

OPERATIONAL RISK MANAGEMENT IN GLOBAL BANKING ORGANISATIONS – A LEGAL AND COMPLIANCE PERSPECTIVE

Robert L Tortoriello and Gregg L Rozansky, Cleary Gottlieb Steen & Hamilton LLP

Recent events – such as the ongoing credit crisis and high-profile episodes of rogue trading – have drawn increased attention to the operational risk-management practices of global banking institutions. For many regulators, banks and industry groups, these developments have underscored the importance for global banking organisations to have effective internal control and operational risk-management mechanisms, including in the legal and compliance context. Increased regulatory focus also reflects the implications of explicit capital charges for operational risk and the “Pillar 2” principle of supervisory review deriving from Basel II – the updated international capital accord being implemented in many countries around the world.

“Operational risk” has generally been defined as the risk of unexpected, direct or indirect loss resulting from inadequate or failed internal processes, people or systems, or from external events. The definition includes legal risk (ie, the risk of loss resulting from failure to comply with laws, ethical standards and contractual obligations). It also includes the exposure to litigation from an institution’s activities. Accordingly, the legal and compliance functions within an institution play a critical role in an institution’s operational risk-management efforts.

The contribution of an effective legal and compliance programme (ie, one instrumental in the creation of a firm’s values, educating personnel on legal and compliance-related responsibilities, evaluating business practices, and tailoring “best practice” models) are wide ranging. These include:

- a reduction of reputational and legal-compliance risks;
- greater confidence and trust placed in the institution – among clients, creditors and other stakeholders; and
- potential reduction in capital costs (especially for those globally active institutions that are or will be subject to the Basel II international capital regime), improved ratings and examination scores.

Recent events have clearly underscored the importance of maintaining effective legal and compliance-related controls and oversight in any economic or business climate – but especially during periods of financial stress, when pressures and challenges faced by legal and compliance personnel are likely to be heightened.

THE SENIOR SUPERVISORS GROUP STUDY

Huge losses at global banking institutions in the fall of 2007 prompted a group of senior financial supervisors from five countries to undertake a review of the risk practices of eleven of the largest banking and securities firms. In March 2008 this group of supervisors (the Senior Supervisors Group) issued a report, “Observations on Risk Management Practices During the Recent Market Turbulence”. Significantly, the report found that those institutions with the strongest risk-management practices have generally been best able to weather the credit crisis thus far.

The Senior Supervisors Group sought to identify examples of risk-management practices that have tended to be associated with better or weaker performance during the current market turmoil. According to the report, hallmarks of the risk-management practices of the better performing firms generally included the following.

Active oversight by members of senior management

According to the report, the timing and quality of information provided to senior management varied widely. For example, in some cases, hierarchical structures tended to delay or lead to the distortion of information sent up the management chain. In contrast, the more successful firms effectively eliminated “organisational layers” as events unfolded to provide senior managers with more direct means of communication and enhanced senior management understanding of emerging issues, as well as management’s ability to act on that understanding to mitigate excessive risks. Such firms

were more likely to detect and address inappropriate practices and weaknesses at an earlier stage.

A comprehensive approach to viewing exposures and risk sharing

Existence of organisational “silos” (ie, segregated and independent operational units) in the structures of some firms appeared to have an adverse impact on performance during the turmoil. At institutions that avoided significant losses, risk management had independence and authority but also considerable direct interaction with senior business managers and was not viewed as remote from the business. According to the report, senior managers at firms that experienced more significant unexpected losses frequently accepted a more segregated approach to internal communications about risk management.

The Senior Supervisors Group intend to use observations made in the report to assess potential future changes in supervisory requirements, guidance and expectations. Indeed, the report can be evaluated in the context of the explicit capital change for operational risk contemplated by Basel II, where it is clear that those institutions with robust and effective operational risk management will be required to set aside less regulatory capital than would otherwise be the case if they had weaker applicable policies, procedures and controls.

ROGUE TRADING AND OPERATIONAL RISK-MANAGEMENT PRACTICES

In early 2008, a trader at Société Générale made headlines around the world by carrying out allegedly unauthorised transactions leading to a loss of €4.9 billion on proprietary trading activities. In particular, the trader is said to have taken unauthorised positions on futures on European stock markets, offset by what turned out to be fictitious transactions (which disguised the increase in the size of the position and in Société Générale’s net risks). The trader in question appears to have been especially

well positioned to carry out unauthorised transactions because he had previously worked in the middle office units responsible for risk monitoring and control of trading and, therefore, had an understanding of control procedures. Less publicised incidents have also arisen in other institutions in terms of trading exposures and unusual market positions that exceeded internal limits or otherwise raised risk management, legal or compliance issues.

In the aftermath of these and other similar events, there has been general recognition of the need to develop new strategies to improve identification of fraudulent activities, strengthen internal supervisory methods and ensure full management involvement in risk monitoring. For example, many institutions have already put in place new trading limit alerts and other security controls (eg, segregation of front office staff from middle and back office functions) to protect against “rogue trader” risk and similar incidents.

In addition, there has been an increasing focus on the integration of ethics and compliance programmes. By design, the ethical elements of such programmes are intended to reinforce compliance elements and vice versa. Successfully implemented integrated programmes reflect an institution's commitment to integrity, honesty and legal compliance. These programmes frequently exhibit the following characteristics:

- coordination between the compliance and ethics specialists and individual business units;
- consistent implementation of the programme throughout the various business lines of the organisation;
- clear and effective division of roles and responsibilities among the ethics office, compliance, legal and other relevant units; and
- periodic evaluation by the board of directors and management of the effectiveness and design of the programme.

CHALLENGES THAT LIE AHEAD AND SUPERVISORY EXPECTATIONS

In view of recent events, bank and other financial institution regulators are likely to raise their expectations for operational risk-management programmes.

Corporate reporting systems, the documenting of appropriate policies and

procedures, and the training and advising of front-, middle- and back office personnel on risk-management requirements will continue to be critical components of satisfying supervisory and regulatory objectives and concerns. As a starting point, a financial institution should implement:

- “tone-at-the-top”, which recognises the importance of board and senior management oversight;
- a formal policy to address tolerance for legal, operational, compliance and reputational risks, including regular assessments of risk tolerance by senior management and procedures for escalating risk concerns to appropriate senior levels;
- consistency in risk definitions, policies, measurement, reporting, accountability and audit;
- written compliance programmes relating to legal, regulatory and supervisory requirements (laws and regulations with respect to banking, securities, commodities, real estate, insurance, etc);
- policies and procedures for satisfying applicable securities law requirements in terms of adequate public disclosure of applicable risks; and
- robust internal audit processes which focus on independence, planning, risk assessment, exception tracking and resolution.

Among the key areas focused on to build a “culture of compliance” are:

- attention from the board and senior management;
- employee training and self-assessments;
- policies to identify, measure, assess, monitor, test and minimise compliance, legal and reputational risk, backed by a well-resourced, independent compliance staff;
- policies governing the accumulation, retention, use and dissemination of data, including customer data;
- procedures for prompt redress of reporting problems;
- cooperation with regulators;
- closer integration of the governance, risk management and compliance functions; and
- limitations on outsourcing the compliance function.

Key current legal and compliance issues in

the context of US bank and bank holding company activities include those related to:

- Recognition of the principal areas which generate reputational risk, including those arising from participation in “complex structured finance transactions” driven by tax, accounting or regulatory avoidance motivations, or novel, complex or unusually profitable transactions that may raise “appropriateness” or “suitability” considerations insofar as marketing to, or selection of, counterparties is concerned; from transactions where the likelihood of customer confusion is enhanced (eg, sale of non-deposit investment products through a bank); from transactions that involve controversial public associations and political figures or dealing with unnamed counterparties; and large but non-controlling investments, especially in companies in high-risk economic (environmental, subprime, gaming, power, etc), political or geographic areas.
- Focus on identification and resolution of conflicts of interest that arise between the financial institution and its customers; among the financial institution's customers; and among different business units of the same financial institution. Conflicts of interest that arise from multiple relationships with a customer (eg, acting as an underwriter and as an adviser to the issuer, acting as market-maker, lender or derivatives counterparty, acting as adviser on M&A transactions coupled with the issuance of fairness opinions, holding positions in debt or equity securities, having a director representative on a client's board, etc) may require special attention so that potentially increased risk of equitable subordination, incurring fiduciary obligations, additional restrictions on information-sharing, etc, can be addressed.
- Restrictions on transactions with affiliates.
- Focus on compliance with equity investment limitations and on monitoring processes, documentation, approval and due diligence procedures.
- Identification and monitoring of key risk indicators with respect to derivative transactions and trading activities.
- Recognition of responsibilities with

- respect to participation in transactional activities as principal or agent, including standards of fair practice, and policies, procedures and controls to guard against manipulative behaviour.
- Evaluation of issues with respect to the identification and treatment of material non-public information in the context of loan, credit derivative and related markets, as well as in the context of “traditional” securities trading.
 - Review or evaluation of outsourcing contracts.
 - Focus on compliance with banking and securities law licensing and supervisory requirements in connection with international securities transactions and linkages.

- Evaluation of relationships between banks and broker-dealers with hedge funds, including in respect of space leasing, service arrangements, brokerage compensation, disclosures and treatment of hedge fund clients in comparison with other clients.
- Focus on compliance with anti-money laundering and economic sanction requirements, including in respect of suspicious activities report-tracking, monitoring and filing; implementation of adequate customer identification and know-your-customer procedures; trade finance; foreign correspondent account review; and diligence in respect of US and non-US shell companies and tax havens.

Huge losses suffered by major financial institutions over the past year have served as reminders of the need across the industry for stronger operational risk management and an improved understanding of effective operational risk-management techniques and the challenges faced by legal and compliance functions in managing operational risk.

Given how quickly inappropriate practices can lead to significant losses and reputational consequences, the legal and compliance function in financial institutions must be vigilant and active in assisting in the identification, monitoring and mitigation of operational risks. To this end, steps must be taken to assure compliance with all applicable legal requirements and policies in any economic or business climate.