IT Governance, Risk and Compliance (GRC) : A Strategic Priority

Joerg Asma
Agenda

- Introductions
- An Overview of IT Governance Risk & Compliance (IT-GRC)
- The Value Proposition
- Implementing an IT-GRC Program
- Market Landscape
- Open Discussion
- Closing Remarks
Introductions
An Overview of IT-Governance
Risk & Compliance
Background to Governance, Risk and Compliance

• There have been many forms of GRC over the years: corporate governance, IT governance, financial risk, strategic risk, operational risk, IT risk, corporate compliance, Sarbanes-Oxley (SOX) compliance, employment/labor compliance, and privacy compliance.

• The introduction of Sarbanes Oxley Sec 404 (SOX 404) has driven an enterprise approach to establish more effective Corporate Governance.

• Insurance companies over the last several years have influenced the enterprise risk management (ERM) initiative which was also further supported by SOX 404.

• There has been an increase in the number of GRC related software solutions coming to the market that is converging a number of initiatives.
An Overview of IT-GRC

**Best Practices**
- Defines policies, standards and processes based on industry best practices and needs of your organization.

**Business Alignment**
- IT is enabling business to meet their goals.

**Regulatory Landscape**
- Takes into account International, Federal, State, Local, etc. mandates that your organization must comply with.

**Measurement of Controls**
- Defines a common criteria for measuring controls across various groups within your organization to ensure uniform measurement during assessments.

**Value Capture**
- Provides a source of cost savings through realized synergies, such as consolidation and rationalization of applications, functions and assets.

**Resource Management**
- Effective resource allocation and appropriate skill set alignment.

**Risk Management**
- Defines Key Risk Indicators based on your unique environment, risk tolerance and key assets. Real time risk evaluation of non-compliance.

**Benefits Metrics and Reporting**
- Communicate track record of achievements to business users and ensure continuous improvement.

**Communicate track record of achievements to business users and ensure continuous improvement.**
The Value Proposition
Value Proposition

- **SUSTAINABLE** – Risk and Compliance Activities will not be going away. Compliance Officers need on-going visibility into the changing landscape.
- **CONSISTENT** – in an era of increased accountability, firms cannot afford to NOT consistently understand, approach and measure risks and controls
- **EFFICIENT** – Automation of risk and compliance processes resulting in reduction of Security and Compliance Management Costs
- **TRANSPARENT** – need transparency into business operations and strategies to help navigate around threats and seize opportunities.
- Enterprise-Wide GRC Solutions assist in sustaining GRC Programs
Market Trends: Top Business Benefits of Compliance

- Streamlining Business Processes: 36%
- Improved Quality Survey Responses & Data Provided: 28%
- Enhanced Information Security: 14%
- Supply Globilization Efforts: 11%
- Improved Operational Visibility: 10%
- Other: 1%

Source of Survey - AMR Research
Implementing an IT-GRC Program
Architectural Overview

Unified IT Risk & Compliance Management
- IT Risk
  - Prioritize Investments
- Compliance & Audit Reports
- IT Operations
  - Prioritize Mitigation

Core Server Functions
- Policy Management
- Control Testing & Gap Analysis
- Risk Analysis & Correlation

Common Control Framework
- SOX
- GLBA
- PCI
- FISMA
- ISO
- Custom
- Control Set

Asset Info
- Reconciled Asset Information

E-Data Gathering
- E-Surveys
  - Manual Surveys
  - Facilities
  - Processes
  - People

Connectors
- Scanners, SIM/SEM, Directory, CMDB
  - Laptops
  - Servers
  - Databases
  - Applications

Customer Assets & Processes
- Policies & Mandates
- Frameworks
- Controls
## Common Control Framework

### Question: What IT Governance frameworks/solutions do you use or are you considering using?

Source: IT Governance Institute - Global Status Report 2008

<table>
<thead>
<tr>
<th>Framework/Approach</th>
<th>2007</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITIL/ISO 20000</td>
<td>13%</td>
<td>16%</td>
</tr>
<tr>
<td>ISO 9000</td>
<td>14%</td>
<td>16%</td>
</tr>
<tr>
<td>Internally developed framework</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>COBIT/COBIT Quickstart</td>
<td>9%</td>
<td>14%</td>
</tr>
<tr>
<td>ISO 17799/ISO 27000/ISO TR13335/ISF or equivalent security standard</td>
<td>6%</td>
<td>10%</td>
</tr>
<tr>
<td>Other international professional organisation's solution</td>
<td>17%</td>
<td>9%</td>
</tr>
<tr>
<td>Software Engineering Institute Maturity Model (CMM &amp; CMMI)</td>
<td>7%</td>
<td>14%</td>
</tr>
<tr>
<td>IT Balanced Scorecard (BSC)</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Internally developed framework, but based on one or more of the above</td>
<td>7%</td>
<td>3%</td>
</tr>
<tr>
<td>Local (national) professional organisations' solution</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>Not yet decided which one</td>
<td></td>
<td>22%</td>
</tr>
<tr>
<td>Six Sigma</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>PRINCE 2</td>
<td>0%</td>
<td>2%</td>
</tr>
<tr>
<td>COSO ERM</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>PMI, PMBOK</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>TOGAF</td>
<td>0%</td>
<td>4%</td>
</tr>
<tr>
<td>Val IT</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>SysTrust</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Source: IT Governance Institute - Global Status Report 2008
Approach to Developing an IT-GRC Program

Scope Assets
- Intelligent Profiling
- People
- Processes
- IT Infrastructure
- Applications
- Buildings
- Partners
- Vendors

Identify Threats & Vulnerabilities

Select
- Common Control Framework
- Regulations and Mandates
- Corporate Policy Best Practices
- Standard Frameworks
- Controls and Subcontrols
- Key Risk Indicators

Run
- Automated Processes
- Human Attestation Surveys
- Technical Control Checks
- Security Tool Integration
- Risk & Compliance Scoring

Decide
- Risk based Prioritization
- Risk Rationalized Tickets
- ROI Analysis vs. ALE / SLE
- Ticket Closure Workflow

Act
- Consolidated View
  - Risk & Compliance Process Management
  - Role-Based Dashboards
  - Trending
  - Custom Reports
  - Report Templates:

© 2008 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in the U.S.A. 295485FO
Market Landscape
Overview of the Market

- Moving from Concept to Practice
  - Initially more divisional/group specific
  - Limited enterprise-wide adoption
- GRC Related Spend in 2007 - $30B (according to AMR Research)
  - SOX still accounts for 20% of all overall GRC Spend
- Adoption Rate in embryonic stage
  - Market for vendors offering solutions growing
- The software is NOT the strategy; without a solid governance structure as a foundation no solution will bring about compliance.
- Existing risk, compliance, organizational structure and processes MUST be in place before implementing any solution.
Overview of the Market, continued

Promising

Source: Gartner “MarketScope for IT Governance, Risk and Compliance Management 2008” 2/11/08
Open Discussion
Open Discussion – Four Key Questions

1. Why should my organization implement IT-GRC?
2. What are the pre-requisites my organization needs in place to have the necessary foundation to make IT-GRC successful?
3. Who should own an IT-GRC Program?
4. What are the investment considerations to implement an IT-GRC Solution?
Valuable Reference Websites

- IT Governance Institute – [www.itgi.org](http://www.itgi.org)
- The Institute of Internal Auditors (IIA) – [www.theiia.org](http://www.theiia.org)
- European Corporate Governance Institute – [www.ecgi.org](http://www.ecgi.org)
Your contact

Jörg Asma
Partner

Barbarossaplatz 1a
50674 Köln
Germany
Office: ++49 221 2073-6233
Mobile: ++49 172 762 0928
E-mail: jasma@kpmg.com