

Speech by SEC Staff: "Risk Management for Broker-Dealers" by Mary Ann Gadziala, Associate Director, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission

2007 AICPA/FMD National Conference on the Securities Industry  
New York, NY  
November 28, 2007

As a matter of policy, the Securities and Exchange Commission disclaims responsibility for any private publication or statement of any SEC employee or Commissioner. This speech expresses the author's views and does not necessarily reflect those of the Commission, the Commissioners, or the other members of the staff.

## I. INTRODUCTION

It's a great pleasure to be here today to speak to this very distinguished group about risk management. Twelve years ago, the SEC Office of Compliance Inspections and Examinations — OCIE — created and implemented a program to examine firms for risk management controls. That year, 1995, coincidentally, was the year of OCIE's own creation. Since the inception of the risk management examination program, our focus has been the largest and most complex firms. However, this year we plan to focus more on mid-sized firms that have significant customer accounts. These firms may not be so familiar with our risk management examination process. Moreover, the SEC has proposed rule amendments that would subject an estimated 500 large firms, many of which have not experienced a risk management examination, to a requirement that they keep current records documenting their implemented systems of internal risk management controls.<sup>1</sup> Therefore, my purpose today is to give you some insights into our OCIE risk management examinations.

As I am sure you know, there is currently no specific rule requiring risk management controls for broker-dealers, except generally for OTC derivative dealers and consolidated supervised entities (CSEs). For the majority of you who do not fall into either of those categories, having effective risk management controls is a proactive sound practice to protect against significant financial losses, violations of law, and investor harm — laudable goals indeed. The SEC, in its recent Proposing Release on amendments to the financial responsibility rules, highlighted the need for firms to have documented controls for managing risks, stating: "A well-documented system of internal controls designed to manage material risk exposures enables a broker-dealer's management to identify, analyze, and manage the risks inherent in the firm's business activities with a view to preventing significant losses."<sup>2</sup>

In my view, there is no single blueprint for risk management controls. Rather, a robust and comprehensive risk management system should be customized, reflecting the risks and complementary controls for the particular organization and all business activities of the firm. The design and implementation of an effective risk management control system may take into consideration many factors — organization and structure of the firm, a historical perspective on growth and business, geographic dispersion, customer base,

trading strategies, counterparties, funding and liquidity needs, potential conflicts of interests, technology and systems available, business activities, products created and/or sold, applicable laws and rules, market events, and changing economic conditions, just to mention a few. Moreover, creating effective risk management controls is not a one time event. Risk management controls should be sustainable and evolve to keep pace with changes at the firm, in the markets, and in legal requirements.

Effective risk management controls are typically proactive rather than reactive. They are meant to be a defense against violations of law and potential reputational harm, financial losses, and investor harm — results that may not only be damaging to the firm and its customers, but may result in firm failures or even unacceptable market instability. During the recent events in the subprime and credit markets, some firms, recognizing the need to be proactive and to continually re-evaluate control systems in view of changing conditions, took actions to strengthen risk management controls. One example was a firm that reportedly created a special executive committee to review lending practices and report to the board's risk and compliance committee. Another firm strengthened its underwriting standards and yet another limited the reset periods for its adjustable-rate subprime mortgages. While ideally, all risk management controls would be proactive and keep firms out of trouble, problems do occur. In such cases, it would be prudent for firms to take corrective action and impose appropriate controls as quickly as possible.

The primary purpose of OCIE risk management examinations is to obtain an understanding of a firm's business activities, risks, and controls, to evaluate the controls in the context of the firm's operations, and to identify concerns or perceived weaknesses. It is then the firm's responsibility to address the concerns. Risk management exams are not primarily meant to identify violations and make enforcement referrals — in fact, I can not recall any examples of enforcement referrals from risk management examinations OCIE has conducted over the past twelve years.

Thus, you might view our risk management examinations as displaying some of the characteristics of "principles based regulation" and "prudential supervision". While the approach towards risk management reviews by OCIE is flexible and customized to the firms, there is available guidance on core principles of effective risk management systems to which we may refer in conducting our evaluations. Such guidance may also be helpful to you in designing and maintaining an effective risk management system at your firm. Next, I shall discuss some of that guidance.

## II. RISK MANAGEMENT PRINCIPLES

The basic principles of risk management go back quite some time, and firms have been using them in designing their risk management programs to protect their reputations and financial integrity, and to protect investors. One of the earliest articulations of general risk management principles arose out of the concerns associated with risks of derivatives. The Group of 30, in 1993, published its report, "Derivatives: Practices and Principles."<sup>3</sup> This comprehensive study contained more than twenty recommendations for dealers and users for managing risks of derivatives activities. These general principles continue to serve as a basic foundation for risk management principles even today, although specific

enhancements continue to evolve. Other sources of information on general risk management standards may be found in materials published by the Bank for International Settlements, the Global Association of Risk Professionals, the bank regulatory agencies, the International Organization of Securities Commissions, and the Counterparty Risk Management Policy Group. You might also refer to Rule 15c3-4 of the Securities Exchange Act of 1934 to get a general sense of what might be considered when adopting a risk management control system.

Perhaps the most timely and relevant publication on risk management principles from the perspective of the SEC, which is specifically related to legal and reputational risks associated with complex structured finance activities, is the "Interagency Statement on Sound Practices Concerning Elevated Risk Complex Structured Finance Activities" (Interagency Statement). This statement was issued on January 5, 2007, by the SEC and the bank regulatory agencies.<sup>4</sup> I shall now spend a few minutes on the Interagency Statement before summarizing what we in OCIE review in our risk management examinations. The Interagency Statement is generally principles based. It describes some of the internal controls and risk management procedures that may assist financial institutions with the identification, review and approval of complex structured finance transactions (CSFTs) that may pose heightened levels of legal or reputational risk to a firm. These policies and procedures should, among other things, be designed to allow the institution to identify elevated risk CSFTs during its transaction and new product approval processes. They should provide for elevated risk CSFTs to be reviewed by appropriate levels of control and management personnel at the institutions, including personnel from control areas that are independent of the business line(s) involved in the transaction. They should provide for the maintenance of appropriate documentation in connection with these processes. In addition, firms should have appropriate training for firm personnel involved with CSFTs, and procedures should provide for periodic reviews and audits of CSFT activities to verify and monitor that procedures and controls are being effectively implemented. Firms engaged in CSFT activities should consider adopting the risk management principles described in the Interagency Statement to assist them in developing and maintaining robust and effective risk management programs with respect to these complex activities.

All of the guidance I have mentioned on risk management principles assists us in conducting our reviews and evaluating the risk management controls at different firms with very diverse operations. It may also assist you in designing or improving your risk controls.

### III. OCIE RISK MANAGEMENT EXAMINATIONS

In general, all OCIE examinations, including risk management examinations, are conducted using the same general process. You may find a brief description of this process on the SEC website, under "Offices/Divisions — Compliance."<sup>5</sup> Generally, risk management examinations are "announced" by sending the firm a letter notifying it of the examination and requesting documents. This is followed by an on-site examination. An initial interview begins the onsite examination, and other meetings and document requests typically follow. Relevant books and records of the firm are examined. On the

last day of the on-site visit, examiners will generally discuss the exam status, outstanding document requests, and if appropriate, issues identified. Examiners then return to their offices to continue their analyses. When the work is completed, a final exit interview is held if issues other than those previously discussed are identified, and the firm will be provided the opportunity to discuss any of the staff's findings. When an examination is concluded, the staff will send the firm a letter summarizing the findings, the firm's preliminary responses, and requesting a written response regarding corrective actions.

During an OCIE risk management examination, we obtain an overview of the firm's organizational structure and risk management system — the process by which managers identify, assess, monitor and control risks within the broker-dealer. This assists us in developing an initial scope of the areas of risk management to be reviewed. These exams are generally conducted in conjunction with a review of the firm's compliance with the SEC financial responsibility rules, including capital rules. We recently added a new preliminary step in our risk management examinations, which involves a review of the work of the firm's internal audit department in the risk management area to assist us in scoping our examination coverage. To the extent we find that the work of internal audit is independent, high quality, and effective, and that timely meaningful corrective action has been taken in response to audit findings, we may leverage off the firm's internal audit work. This allows us to limit the scope of our examinations and focus on other high risk areas, permitting more effective, efficient and less resource intensive risk management examinations by OCIE staff.

Our internal controls examinations include reviews of the following areas:

Internal audit, to ensure that comprehensive and independent assessments get to management and the board, and that deficiencies are addressed in a timely manner; the review also assists us in scoping our examinations;

Senior management, to look for establishment of overall policies and active involvement in the oversight of risk parameters and controls — areas of particular focus for senior management also may include ensuring that firms have sufficient resources for risk management and protecting against the so-called "silo effect" where risk management is not integrated into a common framework; enterprise risk management is the new watchword for comprehensive and effective risk management systems;

Adequacy of resources and systems used for risk management; and compensation or other incentives that may adversely impact independence;

Market risk in trading activities and firm inventory, including VAR (value at risk), economic models, scenario analyses, stress testing, and back testing; we follow trades from the trading desk through the entire risk management system; for firms that have chosen to implement Appendix E for capital changes, we would also be looking specifically for controls to ensure compliance with the requirements of Appendix E; to the extent a firm did not engage in principal trading activities or hold firm inventory, this area may not be a significant area of review during a risk management examination;

Funding, liquidity and credit risks, including counterparty credit risk across all products and businesses, credit limits, pricing models, valuation, guarantees, collateral, margin, and settlement and legal risks — the recent events in the subprime market and impact generally of those events on the capital markets demonstrate the importance of strong and evolving credit controls; for retail firms, the focus would likely be on collateral and margin, as well as counterparty credit risk, as appropriate;

Operational risks, including: segregation of duties; checks and balances; protection of customer funds and securities; controls to prevent identity thefts, phishing attacks, and inappropriate release of sensitive customer information; operating systems; management information systems; management reporting; front and back office operations; security; and contingency planning and disaster recovery — in this last area, the devastating results of 9/11, major hurricane damage, and the California fires are only a few recent examples of why business continuity risk management is so critical;

Legal and compliance controls, including surveillance and monitoring systems and procedures, reports to senior management, and independence — unlike "supervision" by the business area, "compliance" is an independent oversight function; for firms that are more oriented toward retail rather than wholesale operations, controls related to sales practices — highlighted, for example, by rules precipitated by the Guttadauria case, are key elements of risk controls;<sup>6</sup> recent reports have indicated that some firm personnel are not confident that policies and procedures are current and complete and therefore do not bother to read or follow them — having comprehensive and up-to-date procedures is critical and this should help ensure they are read and followed;

And finally, we look to see that new products and activities are assimilated into the risk management system in a timely and appropriate manner — the Enron-related problems with general concerns about CSFTs are just one example that highlights the need for integrating new products in risk management control systems.

In conducting risk management examinations, OCIE examiners look for areas where the firm's controls are weak or inadequate. We will conduct more thorough reviews in those areas. Internal controls and effective risk management are particularly important when firms are more aggressively pursuing innovative ways to increase revenues and enhance profits, or developing new businesses or products. It is important that controls be particularly robust and frequently reviewed and updated during volatile market conditions or when specific risks arise such as those we recently experienced in the subprime and credit markets. Under such conditions, we should all be more vigilant.

Thus, the objective of an OCIE risk management examination is to assess and note findings with respect to the adequacy of the structure and operation of a firm's risk management processes and systems. The ultimate goal is for the firm to take remedial actions to improve its risk management controls as appropriate. In the current environment, you may wish to give special consideration to new or significant business activities or products, compliance controls and operational systems, increased credit risk, sufficiency of margin and collateral (especially for highly leveraged customers), the

valuation process (especially for volatile or highly complex products), data integrity, information leakage, business continuity plans, capacity to handle high volume volatile trading days, and integration of all risk controls. There has been quite a bit of progress at many firms in building more robust risk management programs and we hope this trend will continue as firms realize the benefits achieved from proactive and preventive efforts.

#### IV. FIRM PRACTICES OBSERVED DURING EXAMS THAT MAY MITIGATE RISKS

During OCIE risk management examinations of the largest firms, staff identified practices that firms implemented to mitigate risks. For illustrative purposes, I shall highlight just a few of those in each key area to give you some idea of controls that may work well. In considering these examples and implementing a risk management system, it is important to note that the risks and controls are all interrelated and that different controls may work better at different firms. Examples of practices that may mitigate risks include:

##### 1. Senior Management Involvement

Effective senior management involvement in setting overall risk management principles for the firm and in making key risk management policy decisions;

Comprehensive evaluation of risks and controls and documented periodic review of firm-wide limits or risk levels for authorized business activities; and

Access by senior management to reports and timely information on material risk breaches, events, and overall risk-related issues.

##### 2. Internal Audit

An experienced and independent audit department with necessary resources;

Comprehensive identification of the audit universe and assignment of appropriate risk rankings for auditable areas, resulting in appropriate cycles of review;

Complete documentation of the internal audit process with respect to workpapers, audit cycles, and annual risk assessments; and

Effective monitoring of timely corrective action responsive to audit findings.

##### 3. Operational Risk

An effective reconciliation process to ensure data integrity and completeness;

A dedicated group and/or committee effective in identifying and establishing controls for operational risks; and

Integration of all systems and material operational risks in reports to and discussions with senior management.

##### 4. Market Risk

Acting within market risk limits, or having effective procedures and documentation concerning limit excesses;

Creation/review of internal mathematical models by an independent risk group, periodic independent review of the models, and adherence to conditions imposed by the control group; and

Written procedures established to address pricing of securities, especially illiquid securities, including methodology, models, process, and thresholds for price adjustments with appropriate approvals.

#### 5. Credit Risk

Implementation of effective procedures for timely periodic financial reviews and due diligence on counterparties;

A formal process for monitoring counterparty credit limit overages and recording management approvals and rationales for limit increases; and

Maintenance of complete written credit risk management procedures and reporting, including procedures for monitoring adherence to credit risk limits with documented approval for limit excesses at appropriate levels.

#### 6. Legal and Compliance

Complete up-to-date written legal and compliance policies and procedures;

Effective monitoring and surveillance of compliance and legal issues;

Legal and compliance committee approval participation for new and high-risk business, products, or transactions;

Clear assignment of authority and responsibility for legal and compliance; and

Strong overall compliance culture at the firm.

#### IV. CONCLUSION

The challenges we face continue to grow. I have never before seen the explosion of growth in business diversification, geographic expansion, new complex products, and unexpected contingencies that we have been experiencing. More and more confidential and sensitive trade, financial and other client information is available to firms. These developments raise significant challenges to maintaining an effective internal risk management control system. And it is only with effective compliance and risk management controls that problems can be minimized. As financial markets and products become more complex and risks proliferate and as conflicts arise, firms should continue to promote robust and effective risk management and compliance systems, operations, and controls to meet these challenges. Thank you for allowing me to share these thoughts with you.

Endnotes

---

1 Amendments to Financial Responsibility Rules for Broker-Dealers, Exchange Act Release No. 34-55431 (March 9, 2007), 72 Fed. Reg. 12862 (March 19, 2007).

2 Id. at p. 36.

3 [http://www.group30.org/pubs/pub\\_0901.htm](http://www.group30.org/pubs/pub_0901.htm).

4 <http://www.sec.gov/rules/policy/2007/34-55043.pdf>.

5 [http://www.sec.gov/about/offices/ocie/ocie\\_exambrochure.pdf](http://www.sec.gov/about/offices/ocie/ocie_exambrochure.pdf).

6 See, Federal Register, Vol. 69, No. 120, June 23, 2004.