18 July 2008

Reactions to the Société Générale loss event: results of a stock-take

1. Introduction

In reaction to the recent "rogue trading" event which occurred at Société Générale (hereinafter SocGen) CEBS has conducted a stock-take with its member authorities on how this event affected other banks, their operational risk practices, governance and internal control environment, and the internal models used for calculating capital requirements for operational risk (Advanced Measurement Approaches, AMA).

The stock-take took the form of a survey in which supervisory authorities, guided by a number of questions, sought the views of banks in their jurisdictions. Banks were asked, first, to express their opinions on the types of controls relevant to preventing rogue trading and on whether events similar to the SocGen event would have been possible in their organisations; second, to outline possible or actual improvements to their operational risk frameworks and/or internal control systems as a result of the lessons learnt from this or other "rogue trading" events which have occurred in the recent years; and finally to explain how this loss event is included in their AMA modelling framework and the consequences, potential or actual, for their operational risk capital charge. The last part of the survey focused on the nature and type of supervisory reactions to this event.

It is worth mentioning that the banks' and supervisors' views on the SocGen event are predominantly based on publicly available information and reports at the time of the survey. The outcome of further investigations and discussion on the topic could provide additional and deeper insight that will be needed when deciding on the supervisory way forward.

2. Executive summary

The results of the stock-take are fully consistent with the outcome of reports on the topic recently issued by some supervisory authorities (see the reports of the French Commission Bancaire and the UK FSA). In particular, the analysis of the results highlights the "human factor" as one of the most, if not the most, important drivers of operational risk, especially in the case of very severe events. No operational risk framework or internal control system can be considered completely immune from events like that which occurred at SocGen. However,

strong governance, operational risk management and control culture across all businesses, and especially those potentially able to generate high profits, but also big losses, can significantly mitigate such risks.

While banks believe that some of the distinctive elements of the SocGen event can be found in other rogue trading cases, the extent of the damage is generally felt to be the direct consequence of a widespread internal control system failure. The situation showed the “Swiss-cheese holes” symptom, well-known and feared in the operational risk community.

All the respondents believe that events of such magnitude would be very unlikely in their firms. However, most of them have been engaged, as a direct consequence of the SocGen or similar events which have occurred in the recent past, in a review of their operational risk frameworks/internal control systems and in an assessment of whether and to what extent improvements are opportune or necessary.

The elements to be improved are basically the “good old” internal control tools like the four-eyes principle, the segregation of functions and responsibilities between the negotiation and the payment, control and accounting activities, clear reporting lines and IT-based controls.

Most of the banks questioned believe, on one hand, that senior management should increase its understanding of the operational risks embedded in banks’ operations, in general, and in trading areas, in particular. On the other hand, that there is the need to foster a sound culture and appropriate incentive mechanisms in both the front office and the control functions of the trading rooms in order to prevent such an event from happening again. More generally, there is acknowledgement of the need for higher fraud awareness at various levels within the organisation and greater ability to manage and detect fraudulent activity.

As to the scope of the loss of this particular event, it is widely agreed that the whole of the damage should be considered in the AMA model, including the losses caused by closing the positions after discovery of the rogue trading.

In terms of AMA modelling, the banks that do not include this event in their “external data” component of the model consider it as a basis for scenario analysis or for stress test simulation. Some banks provided estimates of the impact (potential or actual) of the inclusion of the SocGen event in their AMA capital models, leading to an increase in the regulatory operational risk capital charge ranging from a few percentage points to almost 20 per cent. In this respect, it is considered to be important to have mechanisms in place to include external losses of such magnitude in the measurement systems, thus adequately reflecting them in the regulatory capital number.

As to the lessons that supervisors can learn, it is evident that the SocGen incident affects the supervisory community on a broad scale and is not limited to the bank where the loss has occurred. In reaction to this and other similar events, supervisory authorities have asked banks in their jurisdictions to perform ad-hoc assessments of their operational risk frameworks and/or internal control environment, in general, and of trading areas in particular. In some cases supervisors have planned (or already started) to review their supervisory

rules/guidelines in order to assess the need to enhance or introduce additional qualitative requirements on operational risk management and control.

The following section provides the detailed results of the stock-take.

3. Results of the survey of EEA reactions to the SocGen event

1. The stock-take was conducted from mid-February to end-March of 2008 and saw the participation of 17 supervisory authorities and about 100 banking groups in the EEA area.

2. Banks surveyed in the stock-take were selected at the discretion of participating supervisory authorities. In all but one country just AMA or AMA comparable banks were contacted; one authority performed a more widespread survey, involving most of their investment banks, regardless of the approach adopted for operational risk for regulatory purposes.

3.1. Banks' views on the presumed causes of the SocGen event

3. In banks' opinion, the weaknesses occurred - with different degrees of intensity - at all levels of control (first, second and third) within the SocGen organisational structure and related to the management of various types of risk, namely market, operational and counterparty risks.

4. In particular, the main drivers of the loss event can be grouped into the following five broad categories:

   a) failure to adequately enforce segregation of duties between front, middle and back offices (e.g. moving a middle office worker directly to the front office covering the same product; lack of independence between the negotiation and settlement of trades);

   b) lack of IT-related internal controls (e.g. allowing the trader to delete and re-enter fake trades; making unauthorised use of log-in passwords; failing to impose a regular change of employees' passwords);

   c) weaknesses in business/management routines (e.g. failure to ensure two weeks minimum consecutive holiday; failure in the confirmation process of OTC transactions with clients/counterparties and pending counterparty certification; failure to reconcile daily cash flows);

   d) inadequate monitoring and reporting systems (e.g. taking into account only net or risk equivalent amounts; insufficient reports on existing positions, especially on the amount and volume of settled transactions at client/product/trader levels; inefficient counterparty limit analysis; failure to monitor the number of cancelled/amended trades during a certain period of time; failure to control the cash flows and their origin, or where the P&L effects or their magnitude came from; failure to monitor and check trades in "pending" status; failure to identify unexpected large profits); and

   e) weak escalation processes (e.g. leaving aside external and risk management questions not properly acted upon; no rigid consequences of

limit breaks; failure to adequately react to external signals such as the Eurex warnings).

3.2. Banks' views on the possibility of a similar event happening in their organisations

5. There is general agreement that rogue trading can occur. However, all the respondents pointed out that the impact of events like that on their banks would be much lower.

6. Banks stated that their internal control environment and procedures (including commercial trading platforms and control systems) would identify such an event at a very early stage, thus avoiding any material loss. In addition, some of them focused their attention on the specific products/activities related to the SocGen case (arbitrage trading) and considering that they were not involved in this type of activity assumed that such an event was unlikely to happen.

3.3. Banks' reactions in respect of lessons learnt and improvements in operational risk management and control frameworks

7. The SocGen event has acted as a useful reminder for most of the banks included in the scope of the stock-take:

   - to perform an analysis of internal processes in market places and to check whether their own internal control system is sufficiently watertight to prevent such an event from happening;

   - to check whether the quality of execution of these controls has been jeopardised (e.g. by operating functions not having evolved in line with business ambitions/growth; by investments in systems having been postponed/delayed; by overloaded human resources executing manual controls); and

   - to consider introducing, where necessary, improvements in their operational risk framework or, more generally, in their control systems and the environment of the market place.

8. Some banks have recently experienced rogue trading events of lesser magnitude and have carried out comprehensive reviews of their systems and procedures well before the SocGen incident came to light. These banks seem to be in a better position to appreciate improvements in their control mechanisms. A few banks believe that no changes in their internal control frameworks are necessary because of the significant differences in the nature of their business compared to that carried out by SocGen.

9. As for the improvements deemed necessary, emphasis is placed on "good old" internal control tools like the four-eyes principle, clear segregation of functions and responsibilities between the negotiation and the payment, control and accounting activities, well-defined, transparent and consistent reporting lines, and IT-based controls (e.g. access rights).

10. In particular, banks appreciate the need for better alignment between front, middle and back-office functions and systems to ensure higher quality of the reconciliation/confirmation processes (e.g. set up of procedures for recording transactions, for addressing changes/cancellation of trades, for deviations from internal limits imposed, as for instance the validation of payments above predefined limits); enhancing monitoring of exposures and limits to detect in a timely manner trends or atypical behaviour in a trader's business (e.g. daily or intraday monitoring for the market risks limit system, P&L, trading book positions; monitoring of gross positions; implementation of risk indicators at product/trader level on modified/cancelled/backdated deals, on limits breaches, on the occurrence of backlogs in the settlement of trades, on off-premises and after hours trading); and synchronising the assessment of risks by all the assurance functions (internal audit, compliance, controllers and risk management).

11. From a governance perspective, it is widely agreed that the role of senior management in operational risk management should be enhanced. In particular, the senior management should increase its understanding of the operational risk embedded in the trading areas.

12. In addition, the following elements, typical of a sound organisational culture, seem to play a dominant role in preventing such events: the establishment of a front office culture designed to prevent rogue trader activities[1]; the adoption of appropriate incentive mechanisms to ensure that control and oversight of trader activities by all control functions (front, back, middle offices, risk management, compliance, internal audit, etc) is promoted and rewarded; the recruitment, training and retention of capable control and support resources who undertake their responsibilities diligently and with integrity.

13. Finally, the need for higher fraud awareness at various levels (line managers, back/middle offices, risk control/internal audit functions, senior management) and greater ability to manage fraud is considered a priority for many banks. In this respect, it is deemed important to set up integrated and effective alerts/warning systems in sensitive processes, businesses and product lines in order quickly to identify and limit the size of any fraudulent activity.

3.4. Banks' views on the impact of the SocGen event on AMA models and the operational risk capital charge

14. As SocGen is not a member of the industry consortia that share operational risk losses, this loss will not be directly reflected in the AMA models of banks that make use of consortia data as an "external data" source. However, the SocGen loss is public data in the media and so will be reflected in public

[1] For example by stimulating social control in the front office, particularly focusing on unusual behaviour, with particular emphasis on vacation policy and improvement of monitoring of transfers of people from back/middle to front office; by discouraging employees from moving directly from the middle/back office to the front office in the same product line; by requiring traders to conform to a rigorous code of conduct as regards their relations with intermediates and counterparties.

operational risk databases; hence, banks using public sources of data will have their capital calculation directly affected by this large event.

15. Almost all of the banks that do not include this event in their “external data” component will consider it as a basis for scenario analysis. In this way, the SocGen loss will also affect the estimation process of the capital calculation. Other banks will include the event in a stress test simulation and the sensitivity to this event, carefully weighted, is considered a prudential cushion for the regulatory capital measure.

16. As to the scope of the loss from this particular event, it is widely agreed that the whole damage should be reflected in the AMA model, including the losses caused by closing the positions after discovery of the rogue trading.

17. The SocGen event also raises questions about the marginal impact of including external losses of such magnitude in the calculation of the “tail” of the aggregate distribution for AMA modelling and the extent of the use of public operational risk data sets.

18. Some banks provided estimates on the impact (potential or actual) of the inclusion of the SocGen event in their AMA capital models, leading to an estimated increase in the regulatory capital charge of up to 20 per cent.

19. Finally, some banks underlined that the use of parameters estimation procedures characterised by a high level of robustness is a paramount prerequisite for tackling such extreme losses.

3.5 Reaction of supervisory authorities to the SocGen event

20. Most supervisors pointed out that the SocGen case, besides its effect on quantitative capital requirements, underlined the importance of qualitative requirements on operational risk management and control, in general, and in trading areas in particular, within the supervisory rules and guidelines. In some jurisdictions such rules/guidelines already exist and their relevance and adequacy is currently being analysed and, if necessary, revised in light of the SocGen event.

21. Supervisors have contacted banks asking them to investigate, by means of ad-hoc audit examinations, their internal control frameworks and to focus on the review of the adequacy of those frameworks in the light of the control deficiencies detected in the SocGen case. Supervisors have also requested banks to examine whether their scenario analysis related to rogue trading and internal fraud in trading areas is still adequate.