



July 2008

Briefing Note

FINANCIAL REGULATOR ISSUES LETTER ON RISK MANAGEMENT AND INTERNAL CONTROLS TO BANKS AND MIFID FIRMS

This briefing originally appeared in our Newsletter in July 2008. To subscribe send an e-mail with 'subscribe' in header to news@complianceireland.com.

On 6 June 2008 the Financial Regulator wrote to banks and investment firms reminding of appropriate *Risk Management and Internal Controls*. The Financial Regulator has not made its letter, including an Annex A to the letter, publicly available. **Compliance Ireland** has discussed with the Financial Regulator its decision to not publicise the letter and although we respect its position, we do not agree it. The Financial Regulator has confirmed that the letter and Annex A was issued to relevant firms.

Some of our reasons why the letter, or at least Annex A, should be openly published include: (i) that Annex A is an excellent set of standards that should be promoted constantly and be available in a permanent form on its website (as is the case with other financial regulators and indeed other communications of the Financial Regulator); (ii) it could be the case that a firm receives the letter, but it is another thing as to whether risk professionals joining that firm will learn of the details within Annex A and the regulator's expectations; (iii) new investment firms seeking authorisation could be at an information disadvantage; and (iv) even if a firm did receive the letter, will the board of directors be made aware of its importance?

We are hopeful that by further dialogue with the Financial Regulator this letter and similar letters will be made publicly available.

In any event, we have uploaded a copy of a CEBS report dated 18th July titled *Reactions to the Société Générale loss event: results of a stock-take* which deal with the issues in Annex A. The CEBS report is located at

http://www.complianceireland.com/documents/CEBS_survey_Kerviel_governance_good_practice.pdf

So what does the *Risk Management and Internal Controls* letter and Annex A include? Obviously we are not going to publish the letter! However here is a summary of its contents:

- Following discussions with the Committee of European Banking Supervisors (CEBS) on recent events, including **Société Générale** - the biggest fraud investigation in banking history - involving 31-year old Frenchman *Jérôme Kerviel*, European Supervisors agreed that it would be beneficial to firms engaged in trading desk activities to see CEBS's analysis. The analysis is then summarised in Annex A to the letter. *[Ed – the requirements in the letter are not trading specific, except in relation to trading limits. Therefore non-banks and non-MiFID firms (especially their non-executive directors and compliance & risk functions) would benefit immensely from seeing the analysis on Management Information and Governance].*
- The Financial Regulator's letter reminds firms of its expectations that in fulfilling their MiFID obligations firms undertake regular reviews of "the adequacy of existing control policies and procedures, and related verification and compliance systems. The Financial Regulator also expects that all firms will review the adequacy of their current operational framework having due consideration to the recent events and the issues set out in [Annex A]".
- The Financial Regulator required firms to respond by 18 July 2008 confirming that:
 - (i) each firm had conducted a review of the adequacy of current operational risk framework; and

- (ii) to the extent that the review identifies any control issues or areas that need to be strengthened to outline the firm's plan for remedial action.
- Annex A is comprised of three key sections, A. Internal Controls, B. Management Information and Reporting, C. Governance.
 - A. Internal Controls
Under this heading firms are to:
 - review their policies, procedures and controls to ensure traders execute transactions only when doing so is in compliance with trading authorities and limits. Enforcing of these limits and monitoring use of limits is vital;
 - ensure traders acknowledge limits in writing, with senior and appropriate management appointed to monitor back and front office functions;
 - review limits periodically;
 - ensure clear audit trails of cash flows;
 - analyse impact of trades on P&L accounts;
 - adopt rigorous reconciliation systems and controls, to be completed by back or middle office staff independently of front office staff;
 - where trades are performed OTC, use standardised contracts (preferably ones developed by professional associations) and review compliance on a regular basis;
 - have sufficiently qualified staff to verify conformance of contracts;
 - where functions are outsourced, adopt a strengthened control system;
 - properly secure information systems and limit employee access on a 'need to know' basis and 'need to do' basis. Stronger controls to be in place where staff move from back office to front office (and visa-versa) roles;
 - information systems, through which trading and verification are processed, be subject to regular review.
 - B. Management Information
Under this heading firms are to:
 - adopt management information reports which are well understood and that reports by different level of the hierarchy do not pose problems in terms of understanding the data created. *[Ed – this was not just an issue in Société Générale. In the case of Barings, a director was unable to define a 'derivative' under examination in court and admitted he did not know how to read reports submitted by the trading and risk departments];*
 - adopt clear reporting lines *[Ed - i.e. document apportionment of responsibilities]*, especially in relation to escalating of breaches of authorities/limits with a firm and following up of counterparty queries;
 - analyse the root cause of each issue, regardless of the reporting line through which the issue travels, look for and respond to root causes;
 - adopt well organised function charts particularly in complex organisations *[Ed – in our experience from assisting firms in Ireland, the UK and elsewhere, most trading breaches and errors go (collectively) undetected by management because the person who saw the raw data was not sufficiently trained, skilled or confident to raise 'the elephant in the room scenario' and if they were, they did not clearly document the issue in a report. This has then led management to mistakenly overlook the issue because of the poor quality of reporting];*
 - C. Governance
Under this heading firms are to:
 - ensure that monitoring and control functions have sufficient resources in terms of staff, expertise, systems and authority to carry out their functions effectively *[Ed – in Ireland we have lived with this requirement under the Investment Intermediaries Act 1995 (now joined by MiFID – Regs 35-37), the Consumer Protection Code (both as a General*

Principle and Common Rule) and forthcoming Solvency II Directive. No matter how often regulators raise this issue, firms generally do not respond in a proper manner purely on the basis that risk management, compliance and internal audit are labelled 'cost centres'. Years ago when yours truly joined as head of legal and compliance of an investment company, a senior trader said it was good to meet the 'business prevention unit' – it was funny at the time, until I thanked the 'head of the business destruction unit' for his valuable input. Subsequently we uncovered a suspected 'front-running' operation. I think that there is a lesson here somewhere?]

- an independent internal audit function should monitor adherence to and adequacy of policies and procedures, controls and procedures for risk management [*Ed – spotting this as a growing issue under MiFID and Solvency II, Compliance Ireland have developed a new ½ day course on Establishing an Internal Audit Function*];
- front office trading staff should be required to take at least two weeks continuous annual leave during a year [*Ed – this lesson is one we should have learnt two centuries ago!. As reported by Richard Lambert in Financial Times (FT Weekend July 19), one thing to watch out for is employees who never take a holiday. William Pullinger of Union Bank was obliged to attend a funeral in 1860 which led to his massive embezzlement being uncovered. It was the extended leave of Jérôme Kerviel of Société Générale that led to the uncovering of that fraud. The UK FSA earlier this year suggested two week continuous vacation as good practice following its review of the UK market following the Société Générale fraud. But the UK cannot point fingers either – in 2006 Anshul Rustagi, a derivatives trader at Deutsche Bank was suspected of a £30m (\$53m) overstatement of his trading position. Mr Rustagi was dismissed by his employer following a disciplinary hearing over the alleged overstatement. The overstatement was discovered by a colleague who was looking after Mr Rustagi's trading book while - you guessed it - he was on Christmas/end of year holidays.*]
- depending on the nature, size and complexity of a firm and its business, directors should consider establishing risk, compliance, audit and internal committees comprising [*Ed - but not exclusively!*] of independent directors to ensure that sufficient resources are deployed to the departments charged with monitoring compliance, assessing risk and carrying out independent audits [*Ed – enough said*]

Compliance Ireland Regulatory Services Limited is a leading independent regulatory consulting and training business. Collectively the Directors are former financial regulators (UK Financial Services Authority and Australia Securities and Investment Commission), lawyers and accountants specialising in regulatory affairs. This briefing note is not intended as advice. Readers should contact their professional adviser should they require advice. Please contact us at email@complianceireland.com or + 353 (0) 1 425 5962 should you wish to discuss any of the matters above.

To subscribe to briefings such as this briefing, subscribe to our free news service by sending an email with 'subscribe' in header to news@complianceireland.com. Details of our training courses are available at <http://www.complianceireland.com/publictraining.html>