2012 Enterprise Risk Series: Managing Compliance and Related Risks

Presented by:
M. Paige Berry, Esq., Saul Ewing LLP
Paul M. Hummer, Esq., Saul Ewing LLP
Frederick J. Kohm, Jr., Grant Thornton
Steven Skowronski, Grant Thornton

June 19, 2012
The Role of the Board in an Effective Compliance Program

The role of the Board of Directors of a company continues to expand as the focus moves towards management of a company’s “Enterprise Risk” and Boards are asked to be active participants in managing that risk.
An essential element of the successful management of a company's Enterprise Risk is a strong compliance program, for which support from the Board is critical to its success.
Why should the Board Care?

New regulatory focus where Board members are expected to play a more prominent role in Identifying, Managing & Reporting of Enterprise Risk.

» Risk focused financial examinations by regulators involving interviews with selected Board members.

» NAIC’s adoption of changes to the Insurance Holding Companies Model Act requiring statements on Form B filings that Board oversees corporate governance and internal controls.
Board members have a fiduciary duty of care which creates obligations in two ways: decision making and oversight.

- Compliance falls within the board’s *oversight* function and requires the Board to:
  1. Assure the company has an adequate compliance program and reporting system; and
How can a Board assure that an adequate corporate compliance program exists?

➢ The Board must set the “tone from the top”

• Set Expectations
• Communicate Involvement
• Ask Questions
➤ The Board must set expectations and work to create a culture of compliance.

➤ Board must communicate its desire to be kept informed and to be involved in policy decisions which assure that the company maintains an effective compliance program, while recognizing that it is not involved in day to day operations.
Ask questions

Board members should ask questions about the company’s corporate compliance.
Question No. 1

What is the structure of the Company’s compliance program and who is responsible for its implementation?
Structure

Seven elements of an appropriate compliance program:

1. A person or committee with adequate authority and resources will have primary compliance responsibilities;
2. Established system for identifying and evaluating the risks and rules;
3. Development and distribution of written standards of conduct, policies and procedures;
4. Education and training for affected employees;
5. System for receiving and responding to violations;
6. Creation and retention of records; and
7. Audit and evaluation process to monitor compliance program and address deficiencies.
Question No. 2

How does the compliance program identify, evaluate and address significant risks facing the organization?
Identifying and Evaluating Risks

How were the significant risks faced by the company identified, evaluated and incorporated into the program?

- **Identification**: statutes / regulations / case law / market conduct / enforcement actions / contracts / internal policies

- **Incorporation**: Material exposures / core regulations / regulatory focus / other
Identifying and Evaluating Risks

- How are emerging and changing risks identified and made part of the program:
  - Monitoring legislative / regulatory activities
  - Participation in industry groups / associations
  - Use of outside sources / experts
Question No. 3

How does the compliance program prevent and respond to violations?
Preventing Violations

- Prevention:
  - Identifying and understanding the rules
  - Determining the business process that is affected
  - Education and training
  - Identifying necessary changes to processes / procedures
  - Auditing changes
Responding to Violations

Responding:

- Identifying and reporting violations through internal audit / regulatory examinations / complaints / lawsuits
- Investigation process - Internal / external
- Record gathering and preservation
- Reporting violations to the appropriate authorities
- Processes to correct violations or deficiencies
- Established disciplinary protocols
Question No. 4

How is the Board informed about significant regulatory and industry developments affecting the Company’s risks?
Keeping the Board Informed

- What reports does the Board receive and what information is provided?
  - Compliance officer on Board agenda
  - Legislative / regulatory updates
  - All rule changes or only those creating material exposures?
  - All violations or systematic failures?
  - Past activities / future plans
Question No. 5

How does the Board oversee compliance issues?
Oversight

- Does the Board use a committee / subset or individual to monitor compliance issues?
- Is the Board involved in the periodic review of compliance policies and procedures?
- Are there thresholds for Board involvement in violations?
Department of Justice v. Morgan Stanley

- A strong compliance program can protect a company from enforcement action.

- April 2012 – Department of Justice and Securities Exchange Commission declined to pursue enforcement action against Morgan Stanley.
• Managing Director of Morgan Stanley plead guilty to conspiracy to evade Morgan Stanley’s internal accounting controls developed pursuant to the Foreign Corrupt Practice Act.

• DOJ and SEC declined to bring any FCPA action against Morgan Stanley for managing director’s action.
WHY?

• Morgan Stanley’s Compliance Program

Morgan Stanley:

- Maintained System of Internal Controls.
- Updated Internal policies on a regular basis to reflect regulatory developments and specific risks.
- Trained employees frequently regarding its polices and new laws and regulations.
- Monitored transactions and performed random audits.
- Conducted due diligence on new business partners.
- Imposed stringent controls on payments to business partners.
Internal Audit, Enterprise Risk Committees, and Enterprise Risk Officers
Tone at the Top

- Support from Board, Audit Committee, and Senior Management is critical to ensure effectiveness and sense of urgency.
- ERM cannot simply be viewed a necessary evil or an after-thought.
- Fatigue can and has set in given the focus on compliance, risk management, corporate governance, external audit, and internal audit.
Internal Auditing in ERM

- Core Role: provide objective assurance to the board on effectiveness in risk management
- Assurance Activities:
  - Giving assurance on the risk management processes;
  - Giving assurance that risks are correctly evaluated;
  - Evaluating risk management processes;
  - Evaluating the reporting of key risks; and
  - Reviewing the management of key risks.

Source: 1
Internal Auditing in ERM
(Continued)

- Consulting Roles:
  - Facilitating identification and evaluation of risks;
  - Coaching management in responding to risks;
  - Coordinating ERM activities;
  - Consolidated reporting on risks;
  - Maintaining & developing ERM framework;
  - Championing establishment of ERM; and
  - Developing RM strategy for board approval

Source: 1
Internal Auditing in ERM
(Continued)

- Roles Internal Audit Should Not Undertake
  - Setting the risk appetite;
  - Imposing risk management processes;
  - Management assurance on risks;
  - Taking decisions on risk responses;
  - Implementing risk responses on management's behalf; and
  - Accountability for risk management.

Source: 1
Current Roles for Internal Auditing

- 57% of internal audit activities around the world perform audits of ERM processes.
  - 20% indicated performing such audits will become more prominent over next 5 years (2010 IIA Global Internal Audit Survey).
- 24% indicated that their internal audit activity had primary responsibility for risk management in their organization (GAIN Flash Survey).

Source: 2
Implementing Internal Audit Programs

- Start with Internal Audit Charter (or similar for smaller organizations).
- Risk assessment is critical.
- Defined framework is necessary.
Compliance

Compliance is defined by various bodies and regulations:

- Statutory accounting and financial reporting
- GAAP accounting & financial reporting
- SEC
- IFRS
- NAIC and state regulators
- Solvency II
- SOX
- MAR
- ORSA
- Rate and form filings
- Premium taxes, assessments, etc.
- Data calls
- Risk-focused examinations
- IIA
Internal Audit Stakeholders

- Board & Audit Committee Members
- Senior Management
- Employees
- Shareholders
- Policyholders
- Rating agencies
- Regulators
- Lenders
Board Oversight and ERM

- 4 Areas that Contribute to Board Oversight with Regard to ERM
  - Understand the entity's risk philosophy and concur with the entity's risk appetite.
  - Know the extent to which management has established effective enterprise risk management of the organization.
  - Review the entity's portfolio and consider it against the entity's risk appetite.
  - Be apprised of the most significant risks and whether management is responding appropriately.

Source: 3
Prevalence of Governance & Risk Committees

- 83% reported that their boards have a governance committee.
  - 88% public companies
  - 92% public companies with revenue > $1 billion
- 44% reported that their boards have a risk committee.
  - 29% public companies
  - 20% public companies with revenue > $1 billion
- 47% of financial services organizations versus 24% of nonfinancial services organizations utilize risk committees.

Source: 4
Overview of Risk Committees

- The Dodd-Frank Act requires banks with greater than $10 billion of consolidated assets and certain nonbank companies supervised by the Board of Governors of the Federal Reserve Bank to establish stand-alone risk committees.
  - Various bills have been introduced in Congress that would impose even stricter risk management requirements upon boards of directors, including one requiring all public companies to establish a risk committee comprised entirely of independent directors.
  - A risk committee does not supplant the oversight role of the board of directors, rather assists the board in exercising those duties.

Source: 5
Possible Roles of Risk Committees

- Determining the most important of the company's operational risks;
- Making recommendations to the board of directors with respect to the amount of risk-taking activity in which the company should engage;
- Overseeing company-wide risk management practices;
- Establishing and monitoring key risks;
- Reviewing the company's periodic reports to ensure proper disclosure of risks and risk factors; and
- Reviewing communication systems to ensure the proper flow of information related to risk.

Source: 5
Potential Benefits of Stand-Alone Risk Committees

- Setting the tone for a corporate culture of risk management;
- Increasing the overall level of ERM;
- Additional expertise in managing operational risks;
- Additional devotion to risk oversight without significantly increasing responsibilities of the entire board;
- Having directors maintain a continuous view of risks; and
- Increasing communication processes regarding risks.

Source: 5
Potential Drawbacks to Stand-Alone Risk Committees

- Increased demands on director time;
- Increased organizational costs;
- Potential duplication of duties;
- Current effective risk management; and
- Need to set additional internal processes.

Source: 5
Roles & Responsibilities of Chief Risk Officers

- Centralize risk management;
- Understand relationships between risks within separate business units;
- Enable firm to make decisions based on better appreciation between risk and reward; and
- Ensure that the corporate strategic agenda reflects the most important existing and emerging risks.

Sources: 6
NAIC on Corporate Governance

- Insurers must establish and maintain a sound corporate governance framework that adequately recognizes and protects the interests of policyholders.
- Ultimate responsibility for effective governance rests with the Insurer's Board.
- Insurer's remuneration policy should not induce excessive or inappropriate risk taking.

Source: 7
NAIC on Corporate Governance (continued)

- Insurers must share material information with the Commissioner and relevant stakeholders at least annually:
  - Insurer's overall strategic objective;
  - Insurer's governance structure;
  - Background information on members of the Board and its committees
  - General design, implementation and operation of the insurer's remuneration policy;
  - Major ownership & group structures; and
  - Significant affiliations and alliances.

Source: 7
Insurer's Risk Management Systems

- Purpose: to identify, assess, monitor, manage, and report on reasonably foreseeable material risks
- Insurer's risk management systems should develop policies and procedures to manage, mitigate and report on risks.
- The risk management systems should regularly be reviewed and modified and improved as necessary.

Source: 7
Considerations of Risk Management Systems

- Probability, potential impact & time duration of risks
- Insurer's overall business strategy, objectives & risk appetite
- Appropriate processes & tools for identifying, assessing, monitoring, managing & reporting on risks
- Relevant & current emerging local or business specific risks
- Enterprise-wide risks

Source: 7
Characteristics of Risk Management Function

• Should be sufficiently independent and avoid conflicts of interest with other management functions;
• Should establish its own risk tolerances through the adoption of a formal risk tolerance statement;
• Should include provisions for the quantification or risk for a sufficiently wide range outcomes and be responsive to change using appropriate techniques;
• Should allow the insurer to gain and maintain an aggregated view of its risk profile at a solo and group level;

Source: 7
Characteristics of Risk Management Function (continued)

- Should be utilized by the insurer to determine the level of internal economic capital that should be held for solvency purposes;
- Should require that strategic decisions be made consistent with established risk management policies and tolerances; and
- Should be shared with and subject to review by the Commissioner through filing of an ORSA regularly.

Source: 7
NAIC on Internal Audit

• Purpose: to provide independent assurance to the board through general and specific audits, reviews, testing, and other relevant techniques

• The internal audit function should be free from conditions that threaten its ability to carry out its responsibilities in an unbiased manner.

• The internal audit function is ultimately responsible to the board, not Senior Management.

Source: 7
Optimization Areas through Insurers' ERM Implementation

- Risk monitoring & reporting
- Risk appetite statement
- Risk limits & controls
- Economic Capital
- Risk governance structure
- Use of EC in decision-making processes
- Risk culture
- Scenario testing/planning capabilities
- Managing individual risk exposures
- Risk resources, skills & capabilities
- Risk technology or systems
- Allowance for risk within business processes

Source: 8
Business Changes that Can Result from ERM Activities

- Asset strategy
- Risk strategy/appetite
- Pricing
- Management decision-making process
- Reinsurance strategy
- Product mix

- Overall growth strategy
- Capitalization
- Geographic spread of business
- New launch process
- Design of products

Source: 8
Responsibility for Risk Management

• A variety of roles or positions can be primarily responsible for an insurer's risk management:
  – Chief Risk Officer (CRO)
  – Risk management committee
  – CFO or Finance Director
  – Chief Actuary or Corporate Actuary

Source: 8
Key Categories of Risk for Insurers – Credit

Counterparty credit exposure from all potential creditors including:

- agents;
- reinsurers;
- bond issuers; and
- large, institutional clients.

Source: 9
Key Categories of Risk for Insurers – Market

Exposure to liquidity events, asset/liability mismatches and risks in investment portfolios due to changes in:

– equity prices;
– commodity prices;
– interest rates; and
– exchange rates.

Source: 9
Key Categories of Risk for Insurers – Underwriting

Financial exposures arising from damage to a company's reputation or franchise value stemming from factors such as:

- product development;
- regulatory relations;
- establishing reserves and pricing metrics;
- analyzing loss experience, mortality, morbidity, and lapses; and
- loss trends.

Source: 9
Key Categories of Risk for Insurers – Operational Risk

- Financial exposures arising from damage to a company's reputation or franchise value stemming from:
  - management change;
  - business interruption;
  - fraud;
  - data capture;
  - data security and integrity;
  - claims handling; and
  - employee retention.

Source: 9
Key Categories of Risk for Insurers – Strategic

Strategic – financial exposures arising from:

- adverse business decisions;
- improper implementation of decisions; or
- lack of response to industry changes

Source: 9
Risk Management & Ratings

- Risk management is the common thread linking balance sheet strength, operating performance, and business profile.
- If a company is practicing sound risk management and executing its strategy effectively, it will maintain a prudent level of risk adjusted capital and perform successfully over the long term.
- The assessment of an insurance company's risk management capabilities should be viewed in light of a company's scope of operations and the complexity of its business.

Source: 9
Risk Management & Ratings
(continued)

- Organizations must develop and constantly refine an ERM framework.
- The ERM process may be less complex for organizations with a more limited operating scope focusing on more stable, traditional lines of business.

Source: 9
Risk Management & Ratings
(continued)

• A.M. Best perceives risk management as paramount to an insurer's long term success.
  • Each company is expected to explain how it measures, monitors, and manages risk within the ratings process.
• An insurer that can demonstrate strong risk management practices integrated into its core operating processes, and effectively maintain its business plan, will maintain favorable ratings in an increasingly dynamic operating environment.

Source: 9
Best's Capital Adequacy Ratio

- BCAR helps Best differentiate between companies and indicate whether a company's capitalization is appropriate for a particular rating level; however is not the role basis for Best's Rating.
- A company's relative risk management capabilities are a key factor in determining the BCAR capital requirement.

Source: 9
BCAR (continued)

A.M. Best will consider allowing companies with strong risk management profiles to maintain lower BCAR levels relative to the guideline for their ratings based on case-by-case evaluation if ALL conditions are met:

- Superior traditional risk management fundamentals, relative to the insurer's risk profile, in each of the five key risk types;
- Superior capital management and financial flexibility, providing the organization with cost efficient access to capital even in distresses scenarios;
- Strong ERM characteristics; and
- Strong Economic Capital modeling capabilities.

*Source: 9*
Best's Approach to Risk Management & BCAR

- Only companies with STRONG risk management capabilities and LOW relative exposure to volatility are allowed to maintain BCAR levels at or near the guideline for their ratings.
- Companies with WEAK risk management capabilities need to maintain a higher level of required capital, even if there is a LOW exposure to volatility.
- As the exposure to volatility increases, the BCAR requirement increases at a more rapid rate.

Source: 9
ERM Characteristics

- Culture
  - Set the Tone at the Top
  - Establish and clearly communicate risk management objectives
  - Define roles and responsibilities
  - Strategic decision-making processes

- Identification and Management

- Measurement

Source: 9
ERM for Complex Organizations

- Examples of Complex Organizations:
  - Insurers participating in the global reinsurance and retirement savings markets; and
  - Insurers with diverse operations covering a variety of products and distribution channels.
- ERM takes on increasing importance in complex organizations and must constantly be developed and refined.
- Benefits of Developing an ERM Framework:
  - Remain competitive in today's dynamic environment;
  - Build sustainable earnings and capital accumulation; and
  - Ultimately, maintain high ratings.

Source: 9
ERM for Companies with a More Limited Operating Scope

- Companies with a more limited operating scope focus on more stable, traditional lines of business.
- An insurer with a more limited operating scope can:
  - Foster a risk-aware culture;
  - Improve its ability to consistently identify, monitor, and manage risk on a quantitative basis; and
  - Consider the impact of risk correlation within its business model

*Source: 9*
Impact of Volatility on Ratings

- From a ratings perspective, it is crucial to understand the historic and potential volatility the insurer's balance sheet is exposed to and the drivers of volatility.
- Companies should not be compelled to eliminate risk and volatility, but understand and manage the risk profile.
- The right balance can be:
  - Reducing volatility through measures such as the purchase of reinsurance, changes in business mix or the refinement of liability characteristics; or
  - Accepting the current level of volatility and focusing on boosting returns through price actions, expense reductions, changes to reinsurance or business mix.

Source: 9
Characteristics of Strong Economic Capital Models

- Address correlations within and across the five risk categories, incorporating reasonably conservative assumptions on positive correlations.
- Contemplate increased correlations with larger events.
- Show volatility in results.
- Reflect the benefits of diversification.
- Reflect the dangers of concentration.
- Reflect the macro economy.
- Reflect the stages of the underwriting cycle.
- Can reflect changing reinsurance environment.
- Can accept deterministic scenarios for testing.

*Source: 9*
Characteristics of Strong Economic Capital Models (continued)

- Provide sufficient data to explain extreme events.
- Parameters fit company data well.
- Parameters updated/reviewed regularly.
- Staff dedicated to the EC model.
- Quality of input data reviewed/audited/tested.
- Model output easy to read/understand.
- Results can be tied to objectives and/or probability of default.
- Produce cash-flow projections for each scenario.
- Model has tested well against historical adverse events.
- Can produce volatilities over different time frames.

Source: 9
Sources

1. IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management, January 2009
2. The IIARF White Paper – March 2011, Internal Auditing’s Role in Risk Management
3. COSO Effective Enterprise Risk Oversight, The Role of the Board of Directors, 2009
4. COSO Board Risk Oversight: A Progress Report, December 2010
5. The role and construction of risk committees; John C. Partigan & Daniel McAvoy, August 11, 2010
6. The Evolving Role of the CRO, Economic Intelligence Unit 2005 & The Chief Risk Officers are Coming, Lloyd’s July 2009
Sources (continued)


Compliance In The Courtroom

- Substantive Liability and Defenses
- Class Actions
- Market Conduct Examination Reports
Liability and Defenses

• At the heart of many lawsuits
  – Policy and waiver forms, required coverage and coverage limits, sales practices, claim administration practices
  – State unfair practices acts

• Compliance negates liability
Liability and Defenses

• Effective and meaningful compliance process can minimize liability even in individual instances of non-compliance
  – Exemplary damages
  – Statutory penalties
  – Fee shifting
Class Actions

• Sales Practices
  – Siding and Insulation Co. v. Combined Ins. Group, Ltd. (N.D. Ohio 2012) (certifying class based on mass faxing of automobile insurance advertisements in violation of the Telephone Consumer Protection Act)

• Policies and Forms

• Claims Administration Practices
  – Bulmash v. Travelers Indem. Co. (D. Md. 2009) (certifying class claiming entitlement to statutory interest for untimely PIP claims)
Market Conduct Reports

- May be discoverable from an insurer
  - Maple Creek Commons Homeowners Assoc. v. State Farm Fire and Cas. Co. (S.D. Ind. 2012) (insurer compelled to produce draft examination report that was never finalized; relevant to bad faith claim); PHL Variable Ins. Co. v. Sheldon Hathaway Family Ins. Trust (D. Utah 2012) (insurer compelled to produce all market conduct examinations for a six year period; relevant to insurer’s business practices)
  - May be privileged in some states
    - Rowe v. Bankers Life and Cas. Co. (N.D. Ill. 2011) (privileged under CA law)
- May not be admissible to prove compliance
  - Royal Marco Point I Condominium Assoc. v. QBE Ins. Corp. M.D. Fla. 2011)
Pennsylvania CLE Credit

Please submit your PA Bar I.D. number to Chris Lautenbacher at clautenbacher@saul.com to receive 1.5 Pennsylvania CLE credits for your participation. Our logs must show that you logged in and stayed logged in for the duration of the presentation.
New York and New Jersey CLE Credit

Pennsylvania credit is recognized and accepted by New York and New Jersey. If you would like to receive credit, email Chris Lautenbacher at clautenbacher@saul.com to receive a Certificate of Attendance verifying your participation in today’s webinar.
Presentation Materials

- **Print**: Right click anywhere on presentation and select “print to PDF.”

- **Download**: Click on “Handout” button at top right (three pieces of paper together). Click on name of presentation and proceed to download.
DISCLAIMER

The content of this webinar and the presentation materials have been prepared by Saul Ewing for information purposes only. The provision and receipt of the information in this webinar and the presentation materials should not be considered legal advice, does not create a lawyer-client relationship, and should not be acted on without seeking professional counsel who have been informed of the specific facts. Should you wish to contact a presenter to obtain more information regarding your company's particular circumstances, it may be necessary to enter into an attorney/client relationship.
## CONTACT INFORMATION

<table>
<thead>
<tr>
<th>Name</th>
<th>Firm</th>
<th>Address 1</th>
<th>Address 2</th>
<th>City, State, Zip</th>
<th>Phone</th>
<th>Fax</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>M. Paige Berry, Esq.</td>
<td>Saul Ewing LLP</td>
<td>750 College Road East, Suite 100</td>
<td>Centre Square West, 1500 Market Street, 38th Floor</td>
<td>Princeton, NJ 08540</td>
<td>609.452.3138</td>
<td>609.452.6112</td>
<td><a href="mailto:pberry@saul.com">pberry@saul.com</a></td>
</tr>
<tr>
<td>Paul M. Hummer, Esq.</td>
<td>Saul Ewing LLP</td>
<td>Centre Square West</td>
<td>Philadelphia, PA 19102</td>
<td>215.972.7788</td>
<td></td>
<td></td>
<td><a href="mailto:phummer@saul.com">phummer@saul.com</a></td>
</tr>
<tr>
<td>Frederick J. Kohm, Jr.</td>
<td>Grant Thornton LLP</td>
<td>2001 Market Street, Suite 3100</td>
<td>Philadelphia, PA 19103</td>
<td>215.561.1066</td>
<td></td>
<td></td>
<td><a href="mailto:frederick.kohm@us.gt.com">frederick.kohm@us.gt.com</a></td>
</tr>
<tr>
<td>Frederick J. Kohm, Jr.</td>
<td>Grant Thornton LLP</td>
<td>2001 Market Street</td>
<td>Philadelphia, PA 19103</td>
<td>215.561.1066</td>
<td></td>
<td></td>
<td><a href="mailto:frederick.kohm@us.gt.com">frederick.kohm@us.gt.com</a></td>
</tr>
</tbody>
</table>