Demystifying GRC

Understanding Governance, Risk Management, and Compliance Programs

Jan. 16, 2013
After This Webinar, You Will Be Able To:

- Define the meaning of GRC and its components
- Differentiate GRC from risk management, compliance, internal control, and internal audit.
- Define the fundamentals of an integrated GRC approach including processes, tools, and the importance of enabling change.
- Create an awareness of software solutions and the criteria needed to help with your software selection.
Agenda

- Today’s Environment
- GRC – “Mystical GRC Claims”
- Evolution of GRC
- Case Studies
- A Framework for Applying GRC to Your Organization
- Software Solutions
- Conclusion: Tailoring GRC for Your Organization
Today’s Environment

Business Partners
- Outsourcing
- Offshoring
- Internet

Customers
- Performance
- Transparency
- Security and Trust

Economies
- Capital
- Cost Containment
- Globalization

Investors
- Performance
- Transparency
- Active Shareowners
- Board pressure

Regulators
- New Legislation and Rules
- Heightened Expectations
- Scrutiny and Transparency

Media and Public
- Accountability
- Transparency
- Security and Trust

Employees
- Development
- Security and Trust
Governance, Risk, and Compliance: The Challenge

- The term “GRC” is not well understood.
- The benefits often are not clearly articulated.
- The perception is that GRC is:
  - A control or administrative function;
  - Reliant on an IT solution; and
  - Often managed in silos:
“Mystical GRC Claims”

- “Enterprise GRC helps organizations gain a greater understanding of their risk position and control environment, enhances the ability to respond to unforeseen events, and ultimately empowers an organization to take advantage of emerging opportunities.”

- “Become empowered with enterprise GRC solutions and incorporate risk management and compliance into your strategy, planning, and operational execution. Leverage GRC as a competitive differentiator and performance optimizer.”

- “We challenge ourselves and our customers to adopt an approach to risk management that enables us to use enterprise risk management (ERM) in the broader context of GRC management: to mitigate risks and also revisit their business processes to capture value generating business opportunities.”

- “Building an ethical and successful business starts with setting the standards for acceptable and unacceptable conduct in your company. You need to drive the behavior you want from your employees, and our enterprise GRC solutions can help.”
The Open Compliance and Ethics Group (OCEG) Definition of “GRC”

- GRC is an acronym describing an integrated approach to the governance, assurance, and management of performance, risk, and compliance.
- GRC enables an organization to reliably achieve objectives while addressing uncertainty and acting with integrity.
- The term "integration" means using the same or similar approaches across silos of interest in a way that allows for a unified view of the information. Some people refer to this as a “harmonized” or “consistent” approach.
The Real Benefits of GRC

**Strategy:**
- Enables the board and executive management to evaluate whether strategy is realistic or unachievable and in need of modifying

**Governance:**
- Alignment of the company's managers, assets, processes, and technology with its strategy
- Consistency of policy, procedure, and standards
- Provides integrated assurance to the board that assets and reputation are protected
- Provides the board with a formal process to exercise its regulatory obligation for oversight

**Performance Management:**
- Results in better decisions about operations, the viability of investments, and preparation for significant unexpected events
- Directs human, financial, and investment capital to the right areas, and the best decisions are made for the enterprise as a whole rather than within boundaries

**Cost:**
- Potential savings from:
  - Reduced losses
  - Improved credit rating and lower cost of capital
  - Lower Insurance premiums
  - Synergies from integration and process improvement
Evolution of GRC:
A Mature Framework – Integrated Management

- Audit
- Tax
- Advisory
- Risk

2013 Crowe Horwath LLP
Case Study #1

- $1 Billion Community Bank
  - 16 branch locations
  - Conservative appetite for risk
  - Varying risk and compliance terminology
  - Strong IT program management

- GRC Activities
  - Identify GRC objectives and purpose.
    - Enable risk discussions.
    - Strengthen board communications.
    - Meet regulatory expectations.
  - Complete top-down risk assessment.
  - Align risk and compliance activities to top-down risk assessment.
  - Balance internal audit and compliance testing with updated risk profile.
  - Link change-management activities to IT activities.
Case Study #2

- $40 Billion Automotive Group
  - More than 100 locations internationally
  - Media scrutiny following suspected fraud
  - Inconsistent policies and procedures
  - Traditional control structure

- GRC Activities
  - Driven by chairman of the board and the Audit Committee
  - Assessment of:
    - Organizational structure and delegation of authority
    - Current governance culture, rules, and decision-making
    - The relevance and efficiency of processes, policy, and frameworks
  - Implementation of the new model sponsored by the board:
    - An updated organization including an integrated Assurance department reporting to the CEO and the Audit Committee
    - Management committees for Risk, Internal Control, and Ethics
    - A revised group risk assessment based on the value chain
Case Study #3

- $30 Billion Food Retailer
  - 12,000 stores worldwide
  - Many entities with different levels of maturity across the world
  - Different approaches to GRC globally (minimalist, compliance-oriented, or enterprisewide-oriented)
  - An integrated corporate group focused mostly on internal audit
  - An Audit Committee that needs integrated reporting of risks and responses

- GRC Activities
  - A significant Information Systems project (monitored by IT) to drive a standardized approach to all components of GRC throughout the group
  - A strong corporate culture resulting in a light change-management strategy for the project
  - Project freeze while designing a coordinated and common model for GRC
Integrated GRC Framework: Governance

- Risk and compliance management must be built on a good governance foundation.
- Governance will determine the sustainability of GRC activities and the enterprise as a whole.
- Governance can be viewed as constituting seven essential and interrelated components.
Integrated GRC Framework: Risk Management and Compliance

- **Strategy**
  - Chosen goals and objectives for the enterprise

- **Risk and Compliance Universe**
  - Identification of rules and risks in achieving strategy

- **Risk Appetite**
  - Set boundaries within the risk universe

- **Risk and Compliance Programs**
  - Design programs to operate within the risk appetite
  - Specific assessments

- **Controls**
  - Monitor risks
  - Monitor compliance

- **Testing and Monitoring**
  - Test controls
  - Monitor controls

The fabric of the organization includes:
- Values
- Culture
- Processes
- Compensation
- Rewards
- Communication
- Change management
Integrated GRC Framework: A Common Language

- An integrated GRC approach requires common frameworks, methodologies, and tools.
- A consistent “toolkit” significantly facilitates decision-making and reduces cost.
# Select GRC Software Solutions (page 1 of 3)

<table>
<thead>
<tr>
<th>Company</th>
<th>Solution/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC</td>
<td><a href="http://www.emc.com/security/rsa-archer">www.emc.com/security/rsa-archer</a> Modular Approach with Strong IT Risk Capabilities</td>
</tr>
<tr>
<td>Enablon</td>
<td><a href="http://www.enablon.com">www.enablon.com</a> Sustainable Supply Chains</td>
</tr>
</tbody>
</table>

*Sources: Gartner GRC Magic Quadrant, Forrester Wave: Enterprise Governance, Risk, and Compliance Platforms, Chartis RiskTech 100*
Select GRC Software Solutions (page 2 of 3)

<table>
<thead>
<tr>
<th>Company</th>
<th>Solution/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetricStream</td>
<td><a href="http://www.metricstream.com">www.metricstream.com</a> Broad capabilities and industry experience, Quality and Supplier Management</td>
</tr>
<tr>
<td>Misys</td>
<td><a href="http://www.misys.com">www.misys.com</a> Banking, Capital Markets, Treasury</td>
</tr>
<tr>
<td>Moodys Analytics</td>
<td><a href="http://www.moodysanalytics.com">www.moodysanalytics.com</a> Capital Analysis, Scenario Analysis, Credit Risk Modeling</td>
</tr>
<tr>
<td>MSCI</td>
<td><a href="http://www.mcsi.com">www.mcsi.com</a> Analytics, Credit Risk, Portfolio Management</td>
</tr>
<tr>
<td>Oracle</td>
<td><a href="http://www.oracle.com/us/solutions/corporate-governance/overview">www.oracle.com/us/solutions/corporate-governance/overview</a> Broad, Integration of Controls Monitoring</td>
</tr>
<tr>
<td>Protiviti</td>
<td><a href="http://www.protiviti.com/grc-software">www.protiviti.com/grc-software</a> ERM, Internal Audit, Compliance, Financial Controls, Information Technology</td>
</tr>
</tbody>
</table>

*Sources: Gartner GRC Magic Quadrant, Forrester Wave: Enterprise Governance, Risk, and Compliance Platforms, Chartis RiskTech 100*
## Select GRC Software Solutions (page 3 of 3)

<table>
<thead>
<tr>
<th>Company</th>
<th>Solution/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAI Global</td>
<td><a href="http://www.compliance360.com">www.compliance360.com</a> Compliance 360, Healthcare, Insurance, Financial Services, Software as a Service</td>
</tr>
</tbody>
</table>

*Sources: Gartner GRC Magic Quadrant, Forrester Wave: Enterprise Governance, Risk, and Compliance Platforms, Chartis RiskTech 100*
Technical Criteria for Making the Right Choice

- **GRC Maturity**
  - Now and in the future
  - Time and budget

- **Functionality Requirements**
  - Risk identification and assessment
  - Regulatory knowledge
  - Risk modeling
  - Dashboards and reporting
  - Self-assessments
  - Workflow
  - Internal controls
  - Internal audit
  - Issue and case management
  - Department/function management

- **Software Genealogy**
  - Audit, risk management, compliance, legal, strategy, fraud

- **Industry Relevance**
  - Financial services, healthcare, government, pharmaceuticals, telecommunications and media

- **Configuration Needs**
  - Number and scope of users, security, integration requirements, compatibility, system impact, maintenance, scalability
Tailoring GRC to Your Organization

**Why** do you want to improve GRC?
- What are the drivers and anticipated benefits?
- How will you articulate this to others?
- Is senior management on board?

**How** will you formalize your program?
- Governance structure
- ERM, compliance, internal audit...

**What** is the scope?
- What can you leverage?
- Where to pilot and how to phase?
- Which technology and software?

**Who** will take which responsibility?
- CEO, CFO, GC, CAE, other senior managers
- Board members
- Business managers, risk, compliance, and other managers

**When** is the best time to:
- Identify your risk universe?
- Assess strategic risks and allocate resources to respond?
- Monitor and report to stakeholders, including the board?
Conclusion

- There is no definitive standard for GRC.
- It’s all about governance!
- A common language, coordination, and integration drive value.
- Before implementing:
  - Know your organization’s maturity.
  - Know why your organization will benefit.
  - Know how each component will work.
- IT is an enabler, not the answer.
- Enabling change will determine the program’s success.
Questions?
For more information, contact:

Gregg Anderson, Crowe Horwath LLP
Direct +1 630.586.5142
Gregg.Anderson@crowehorwath.com
www.linkedin.com/in/gregarkeanderson

Jonathan Burnett, Crowe Horwath Global Risk Consulting
Direct +33 1.53.53.03.92
Jonathan.Burnett@crowehorwathgrc.net