



Governance, Risk and Compliance

North Texas ISACA March Luncheon

March 11, 2010



Agenda

- Introduction to GRC and the current challenge
- GRC Tools Market
- EY Observations and Thoughts

Defining GRC

What are the needs?

- ▶ Stakeholders increasingly require a measurable and documented enterprise commitment to transparency and compliance
- ▶ Difficulty or failure to respond to changing regulatory requirements
- ▶ Need to streamline risk and controls convergence process
- ▶ Inconsistent measurement of risk with no common taxonomy for compliance initiatives
- ▶ Inefficient assessment process and evidence management
- ▶ Disparate risk management functions cause inefficiency and confusion
- ▶ Moving to a combined approach to risk / compliance and performance improvement
- ▶ Require preventative and continuous protection against fraud and a host of operational risks

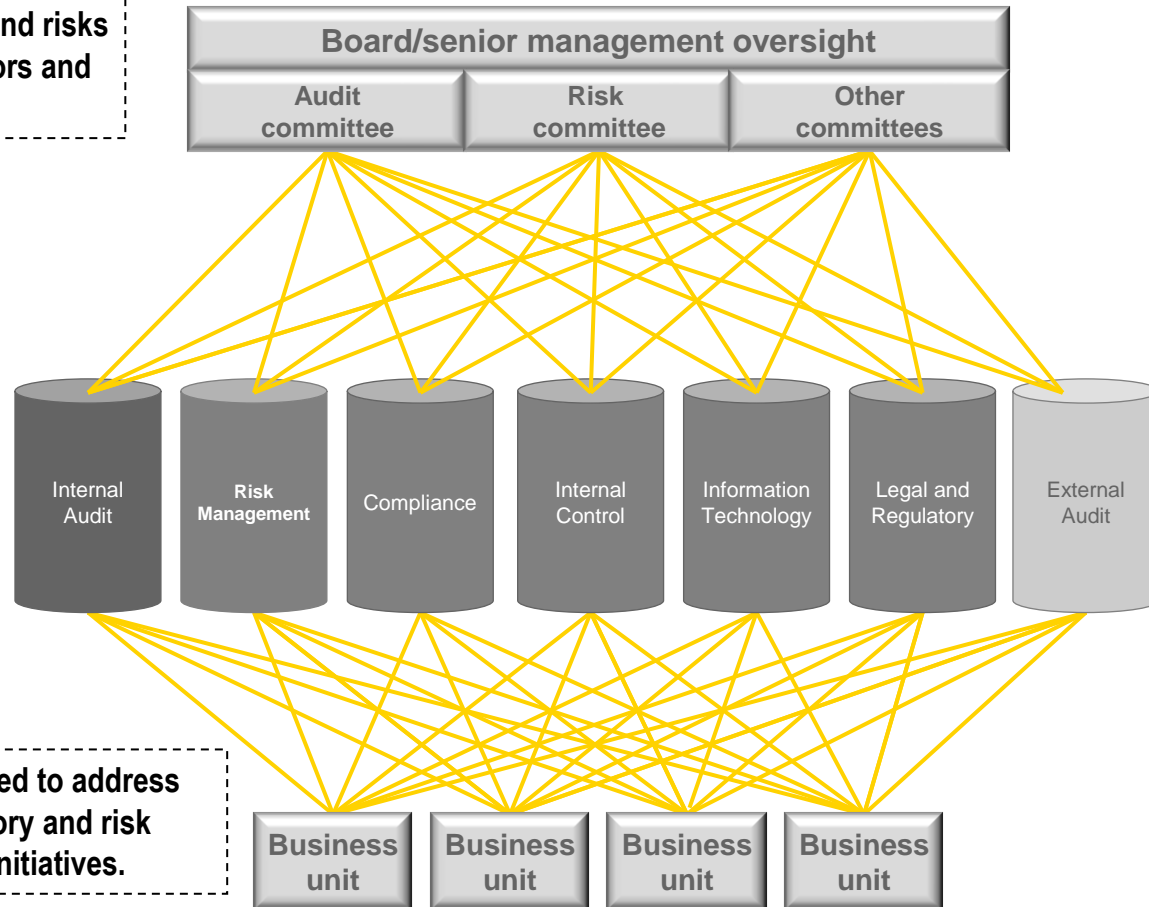
Defining GRC

The current challenge

Inconsistent views of business and risks reported to the Board of Directors and senior management

Different Concepts and definitions of risks and controls

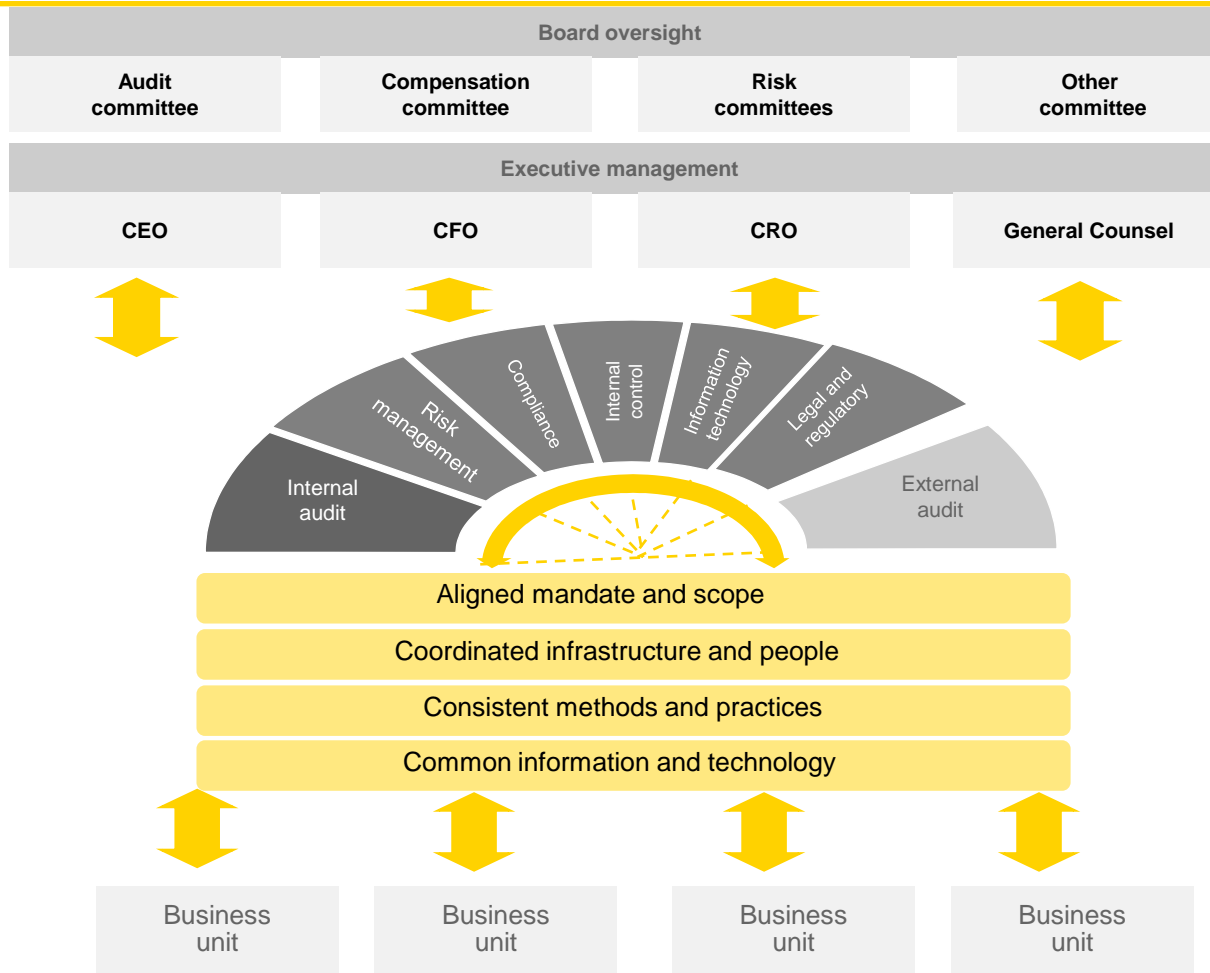
Businesses required to address multiple regulatory and risk management initiatives.



Siloed risk functions reduce value, increase costs, and impact business performance

Defining GRC

The desired future state



*Clearly Defined Responsibilities
Clear and comprehensive risk reporting*

*Opportunity to Leverage/
Coordinate with other control functions*

Foundations of Convergence

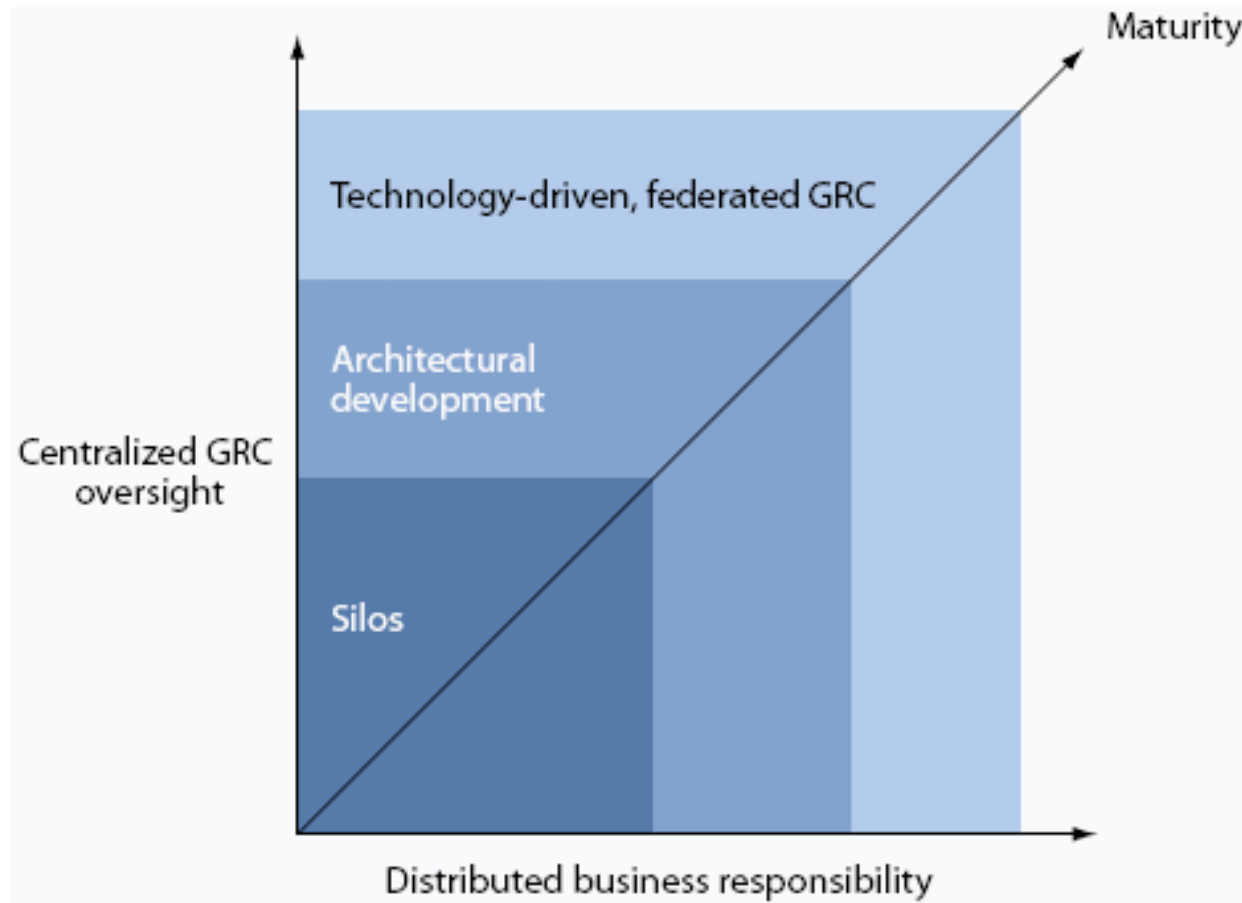
Efficiency and Effectiveness

Risk management convergence

Defining GRC

GRC program maturity

“GRC solutions must be **Sustainable, Consistent, Efficient** and **Transparent**”



Source: Forrester

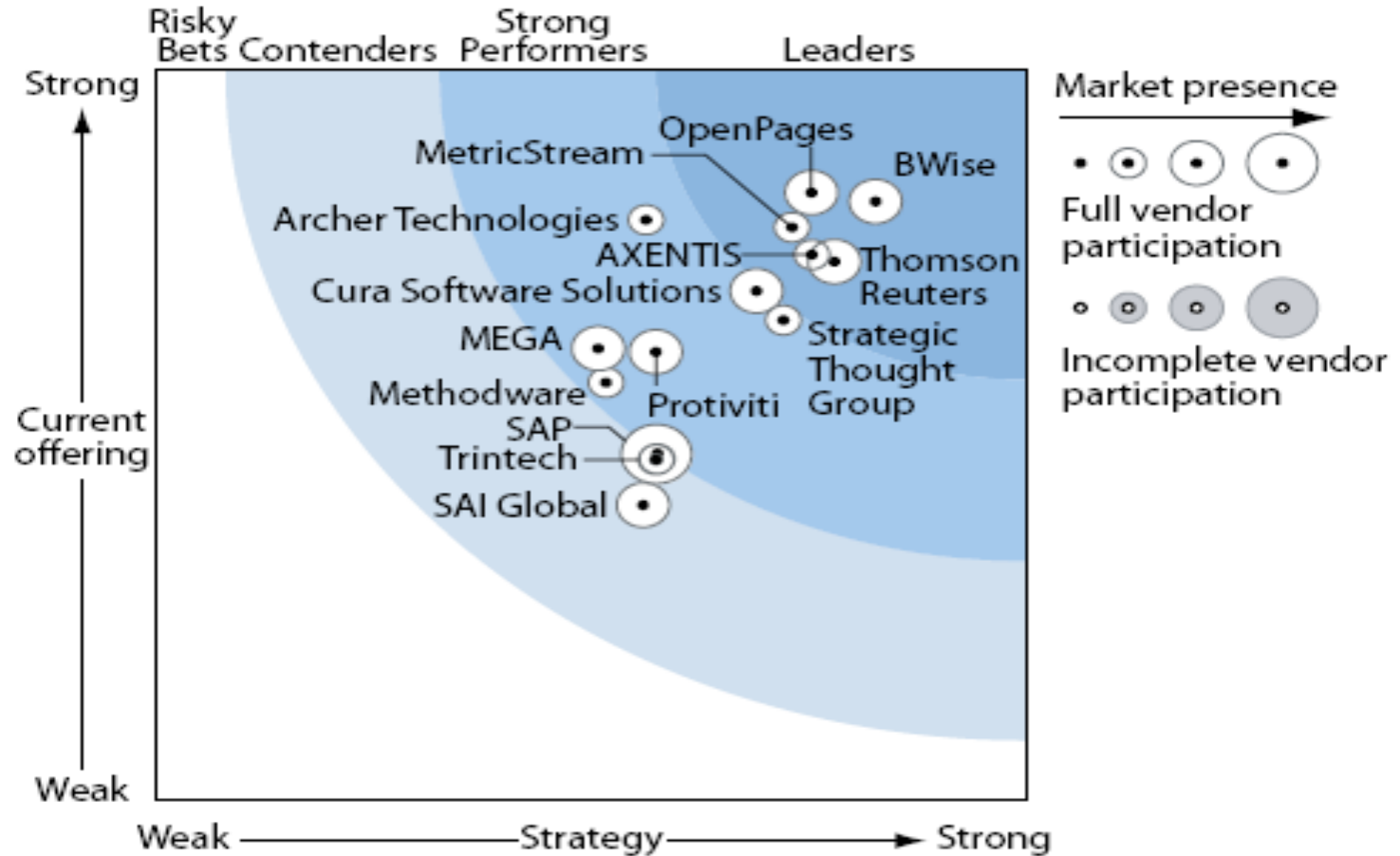
GRC Tools

Key trends

- ▶ Continued evolution and broader use of technology for GRC
- ▶ Entrance of technology “heavyweights” into GRC market (ie, EMC, SAP, Oracle, etc)
- ▶ Integration of Web Services to enable risk and regulatory intelligence
- ▶ Implementation of a central corporate policy management portal
- ▶ Use of business process management and rules engines along with continuous auditing, monitoring, and control testing
- ▶ Vendors are not yet able to bridge all aspects of GRC holistically in terms of processes and technologies. There is no single package that can do it all.
- ▶ Many of the systems currently in use were developed for a specific function’s or sector’s needs. These vendors are challenged with finding alternative uses for their applications.
- ▶ GRC vendors are developing relationships with other application vendors (competitors and complementary products) to extend the range of the software. Others have been acquired to combine product offerings into larger, more comprehensive packages.

GRC Tools

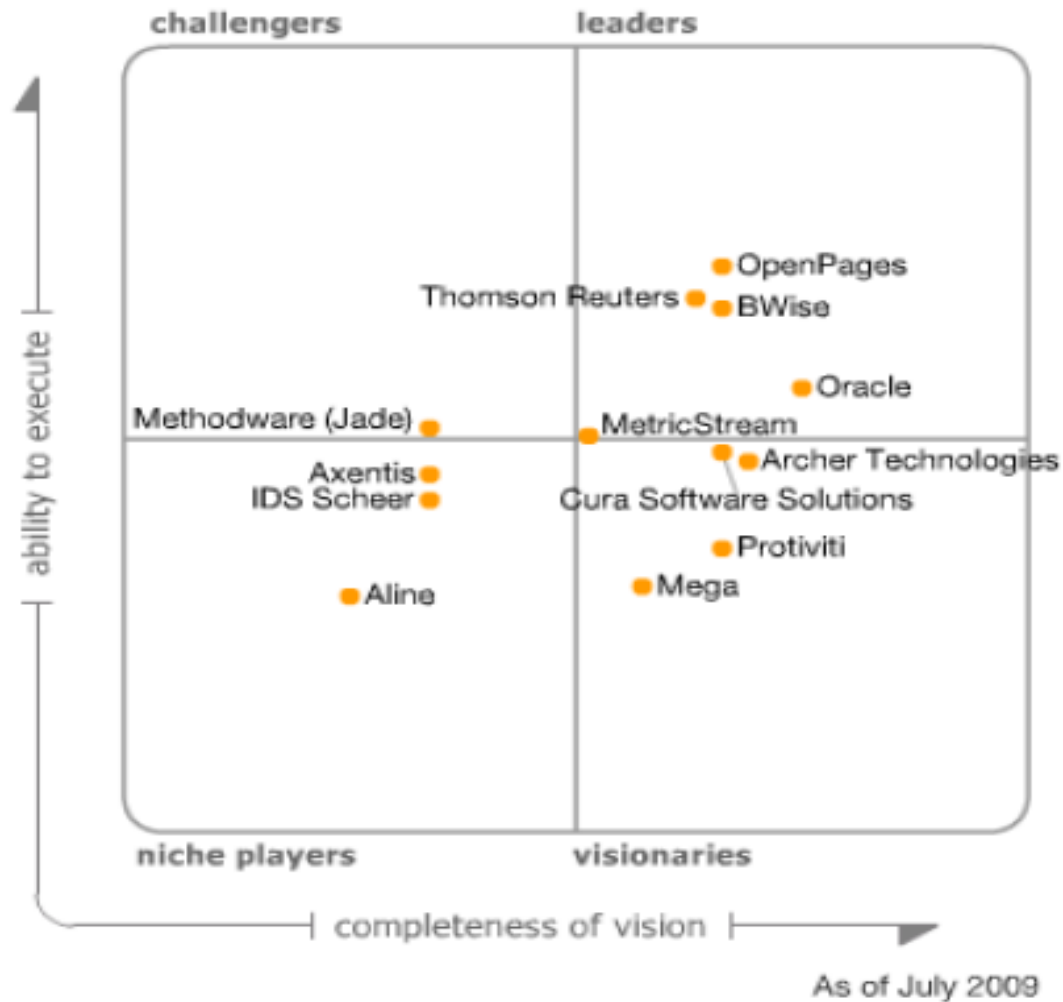
Forrester ratings



Source: Forrester Wave™: Enterprise Governance, Risk and Compliance Platforms, Q3 '09

GRC Tools

Gartner ratings



Source: Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms

GRC Tools

Limitation of current tools in the market

- ▶ The definition of GRC differs from client to client and vendor to vendor, leading to an inability to standardize GRC requirements and guide future development
- ▶ All solutions perform well for certain aspects of GRC, but no one solution provides a complete holistic solution for all GRC requirements
- ▶ Not all tools provide web enabled reporting and dashboards
- ▶ Non Financial RM tools do not provide advanced charting capabilities to address complex risk scenario analysis
- ▶ Not all tools have robust data integration services that allow for real time data correlation with other risk and monitoring tools.
- ▶ Virtually Non-Existent Global Regulatory Content
- ▶ Inconsistent Framework Mapping and Content
- ▶ Only a select few tools provide a minimal amount of configuration flexibility, which allows clients to mold the tool to their business processes and taxonomy
- ▶ Only a select few tools allow for logic based assessments (questionnaires, survey's, etc.), which integrate business workflow and risk calculations driven by assessment results.

GRC Tool Selection and Implementation

Best Practices

Few vendors offer a full GRC solution, making the requirements definition phase prior to solution evaluation critical. Detailed requirements should be documented by the following areas:

- ▶ Corporate Governance (Including IT)
- ▶ Risk Management (ERM, ORM, FRM, ITRM)
- ▶ Legal & Compliance (SOX, GLBA, FFIEC, etc...)
- ▶ Audit
- ▶ Security
- ▶ Other GRC Functional Areas

Management needs to understand the GRC solution's functionality and limitations especially around the following key areas:

- ▶ Policy, Standards and Procedures Management
- ▶ Risk Management Processes (Assessments, KRI's, Event Capture, etc...)
- ▶ Frameworks and Hierarchy Structure (Org, Process, Risk, Control)
- ▶ Regulatory Compliance (SOX, GLBA, Basel II, etc...)
- ▶ Business Process Management Modeling
- ▶ Business Workflow Management
- ▶ Audit Processes
- ▶ Control Automation and Monitoring
- ▶ Metrics, Measurements and Reporting (including ad-hoc reporting)
- ▶ Financial Risk Management
- ▶ Configuration Flexibility

GRC Tool Selection and Implementation

Lessons Learned

- ▶ Lack of an understanding and definition of what GRC truly means and represents
- ▶ Functional Requirements roadmap for organizational and process convergence should be defined prior to tool selection by performing a feasibility study
- ▶ Initiative should be a directive from executive management with agreement from all key stakeholders – Governance, Risk, Compliance, Audit, Security, etc.
- ▶ A lack of understanding of how other business tools can integrate into GRC solutions and of future GRC state requirements still exist
- ▶ Many organizations will need to customize their selected GRC tool or change their current methodologies, business processes, and hierarchies
- ▶ Content management decision – if aligning to leading practices, frameworks, and regulations, a decision needs to be made to determine if you will rely on a vendor to provide and manage content going forward or will it be customized and managed by the client
- ▶ Most organizations take between 12 - 24 months for successful implementation and for operational competencies to be realized
- ▶ Lack of experience and knowledgeable resources that are dedicated to GRC tool implementation

Next Steps

What Should I Do Next

- Assess your current environment
- Identify your requirements
- Understand your processes
- Develop a convergence roadmap
- Look for ways to leverage a tool (can be done in silos)

Contact Information

Anil Markose

anil.markose@ey.com

214 969 9734