INTEGRATED Governance, Risk and Compliance:

What is it?
How is it different?
Why companies need it to protect investors.

Jim Gurowka
Institute of Management Accountants

March 2009
Highlights

• You need to build quality in. Inspection at the end of the process is too late and not enough.

• Show me a measurement and compensation system and I will predict behaviour.

• An integrated approach to governance is required in order to be successful.

• Certified accounting and finance professionals will help to ensure accurate and “useful” internal and external reporting. The Certified Management Accountant (CMA) program is designed for those working inside organizations.
There is not much trust in finance these days
Investment Advisors Cannot be Trusted
January 2008 – Northern Rock Collapses

“The Financial Services Authority (FSA) should not have allowed nor ever again allow the two appointments of a chairman and a chief executive to a "high-impact" financial institution where both candidates lack relevant financial qualifications.

The FSA should undertake an urgent review of the current qualifications of senior directors in financial firms, especially of those firms considered to be "high-impact", and ensure that the current approved person regime requirements are adequate.”
Are Accountants to Blame?

MP George Mudie vs Brendan Nelson, Global Chairman of KPMG’s Financial Services Practice

28 January 2009

Mudie: Brendan, if you were watching this on television and you had lost your job, you were going to lose your house, you would be pretty bloody angry at the auditors for allowing the banks to get away with all the off balance sheet derivatives, the lot. As you go in and audit them the ordinary person would say "Why the ... didn't the auditor pick it up?" In an intelligent discussion you are saying to me "Well, it is not our business." Will it be your business in future or will there need to be discussions and changes, maybe even changes in the law? Have you started those?

Nelson: Those discussions clearly will take place with the Auditing Practices Board, the International Accounting Standards Board, the Financial Reporting Council in terms of the role of the auditor going forward, but I really do want to come back to this point about the fact ----
Are Boards to blame? – Senior executives may be in jobs they’re not qualified to do

James Cayne, Former CEO, Bear Stearns – Harvard lawyer
Angelo Mozilo, Former Countrywide Financial CEO – BS in Marketing & Philosophy
Dick Fuld, CEO, Lehman Brothers - MBA
Erin Callan, Ousted Lehman CFO – Tax Attorney
Martin Sullivan, CEO, AIG – High school diploma
Franklin Raines, former Chairman/CEO, Fannie Mae – Harvard lawyer
Chuck Prince, Former CEO, Citigroup - Lawyer
Christopher Cox, 28th Chairman of the SEC - Joint Harvard MBA & JD
Who can you trust. Financial Restatements: Is a 10%-13% Error Rate Acceptable?? (source: Audit Analytics)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Accelerated Filers (AF), Foreign</td>
<td>2</td>
<td>15</td>
<td>33</td>
<td>29</td>
<td>58</td>
<td>46</td>
<td>465</td>
<td>9.9%</td>
</tr>
<tr>
<td>Non-AF, Foreign</td>
<td>26</td>
<td>38</td>
<td>73</td>
<td>75</td>
<td>143</td>
<td>210</td>
<td>2113</td>
<td>9.9%</td>
</tr>
<tr>
<td>Large AF U.S. &gt; $750M market cap (subset)</td>
<td>46</td>
<td>77</td>
<td>120</td>
<td>154</td>
<td>242</td>
<td>196</td>
<td>1963</td>
<td>10.0%</td>
</tr>
<tr>
<td>All AF, U.S. &gt;$75M market cap</td>
<td>138</td>
<td>177</td>
<td>314</td>
<td>404</td>
<td>620</td>
<td>512</td>
<td>3861</td>
<td>13.3%</td>
</tr>
<tr>
<td>Non-AF, U.S. &lt; $75M market cap</td>
<td>286</td>
<td>355</td>
<td>491</td>
<td>510</td>
<td>778</td>
<td>1108</td>
<td>11986</td>
<td>9.2%</td>
</tr>
</tbody>
</table>
Part of the answer – a new view of risk

<table>
<thead>
<tr>
<th>Old Paradigm</th>
<th>New Paradigm</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Historically focused</td>
<td>• Strategic</td>
</tr>
<tr>
<td>• Ad hoc activity</td>
<td>• Continuous activity</td>
</tr>
<tr>
<td>• Accounting, treasury and internal audit</td>
<td>• All of management</td>
</tr>
<tr>
<td>• Fragmentation (Silo Approach)</td>
<td>• Focused and coordinated (Holistic)</td>
</tr>
<tr>
<td>• Financial risk</td>
<td>• Business risks</td>
</tr>
<tr>
<td>• Inspect, detect, react</td>
<td>• Anticipate, prevent, monitor</td>
</tr>
<tr>
<td>• Focus on people</td>
<td>• Focus on processes and people</td>
</tr>
</tbody>
</table>

The Economist Intelligence Unit, *Managing Business Risk*, p. 10
The Answer - Governance, Risk and Compliance.

GRC in Everyday Life
G - GOVERNANCE

SIMPLY PUT

Governance is fundamentally about how an organization is run by the people in charge. Some companies have "good" corporate governance and others have "bad" corporate governance. Most companies are somewhere in the middle with a mix of “good” and “bad”.
R – RISK MANAGEMENT

SIMPLY PUT

Risk management is fundamentally about identifying and considering events or situations that could impact on the achievement of objectives and asking whether the organization's position, after considering what has been done so far to manage or "treat" those risks, is tolerable and appropriate given the organization's appetite for risk.
C – COMPLIANCE

SIMPLY PUT

Compliance in business is about ensuring external laws and regulations and internal policy directives are being complied with at a level consistent with corporate morality and risk tolerance.
The good news. There are resources available to help you

- SOCPA
- COSO
- IMA
- IFAC
- XBRL International
- ACCA and other accounting associations focused on the entire accounting supply chain.
IMA FGRC Resources – Available for free

✓ SMAs (Statements on Management Accounting) on Enterprise Risk Management.
✓ Research studies, global discussion papers, comment letters filed with SEC and PCAOB, Congressional testimony.
✓ Webinars (live and for re-broadcast), conferences, Strategic Finance articles.
✓ New FGRC Research Advisory Committee formed – Global members being sought!!
✓ Visit www.imanet.org/fgrc for current FGRC resources
About the Institute of Management Accountants

- IMA founded in 1919 as a not-for-profit.

- **Mission**: To provide a dynamic forum for management accounting and finance professionals to develop and advance their careers through certification, research and practice development, education, networking, and advocacy of the highest ethical and professional practices.

- **Certification**: Certified Management Accountant (CMA®).

- **Global Reach**: Members in over 125 countries.

- **Research Practices**: Leadership Strategies & Ethics; Strategic Cost Management; Business Performance Management; Technology Enablement; and, (NEW) Finance GRC (Governance, Risk and Compliance).
About COSO (Committee of Sponsoring Organizations)

1987: Treadway Commission Report


1992: Internal Control

1998: Fraud Study Financial Reporting

2004: Enterprise Risk Management

2006: Guidance for Smaller Businesses

2008: Fraudulent Financial Reporting

2008: Monitoring
GRC and Strategy: Two Sides of the Same Coin

“Strategy that lacks alignment to risk management is not only insufficient but downright dangerous...Risk management is pointless unless it is closely tied to the company’s strategic objectives.”

T. Nagumo, *Balanced Scorecard Report*  
(Sept.-Oct. 2005)
The ERM Framework

- Internal Environment
  - Objective Setting
  - Event Identification
  - Risk Assessment
  - Risk Response
  - Control Activities
  - Information & Communication
  - Monitoring
C – COMPLIANCE

COMPLIANCE = GOVERNMENT INTERVENTION – GOOD AND BAD

PROPOSED PRIVATE TREE BY-LAW – City in New Jersey

Permit required to prune or cut:

1. Any tree greater than 12 inches in diameter or greater
2. On a heritage lot for trees 6 inches in diameter or greater
3. On any lot if it involves 4 or more trees 6 inches in diameter or greater
C – COMPLIANCE

- Total cost of U.S. regulation in 2005 estimated at $1.27 trillion
- Total cost of U.S. regulation in 2005 estimated at $4,680 per man, women, and child
- Other countries have similar or even higher regulatory burdens
- Good regulation protects society but bad regulation cripples and hurts society.
IMA's Risk Based Approach: The Heart of our FGRC PD Program

Assurance Context
(self determined or mandated)

Threats to Achievement/Risks
Control Portfolio - the controls selected:

(Consciously or unconsciously)

Residual Risk Status

Re-examine control design and/or assurance context and develop an action plan.

Risk Sharing/Avoidance

Acceptable?

YES

Portfolio Optimized?

YES - Move On

NO

Information that helps decision makers assess the acceptability of residual risk. Status data can include issues/concerns, indicator data, impact information, impediments, risk sharing mechanisms and other relevant data.

The outcome, objective, process or subject one or more stakeholders want some type of formalized assurance on.

These are possible problems or situations that could threaten the assurance context.

Controls are methods, procedures, equipment or other things that provide additional assurance relevant risks are mitigated to an acceptable level.

Is the residual risk status acceptable to the work unit? Management? The board? External audit? Regulators? Other stakeholders?

Is this the lowest cost set of controls given our risk tolerance?
Questions
Part of the Answer - Criticality of Internal Controls/Risk Management (IC/RM)

• “Good” IC/RM generally means
  – Greater investor/stakeholder protections, trust and confidence
  – Lower cost of capital for the organization
  – Higher value creation potential for the organization
  – Fewer # of material financial restatements
  – Fewer errors and lower “cost of rework”
  – Ability to dynamically address environmental changes
  – Staying out of jail!!
Criticality of Internal Controls/Risk Management (IC/RM)

• “Bad” IC/RM generally means
  – Lower investor/stakeholder protections, trust and confidence
  – Higher cost of capital for the organization
  – Lower value creation potential for the organization
  – Higher # of material financial restatements
  – More errors and higher “cost of rework”
  – Reactive approach to environmental changes
  – Higher reputation risk/damage and if you commit fraud, possible jail time!!
R – RISK MANAGEMENT

COSO ERM

"a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"