

**Panel Discussion at AICPA/SIFMA FMD National Conference,
November 27-28th, New York**

Panel Topic: Risk Management Policies and Procedures

**Speech presented by Steven Goldberg, Principal, Grant
Thornton, LLP, Business Advisory Services Practice**

Introduction

Risk management is clearly a key issue in today's markets. Recent failures in risk management models and systems point to the need for increased diligence relating to managing market and credit risk, as well as continued regulatory and operational risks. The renewed focus on risk management can be seen in the recent appointments of new Chief Risk Officers at several major firms including JP Morgan, Lehman Brothers, Merrill Lynch and CitiGroup.

In addition to the challenges of complex new products available in today's markets, firms must also be concerned with increased trading volumes, new and complex regulations such as Reg NMS as well as new products that carry additional risk such as Portfolio Margining. Performing adequate risk management procedures is especially important and difficult for mid-sized firms given the limited compliance and internal audit organizations and budgets. The importance of clear policies and procedures including those around market risk models and escalation procedures can be seen in the current credit crisis.

Today, I will provide an overview of key risk related considerations and general thoughts on how to best assess, test and manage those risks. As regulators focus more attention on smaller firms, it is critical that those firms follow an efficient process in identifying and assessing key risks,

mitigating them where possible and testing them based on established audit and regulatory guidelines

In addition, it is important to ensure that the firm continues to send the right message regarding risk management. Setting a *tone from the top*, and creating a *culture of compliance* sends the appropriate message regarding everyone's responsibility for managing the firm's risk.

Organizational Roles and Responsibilities and the Risk Management Process

There are several key considerations relating to risk management roles and responsibilities, especially in those firms with limited compliance and audit staff. Clear responsibilities should be defined and procedures to carry them out should be developed – some roles will be formal, and governed by the firm's risk management policies and procedures, others less formal, and set by the tone of the organization in managing risk.

The entire organization should know that managing risk is an essential part of the business process and is filtered throughout the organization through formal policies and procedures, and the general way that business is conducted. The Risk Management process starts with senior management, who has specific as well as symbolic roles:

Under FINRA 3013 rules, the CEO must provide an annual certification that the organization has an adequate supervisory control system in place. This is an opportunity to truly assess the control systems and policies in place and take corrective actions where needed.

The CEO and other senior executives must also set the tone – where there is a decision to be made between supervisory responsibilities and financial gain – managers and supervisors (as well as staff) must understand that they are expected to make the right decisions and not put the firm at risk

An independent internal audit function is essential, whether it is maintained in house, co-sourced or outsourced to an independent third party. The internal audit group should be expected to present a thorough risk assessment to the audit committee – the audit committee should continue to provide independent oversight throughout the audit process

The Chief Compliance Officer must meet with the CEO on a regular basis to discuss the system of supervisory controls, as called for by FINRA 3013. In addition, the CCO must ensure that Written Supervisory Procedures are developed and updated as business conditions change, and that the WSP's are independently tested as part of the FINRA 3012 and NYSE 342 reporting requirements. Oversight of regulatory compliance, regulatory reporting and compliance with Anti-Money Laundering/Bank Secrecy Act requirements are also critical.

In a smaller firm, roles will overlap – to the extent that exemptions may be made for the independent supervisory testing requirements of FINRA 3012 – this makes the development of concise written policies and procedures even more important for those firms.

Policies and procedures will guide and drive behavior – Written Supervisory Procedures will govern responsibilities for supervisors in revenue producing areas; internal controls and related procedures will cover operations, technology and financial areas – in addition, procedures should be concise in terms of addressing market risk – and use of VaR and other pricing models. Use of these models should be fully documented along with clear limits, lines of authority and escalation procedures.

Procedures should also govern introduction of new businesses and products – business plans for new products should be run through a “New Business Committee” in order to assess cost versus benefits, as well as the market and operations related risks.

Firms should follow a comprehensive program in assessing risks – especially in a smaller firm, where there is much less of a margin of error – regulatory findings and fines will have a much greater financial and reputation risk for these firms.

A Risk Assessment (performed as part of the internal audit process, and/or FINRA testing) will determine areas of highest risk, and provide a framework for prioritizing and testing processes. Areas to focus on should include:

- Operational Risk – including Information Technology, Operations, Business Continuity Planning, credit and capital risks
- Regulatory Risk – Regulatory Reporting obligations (a recent review of a mid-sized broker dealer identified almost 2,000 reports required by various regulators), annual certification and reporting, examinations
- Market Risk – Risk Management pricing models, supervision and control of revenue producing areas, procedures on risk limits, use of Value at Risk and theoretical pricing models, documentation of models and associated procedures for escalation and review are all included here.

The risk assessment provides a method, by which risk areas can be identified, addressed and monitored, and can be used as an oversight tool by senior management and the audit committee. It can also highlight areas where additional policies and procedures may be required to further mitigate risks.

Additional Risk Considerations

I mentioned Supervision and Control and the required CEO certification and independent testing process. There are additional considerations for smaller firms – exemptions are provided for independent testing rules if not enough officers are available to provide independent testing – in this case multiple roles can be designated. Firms are also required to provide a

heightened level of scrutiny where a supervisor is responsible for a desk generating a high percentage of the revenue in a particular business area – this situation is more likely to occur in a smaller firm. Supervisory coverage at branch or other remote locations also need to be considered.

The pilot program for portfolio margining, or risk based margin rules is in place – larger firms have been approved and are providing this margin product to their customers – this is already having a significant impact on options volume and margin outstanding. Implementation thus far is currently geared towards Hedge Funds and large investors – this will move to the retail business relatively quickly, which could increase margin and credit risk significantly for mid-sized firms offering this new product.

Firms wishing to offer portfolio margining to their customers will need to obtain approval from their Designated Examining Authority (DEA) and will have to develop extensive procedures relating to managing the new margin process – firms will also be required to implement the standard OCC theoretical pricing model, TIMS, as well as integrate the pricing model into their existing systems – this is a potentially significant cost to the firm. Firms considering offering this product should perform a cost benefit analysis and risk assessment, to make sure that all issues are understood and addressed before proceeding.

Reg NMS was implemented this past year – there is an impact on best price/best execution rules – compliance with the new requirements would presumably be included in next years regulatory exams – increased electronic volume may strain operations and technology at many firms – the burden of the cost to comply with the rules have a greater impact on smaller firms – causing some to outsource more technology functions.

Conclusion

Risk management policies and procedures are receiving increasing attention. Market conditions have highlighted gaps in the risk management systems at major firms.

In this environment, it is important to understand key risk related roles and responsibilities – setting a tone from the top – and creating a “culture of compliance”

Firms should utilize supervisory certification and testing requirements to identify and address gaps in the risk management process and organization. Firms should also perform risk assessments and coordinate activities with the audit committee and senior management

In addition firms should assess the risk of new business and products through a formal and documented process, and address regulatory issues proactively

Risk management is, in many ways a greater challenge for smaller firms, given fewer people and resources to proactively address risk management and meet regulatory requirements – However the investment is worth it, given the potential cost of a major failure of risk management systems.