overabundance of information.
- The signals can come from multiple directions. They are likely to emerge from fragmented functions and silo-based systems. There is no coherent picture of the signals, as a whole.
- The signals are volatile. Because the signals can change frequently, it is easy for their value (their meaning) to be diminished.

This leads to the problem defined by Yves Morieux<sup>7</sup> as the weak-signal syndrome, which is characterized by declining signal-to-noise ratios—the amount of ambient noise makes it almost impossible to hear the signals. To overcome this problem, Yves Morieux suggests using two mathematical relationships: one concerns signal detection and interpretation and the other concerns signal transmission:

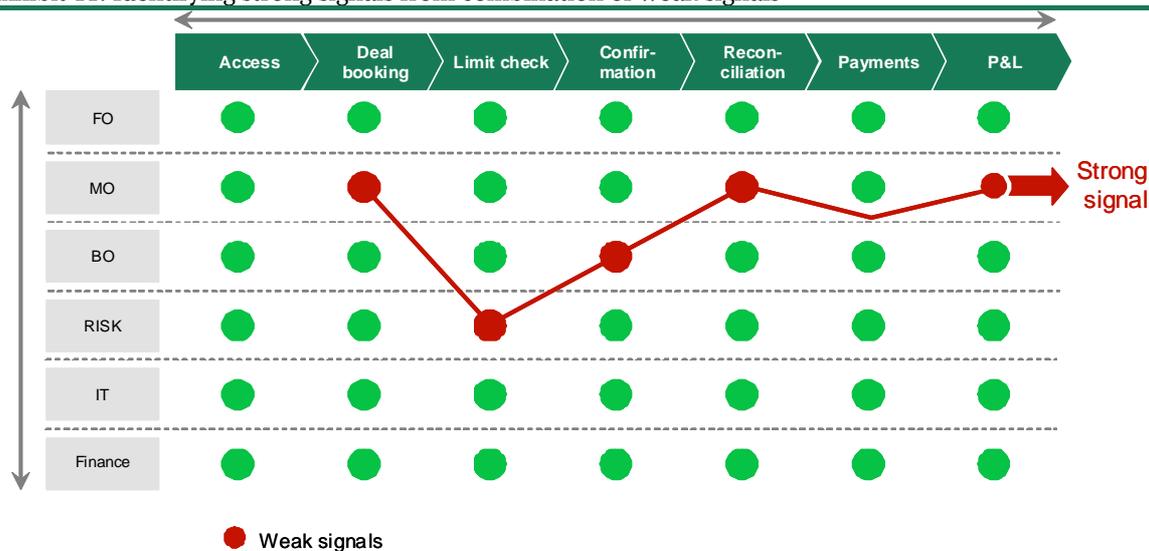
To enhance signal detection and interpretation, banks need to triangulate information between independent sources (**See Exhibit 11.**).

By improving the connectivity of information related to operational risk, the bank will greatly improve its ability to detect operational failures. To this end, the banks should set up a centralized team whose mission is to aggregate all of the signals, build an integrated view of different types of alerts (ones that already exist in the organization), and transform different weak signals into concrete alerts. Once identified, alerts would be analyzed and eventually escalated to top management. The team would be responsible for ensuring that the proper actions are taken.

<sup>7</sup> “Restructuring Strategy: New Networks and Industry Challenges”, *Generative Interactions*:

*The New Source of Competitive Advantage*, Yves Morieux, Mark Blaxill, and Vladislav Boutenko; 2005. Yves Morieux is a Senior Partner at BCG Paris.

Exhibit 11: Identifying strong signals from combination of weak signals



*Set up an Extreme Stress Team.* Being proactive also means anticipating the worst. Banks should create an Extreme Stress Team that focuses on developing scenarios that can have a material impact on operations (and the business) and conducting exercises to test the bank's operational risk capabilities.. This is comparable to a hacker employed to test IT security. Similarly, this team will be charged with testing specific processes.

The effectiveness of the team would depend on its ability to understand the most critical operational risks and to leverage information produced by other parts of the organization, such as Compliance or Internal Audit. Its tests might include:

- Inputting fake deals into front office systems and analyzing how long it takes for the deals to be detected.
- Artificially increasing transaction volumes to understand the capacity limits of the operating model.
- Breaking into confidential information within a core system.
- Simulating system performance issues and assessing the resiliency of processes.
- Identifying a series of events that could trigger a large loss.

#### *Integrate, Don't Segregate*

The segregation of operational risk activities leads to two main problems. First, people are not incentivized to work together. As a result, the Compliance, OpRisk, Audit, and Control functions are not motivated to collaborate. This can lead to inefficiencies and lack of accountability, as each function tends to extend its scope. Second, information related to operational risk—including fraud alerts, IT alerts, and operational loss information—is not shared, much less pieced together. This increases the cost of data collection. More important, it limits the capacity to build a data infrastructure capable of “connecting the dots” and yielding insights into the state of operations, including the effectiveness and resilience of certain processes.

Exhibit 12: Separation of operational risk and control activities across many different departments

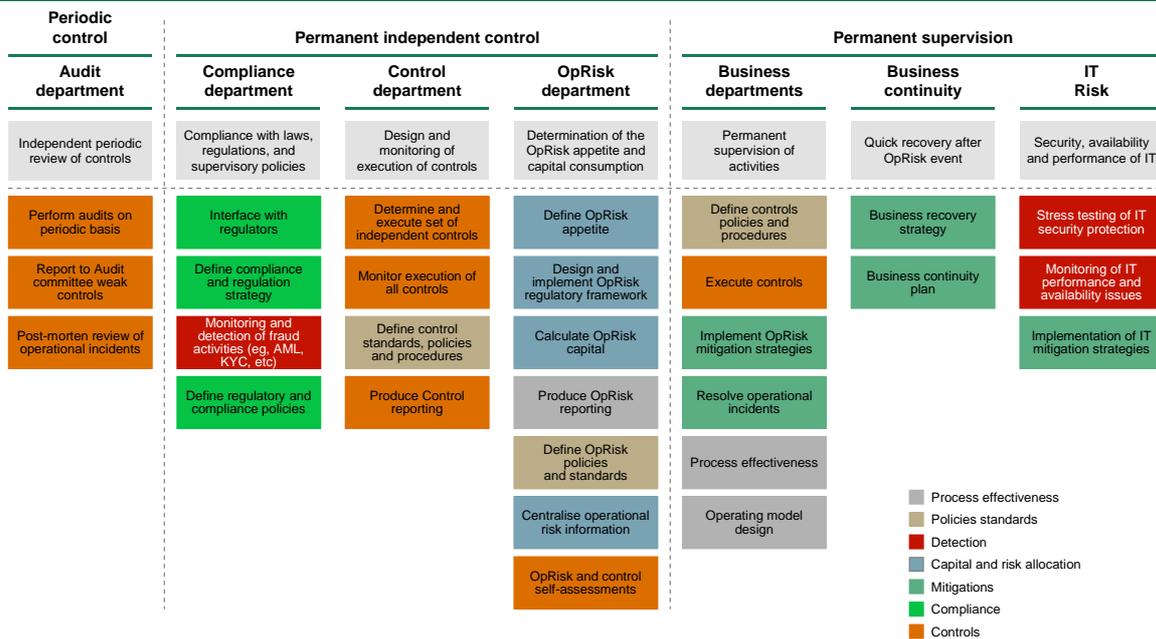
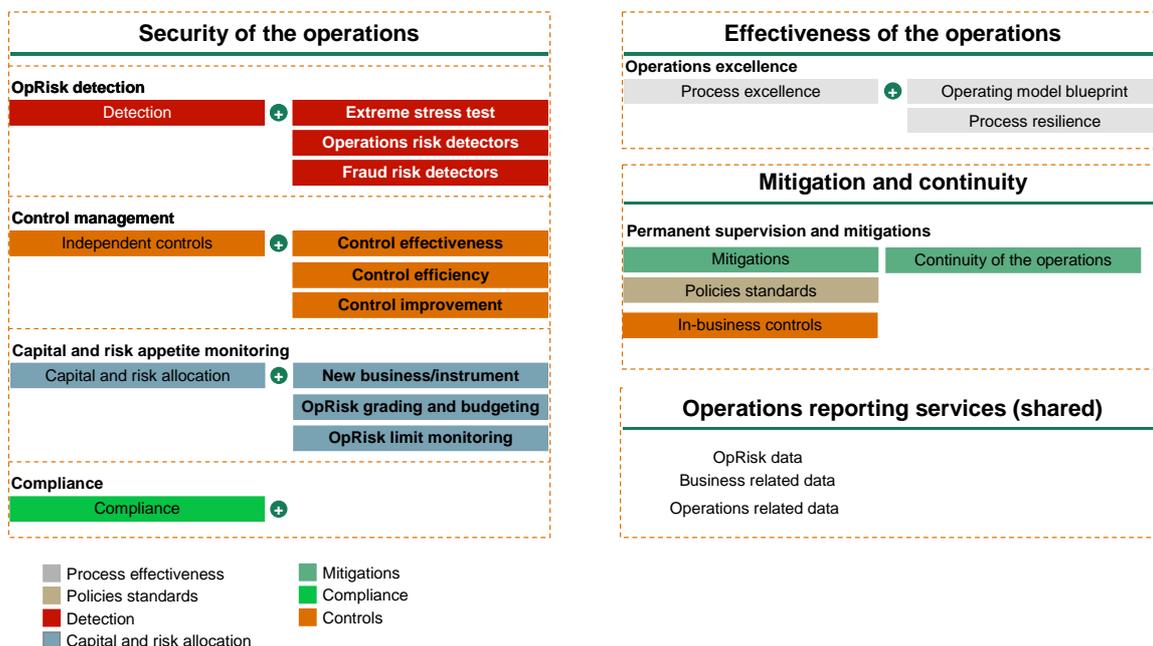


Exhibit 13: Integration of operational risk and control activities



Banks should therefore integrate operational risk management at both an organization and an information level. At the organization level, banks should:

- Clarify the role of the centralized function. The centralized function should have three main roles: ensure the overall effectiveness of the controls; detect operational risks and

- monitor weak signals; and stress-test controls, systems, and processes.
- *Deploy local OpRisk managers in the organization.* To better understand the complexity of each business line and function, the centralized function needs to be supported by local operational risk managers. Their focus will be to identify any abnormal behaviour not captured by the central team; to work with the central unit as it investigates incidents; and to identify new types of fraud as the business evolves.
- *Regroup activities by logic rather than labels.* Activities relating to operational risk are often spread across different departments such as OpRisk, Compliance, Audit, and Control (See **Exhibit 12.**). There are obviously many ways to regroup these activities. We propose to group them into three categories (See **Exhibit 13.**):
  - Activities that relate to the security of the operations.
  - Activities that relate to the design and implementation of effective processes and an effective operating model.
  - Activities that relate to the permanent supervision of risks by the business and the implementation of the remediation strategies (which include the business continuity).

*Create an integrated operations and risk information infrastructure.* To integrate operational risk management at an information level, banks should combine operational risk information with business information to provide meaningful insight to the decision-maker. Identifying operational losses will help identify areas at risk, but this is of limited help when making business decisions about risk-mitigation strategies, investments in new capabilities, or the potential impact of risk on other business activities.

Operational risk information that is isolated from its business context is of little value. The operational risk function should aim to deliver business-oriented, standardized risk information and analysis. This will lead to a range of benefits for the business:

- Provide the businesses with a holistic view of operational risk.
- Identify and address the root causes of operational risks, and thus enable

organization-wide operations management.

- Identify the right trade-offs in terms of risk tolerance, opportunities to the business, and the cost of mitigation.
- Develop a new mindset and culture, where decisions weigh the dimensions of both risk and reward.

### *Make Individuals Responsible*

In most banks, operational risk is managed through multiple committees and functions, making it difficult to identify who is accountable for the long-term remediation of a specific risk. The operational risk framework should ensure accountability along the operational risk chain. More important, banks should instil a risk culture, where everyone feels responsible for the safety of the bank. This is vastly better than multiple responsibilities and committees. Several principles could help cultivate such a culture:

- Recognize the importance of judgement in assessing operational risk.
- Be able to challenge the business whenever necessary (the operational risk function must therefore have people with the experience and confidence to challenge the business).
- Ensure that people transition between business and risk roles.
- Implement the right incentive schemes across the organization to support a risk-aware culture.
- Design a governance model that reinforces the role of the operational risk function.

These last two principles are critical. An operational risk function without proper authority is likely to fail. Such authority cannot be imposed on the organization. Rather, it must be earned through the development of strong capabilities and expertise that extend beyond operational risk measurement. This is a prerequisite for being considered “equal” with the business and is precisely why the operational risk function should focus on recruiting and developing high-profile, senior talent. Only after this function is seen as strong and decisive can it assume a more business-oriented, advisory role.

It should not be a surprised to see that the best performers in this dimension have established stronger counter-power to the Front Offices. In these cases, successful career tracks often integrate management of Back Office and risk functions to access top management.

Ensuring that remuneration structure of banks is consistent with sound risk management is another priority. In many cases, banking firms gave staff incentives to pursue "risky policies" that undermined the impact of risk-control systems.

Even if any material improvements will only happen in 2010 and beyond – as many banks have already set in place the following year's remuneration contracts – banks need to show they are moving to change bad practices.

New compensation model should take into account long term value creation, sustainability, level of risk taken and compliance to business ethics.

One example of a European financial services firm taking a proactive approach is UBS, which in November 2008 announced a new compensation model by which up to a third of the annual variable cash component of compensation will be paid at year-end subject to 'positive business development', while the larger portion will be held in an escrow account. The overall amount will be reduced 'if regulations are grossly violated, if unnecessary high risks are undertaken or if individual performance targets are not met'. UBS's variable equity programme will only vest shares after three years and oblige top managers to hold onto these for longer.

However, changing compensation scheme is not enough and it is also critical to enforce "longer term" oriented behaviours at all levels. Here the main objective is to change the mindset and attitude of the people towards risks. This can only be achieved by understanding and, if necessary changing the key drivers of behaviours (e.g. goals, resources, constraints) and aligning them with the overall risk appetite of the firm.

### *Support the Business*

The operational risk function should take steps to ensure the bank is pursuing a sustainable level of growth. It should position itself

differently by developing a new set of capabilities that are focused on improving the effectiveness and resilience of the processes. The function can, for example:

- Support business planning by highlighting capacity constraints, thus allowing management to take timely action.
- Establish and monitor operational risk limits. Those operational limits can be based on current capacity constraints and the risk appetite of the bank.
- Gauge the operational risks of a given operating model and its key design principles.
- Clarifying the critical trade-offs that need to be considered during the transformation of operating models or critical processes. The objective is to ensure that decisions are being taken with a full understanding of the consequences in terms of their impact on cost, profitability, agility, resilience, risk, effectiveness, and automation.
- Contribute to operational excellence and industrialisation of the bank by enabling the business to test the resilience of the processes and helping to design processes from an operational risk point of view.
- Enable the comparison of areas/franchises from an operational risk perspective and provide a basis for effective operational-risk capital management.
- Provide insight to the firm from the combination of operational risk and business related information. Operational risk information that is isolated from its business context is of little value. Therefore the objective is to deliver business oriented, standardized operational risk information and analysis linked to value.
- Before the bank introduces new financial instruments, ensure that the right processes, people, and IT infrastructure are in place (or in construction). After the launch, ensure that the processes, people, and IT infrastructure are providing adequate support.
- Support the business by optimising the allocation of scarce resources. It

includes the allocation of capital that is due to operational risks and a better alignment of competencies and talent with critical activities (e.g. product control function).

- Develop simpler methods for measuring and allocating OpRisk capital that are both robust and easy to understand.

## Recent BCG papers in risk management:

---

This discussion paper is the fifth in a series following:

- "The Subprime crisis: Do Not Ignore the Risks" by Philippe Morel, Pierre Pourquery and Peter Neu (September 2007);
- "The Current Crisis: Is the Worst Behind Us?" by Philippe Morel and Pierre Pourquery (March 2008);
- "All dried up: The impact of the subprime crisis on liquidity risk management" by Peter Neu and Philippe Morel (May 2008);
- "New risk regime" by Philippe Morel, Peter Neu, Pierre Pourquery and Duncan Martin (November 2008)

The authors are grateful to Philippe Morel, Yves Morieux and Dan Coyne for their help.

### Authors:

Pierre Pourquery  
Partner, Risk Expert Team  
BCG London  
+44 207 753 5643  
[pourquery.pierre@bcg.com](mailto:pourquery.pierre@bcg.com)

Johan De Mulder  
Principal, Risk Expert Team  
BCG London  
+44 207 753 5353  
[demulder.johan@bcg.com](mailto:demulder.johan@bcg.com)