Box 12

A REFLECTION ON RECENT DEVELOPMENTS IN THE OPERATIONAL RISK MANAGEMENT FRAMEWORKS IN THE BANKING INDUSTRY

Trading losses at UBS in September 2011 (estimated at around €2 billion) – with similarities to another loss at Société Générale in 2008 (€4.9 billion) – recall the events that led to the bankruptcy of Barings Bank more than fifteen years ago, after the fraudulent activities of one of its employees had resulted in a USD 1.3 billion loss. These recent events show that despite tighter regulation of the banking industry, the failures in operational risk management continue to represent a recurring problem. All three cases are classic large operational risk events that arose as a consequence of numerous control and governance failures. The distinguishing common feature in all these cases is a single rogue trader who manages to circumvent a series of internal controls and take advantage of weak governance to implement elaborate trading strategies resulting in losses, further exacerbated by adverse market movements. From a theoretical point

of view, the trading strategies in question did not involve a significant amount of risk *per se* as they were based on arbitrage, i.e. making bets on small price differences between related "plain vanilla" instruments: Asian stock index futures in Barings' case, European stock index futures at Société Générale and exchange-traded funds (ETFs) at UBS. Such strategies intend to capture micro-inefficiencies in market pricing that could be converted into low-risk profits with an overall low market risk exposure. The risk materialised, rather, from the traders' recurrent engagement in unauthorised activities, moving away from the authorised arbitrage strategy into directional bets with large risk exposures, the breach of risk limits and manipulation of trade data. In each case, the trader had not just control of the front-office functionalities, where trades were placed, but also in-depth knowledge of the middle and back-office systems for confirmation and settlement of trades that allowed the fraudulent activities to be concealed. Additional contributing factors arose from the lax governance framework, insufficient supervision, lack of appropriate control measures, and inadequate technology and procedures, coupled with senior management's complacency when profits resulted from the trading strategies. These facts highlight the importance of establishing an adequate operational risk management framework that goes beyond the mere implementation of regulatory directives and encompasses a deep understanding of the business model of the financial institution, its processes and procedures, as well as a sound implementation of governance and risk management policies.

As regards the development of the regulatory framework, several new aspects have come to the fore recently, in reaction to the marked increase in severity of operational risk events. In particular, it has been highlighted that the current framework fails to capture the fact that operational risk often arises in conjunction with other types of risk and that its size may be exacerbated by adverse market or credit risk events. In the cases described above, unauthorised activities were initiated with the objective of concealing trading losses due to adverse market price movements, and were further impacted by the increased market risk.[1] Hence, the development of an integrated risk management approach would be required so as to address the relationships between different risk categories. Moreover, although historically overshadowed by market and credit risk regulation,[2] operational risk capital modelling has also recently received significant attention from the supervisory authorities. In particular, modifications to the current operational risk capital calculation methods are being considered since, in light of the high severity of the recent operational risk events, the use of current multipliers under the standardised approach seems not to provide sufficient protection for the banks' actual operational risk exposure. To address this issue, in addition to the increases in the multipliers under the standardised approach, regulatory discussion is focusing on the creation of incentives to encourage banks to move towards more advanced measurement approaches (AMA). The obstacles to an effective AMA development stem from difficulties in estimating the loss distribution due to operational events, properly measuring the fatness and skewness of its tails, setting the appropriate confidence level and addressing the interrelations with market and credit risk.

Finally, a sound operational risk control framework should also focus on governance, providing robust policies and procedures to reduce the likelihood of operational risk events, and driving culture change to effectively implement these policies and procedures. In February 2003,

1 Similarly, events which include both credit and operational risk elements may also arise, e.g. if a trading counterparty defaults, and there is an operational error in securing adequate collateral, then the credit risk event is magnified by the operational risk event.

2 An initial report on "Operational Risk Management", which did not mention regulation, was published by the Basel Committee in September 1998. In the "New Capital Adequacy Framework" of June 1999 the Basel Committee called for capital charges for operational risk as a component of Pillar 1.

the Basel Committee provided an outline for the creation of an effective operational risk management framework by drawing up a list of sound operational risk principles.[3] Further improvement, based on the ongoing discussion among supervisory authorities and the banking industry, has been achieved recently by incorporating a full range of sound operational risk management principles covering governance, the risk management environment and the role of disclosure (see table).

The challenge remains as regards the incentives for banks to adopt these guidelines and their final interpretation. The recent events at UBS highlight the importance of applying effectively those principles not only to stem the effect of operational events in individual institutions,[4] but also to reduce the systemic implications of a large failure. After all, a one-in-a-hundred-year hurricane does not materialise necessarily only once every one hundred years.

Basel Committee's list of sound operational risk principles

1. The role of the board and senior management in the establishment of a strong risk management culture.
2. Development, implementation and maintenance of an operational risk management framework fully integrated in the bank's overall risk management processes.
3. The role of the board in the establishment, approval and review of the operational risk framework.
4. The role of the board in the approval and review of the bank's risk appetite.
5. The senior management's responsibility in the development, implementation and maintenance of a robust and transparent governance structure.
6. The senior management's responsibility for risk identification and assessment.
7. The senior management's responsibility for the full operational risk assessment for new products, activities, processes and systems.
8. The senior management's responsibility for risk monitoring and development of reporting mechanisms.
9. Development of strong risk control and mitigation strategies.
10. Development of business resiliency and continuity plans.
11. Role of public disclosure.

Source: Basel Committee on Banking Supervision, "Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches", June 2011.

3 Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk", February 2003.
4 UBS is currently using an internal operational risk capital methodology which meets the regulatory capital standard under the Basel II advanced measurement approach (AMA).