CRO Roundtable for Mid-sized Life Insurance Companies
Nov. 29, 2016
Rosemont, IL

Three Lines of Accountability

Brent Mardis

Sponsored by

- AM Best
- Society of Actuaries
- Willis Towers Watson
Active participation in the Society of Actuaries is an important aspect of membership. However, any Society activity that arguably could be perceived as a restraint of trade exposes the SOA and its members to antitrust risk. Accordingly, meeting participants should refrain from any discussion which may provide the basis for an inference that they agreed to take any action relating to prices, services, production, allocation of markets or any other matter having a market effect. These discussions should be avoided both at official SOA meetings and informal gatherings and activities. In addition, meeting participants should be sensitive to other matters that may raise particular antitrust concern: membership restrictions, codes of ethics or other forms of self-regulation, product standardization or certification. The following are guidelines that should be followed at all SOA meetings, informal gatherings and activities:

- **DON’T** discuss your own, your firm’s, or others’ prices or fees for service, or anything that might affect prices or fees, such as costs, discounts, terms of sale, or profit margins.
- **DON’T** stay at a meeting where any such price talk occurs.
- **DON’T** make public announcements or statements about your own or your firm’s prices or fees, or those of competitors, at any SOA meeting or activity.
- **DON’T** talk about what other entities or their members or employees plan to do in particular geographic or product markets or with particular customers.
- **DON’T** speak or act on behalf of the SOA or any of its committees unless specifically authorized to do so.
- **DO** alert SOA staff or legal counsel about any concerns regarding proposed statements to be made by the association on behalf of a committee or section.
- **DO** consult with your own legal counsel or the SOA before raising any matter or making any statement that you think may involve competitively sensitive information.
- **DO** be alert to improper activities, and don’t participate if you think something is improper.

- If you have specific questions, seek guidance from your own legal counsel or from the SOA’s Executive Director or legal counsel.
Presentation Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the participants individually and, unless expressly stated to the contrary, are not the opinion or position of the Society of Actuaries, its cosponsors or its committees. The Society of Actuaries does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented. Attendees should note that the sessions are audio-recorded and may be published in various media, including print, audio and video formats without further notice.
Three Lines of Accountability

CRO Roundtable November 2016

Brent Mardis
Vice President & Chief Risk Officer
<table>
<thead>
<tr>
<th>First Line - Business Units</th>
<th>Second Line – Control Functions</th>
<th>Third Line – Internal Audit</th>
<th>External Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Five Different Business Units</td>
<td>ERM and other Control Functions (Compliance, IT Risk)</td>
<td>Independent review of business.</td>
<td>Sammons Enterprises Inc. – holding company</td>
</tr>
<tr>
<td>Business Units have primary risk &amp; control ownership responsibilities</td>
<td>ERM and other second line functions have standard setting, oversight, and reporting responsibilities for overall enterprise risk appetite and risk limits.</td>
<td>Assurance concerning the controls, policies, procedures, processes, and practices. Operates independently from the business.</td>
<td>Regulators and rating agencies.</td>
</tr>
<tr>
<td>Accountable for identifying, prioritizing and mitigating all risks</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Three Lines - Roles

<table>
<thead>
<tr>
<th>First Line of Accountability</th>
<th>Second Line of Accountability</th>
<th>Third Line of Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Functions – Take, Own, &amp; Manage Risk</td>
<td>ERM Committees, IT Risk Subcommittee, Compliance</td>
<td>Internal Audit</td>
</tr>
<tr>
<td>Responsible for managing risks; including identifying, measuring, monitoring, reporting, and escalating up to second line Committees</td>
<td>Provide support &amp; effective “challenge” to first line</td>
<td>Validate: responsible for providing independent assurance</td>
</tr>
<tr>
<td>Measure &amp; monitor through self assessments</td>
<td>Direct action to mitigate, monitor overall risk taxonomy, identify trends</td>
<td>Conduct independent testing of controls</td>
</tr>
<tr>
<td></td>
<td>Report to Executive ERM Committee, Board</td>
<td></td>
</tr>
</tbody>
</table>

Confidential. For Internal Use Only.
ERM at Sammons

- ERM program established in 2006, CRO in place for seven years
- Developed in response to rating agency comments
- Continuous monitoring and enhancing in line with changing regulations (ORSA) and rating agency guidance
- ERM Committee structure in place
- Recently added monthly Executive Committee Level Risk & Compliance meeting
- Recently added Board Level Risk & Compliance Committee
ERM Committee Overview

- Seven total Risk Committees (Executive ERM Committee, six functional committees)
- 80 total employees involved with ERM Committees
- Committee membership combination of first and second line employees (all committees have at least one advisory member from both Legal/Compliance and Internal Audit)
- Added a handful of risk sub-committees over past two years
- Committees meet monthly or quarterly, metrics reviewed anywhere from monthly to annually
Future Enhancements to Three Lines

- Adoption of common set of language between Audit, Risk, and Compliance; including enhancements to enterprise risk taxonomy
- Increased collaboration between Audit, Risk, and Compliance
- Enhanced training to all levels of the organization. Drive home concept of Three Lines of Accountability. Address roles and responsibilities of each line. Utilize manager meetings and in-house training platform.
- Development of quarterly newsletter, in collaboration with our IT Risk area