

# Exploring GRC and Tools Discussion

Kevin D. Heckel  
Deloitte & Touche LLP

January 17, 2008



**GRC Overview:** Explore what the term **Governance, Risk and Compliance** “GRC” means along with various related tools that enable GRC in a variety of ways.

# What is GRC?

---

- Governance
- Risk
- Compliance

Is this a new concept?

Is it software?

Is it a methodology?

# What's This all About?

---

- Increased board and executive accountability
- Ever-mounting regulatory requirements
- Spiraling compliance costs
- Need to more effectively manage risk
- Silos, fragmentation, poor information quality
- Speed and consequence of adverse events

>>>> an imperative to improve governance, risk and compliance processes and practices <<<<<

# Key Challenges

---

- Most organizations have viewed governance, risk and compliance as discrete activities, separate from mainstream business processes and decision-making
- Governance, risk and compliance have *not* received sufficient attention in performance improvement, business process reengineering efforts
- Governance, risk and compliance have not received sufficient attention in IT strategies, projects or processes.
- Existing IT infrastructures, architectures, organizations and processes do not provide for sufficiently effective risk management

# The Current State of GRC

---

- Managed in Silos
- Reactive, One-Off Approaches
- Not Integrated into Core Processes and Decision Making
- Humans Utilized as Middleware
- IT Assets Not Aligned with GRC Needs
- Poor Information Quality



- Greater Risks
- More Complexity
- Lower Confidence
- Higher Costs

What are we seeing in  
the marketplace?

# What do companies typically look for?

---

- Risk Management
- Data Extraction
- Fraud Detection/Prevention
- Audit Management
- Control Self-Assessment
- Sarbanes Oxley
- Continuous Monitoring

# Recent Trends in the Marketplace

---

- GRC becoming the new model
- Dominant ERP Vendors investing heavily in GRC
- Many new vendors entering the marketplace
- Existing software solutions expanding several modules:
  - SOX
  - Internal Audit
  - Compliance
  - Risk Management
  - IT Governance

# Current Industry Perspectives

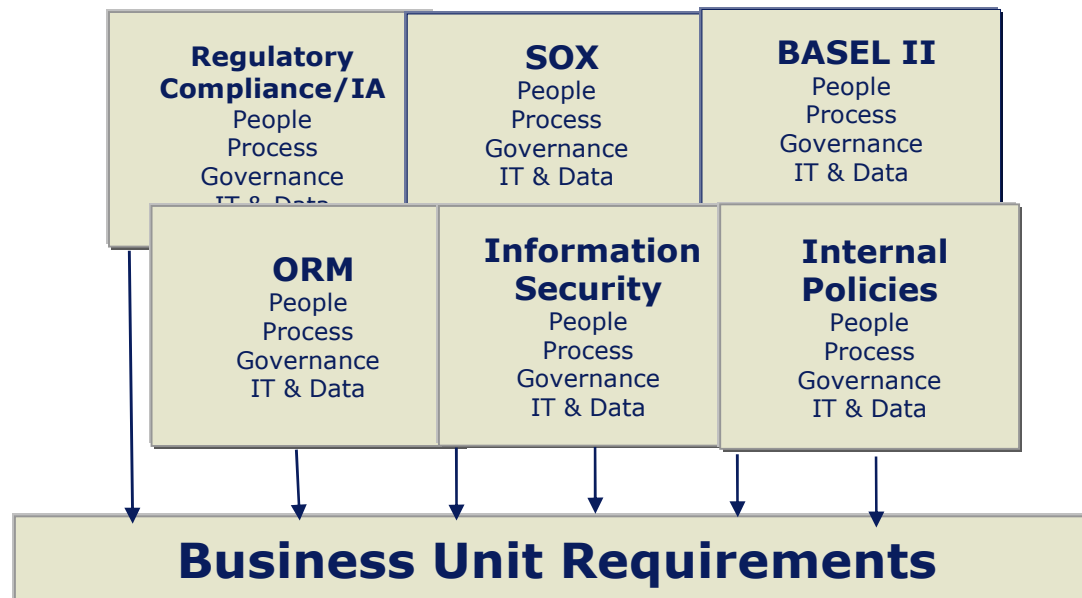
---

- Struggling to understand silos and “who owns what”
- Efforts to reduce complexity to improve effectiveness and lower cost
- Coping from a technology perspective—systems primarily used for one purpose
- Manually-intensive processes; desire for better metrics and timely reporting
- Want increased confidence at lower cost
- Focusing on one-offs / “band-aiding”
- Working on “nuts and bolts” - controls and tactical matters
- Line of business owns compliance, with enterprise-wide function serving as checks-and-balance

# Traditional Risk & Compliance Management: The challenge of silos

---

- Focused on establishing well maintained and controlled processes around *single* compliance areas. This approach has created redundancy and excessive burdens on the businesses, without enterprise-wide oversight of risks.



# How does it work?

# GRC – New Challenges Require a New Approach

---

- Governance, risk, and compliance must be viewed comprehensively and integrated with performance management
- Common information, processes, controls, and systems must be leveraged to simultaneously improve the effectiveness of decisions and produce significant efficiencies and cost savings
- Overcome disparate data and the inertia of “silos”



# GRC Technology Observation

---

**State of GRC** – In 2007 early adopters are moving past the current state, but overall largely unchanged from 2006

**Change Imperative** – Many companies really recognize the imperative and want to progress; but are still challenged to do so

**Technology Gap** – The vendors are getting closer to removing technology barriers – but the market is still highly fragmented. “no GRC in a box yet”

**Companies are ramping up IT GRC related projects, but many are still missing the overall roadmap**

# The Technology Gap

---

- Technology is not adequately used to support compliance, risk management, or governance
- Compliance and risk management procedures and controls are still mainly manual
- Organizations simply don't have the IT assets in place to efficiently and effectively turn data into information
- Existing IT assets are not providing information to allow identification of problems before they become crises
- A programmatic approach is not being applied to Governance, Risk and Compliance information management

# Utilizing Technology

---

## Potential Benefits

- Efficient testing of controls
- Increased reliability
- Visibility into changes to controls
- Alerts for control failures
- Automated tracking of exceptions to tolerances
- Single view of control “health”

## Potential Outcomes

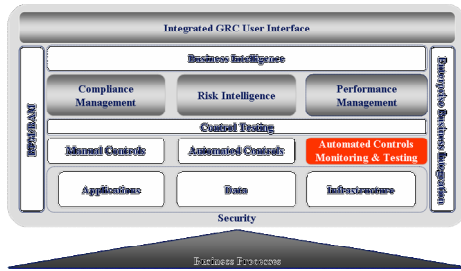
- Reduced compliance cost
- Opportunities to go beyond compliance to improve business processes
- Improved governance across the enterprise resulting in greater earnings potential

## Challenges

- Bringing the management teams together for one solution
- Integrating into business processes
- Developing policies and procedures to address exceptions
- Fragmented tool market

# Tools in the Marketplace

# Automated Controls Monitoring and Testing External Tools and Vendors



ACMT tools are technology-enabled solutions to actively monitor and/or test controls, transactions, and configurations. Typically, these solutions provide functionality to provide testing documentation and/or notify “owners” when exceptions are detected. Some tools provide functionality to automate the control itself as well as monitoring/testing capability.

Activity	Sample Vendors
Transaction and Master Data Monitoring	ACL, Approva, IBM, Oracle/PeoplesSoft, Oversight, SAP/Virsa, SAS, webMethods
Access Controls and SOD Monitoring/Testing	Approva, Applimation, Courion, IBM, Logical Apps, Oracle/PeopleSoft, Oversight SAP/Virsa, Sun Microsystems
Business Process Control Monitoring/Testing	Appian, Approva, Compliancy Software, Computer Associates, Fujitsu, Movaris, Oracle, webMethods, SAP/Virsa
IT General Controls (GCCs)	Cisco, HP, IBM, Microsoft, Novell, Sun Microsystems

**At this point in time, there are multiple vendors that can offer GRC technology solutions.**

# Access Controls & Segregation of Duties Considerations

---

- Does your company need to implement stronger information security measures to comply with requirements imposed by such regulations as the Sarbanes-Oxley Act, HIPAA, and the Gramm-Leach-Bliley Act?
- Does your company need to limit access to authorized third parties, customers, and employees to only data and applications they need to conduct business?
- Have your company's manual processes for compliance proved to be extremely time-consuming, inaccurate, or costly?
- Have your company's financials been restated due to errors?
- Does your company rely heavily on mitigating controls?
- Have your auditors identified segregation of duties issues in management letter comments?
- Has your company experienced unauthorized transactions or fraudulent transactions as a result of excessive access or inadequate segregation of duties?

# The Need for Access Controls & Segregation of Duties Monitoring

---

- **Regulatory Compliance** - Sarbanes-Oxley and other regulatory issues are forcing companies to increase their awareness and accountability of their employees actions within the company
- **Security and Data Management** – Recent privacy laws and prosecution of security violations is bringing a new awareness to monitoring and controlling security and access to data within the organization
- **Access Management** – Provisioning and management of users access to applications have not been enforced, resulting in access creep
- **Rapid Implementation of ERPs** – Application Security was often overlooked or implemented incompletely (e.g. Segregation of Duties was not adequately addressed, or system level security was not appropriately established, etc.)

# Examples of Access Controls & Segregation of Duties Monitoring

Access Control Area	Configured Controls
User Access Controls Monitoring	<ul style="list-style-type: none"><li>• Settings for monitoring sensitive access to specific transactions</li><li>• User tracking of sensitive transactions (date and time stamp of transaction and changes made)</li><li>• Tracking of user changes to a user access role and profile</li><li>• Monitoring of emergency access in production</li></ul>
Segregation of Duties Monitoring	<ul style="list-style-type: none"><li>• Conflict rules for all business process segregation of duties (all business cycles)</li><li>• Identification and rules for mitigating controls and tracking</li><li>• Risk alert settings for various levels of SOD conflicts</li><li>• Workflow routing settings for approval of conflicts</li></ul>
System Access Controls Monitoring	<ul style="list-style-type: none"><li>• Access control system configuration changes</li><li>• Configuration of allowable ID and password length and combinations</li><li>• Session Time Outs and Lock Outs</li><li>• Multiple Log In session settings</li><li>• Password Management (length, character combinations, and expiration)</li></ul>

**Technologies are available to assist with all the above categories for access controls and SOD monitoring (e.g., Approva, SAP/Virsa, etc.)**

# Application Configuration & Control Monitoring

---

## **FEATURES:**

- Detect changes to system configurations that may increase risks of fraud, error and control breakdown
- Monitor the effective performance of business process controls and the collection of testing documentation

## **POTENTIAL BENEFIT:**

- Timely detection of control breakdowns and/or continuous confirmation that controls are working effectively

# Now What?

# What can I do?

---

- Conduct a cross-functional workshop to compare current state to desired future state
- Conduct an honest self-assessment
- Align your team; engage senior leaders
- Define what integrated GRC looks like for ***your*** company
- Develop business case and define success criteria
- Develop ***your*** roadmap
- Start the journey

# Technology to Leverage

---

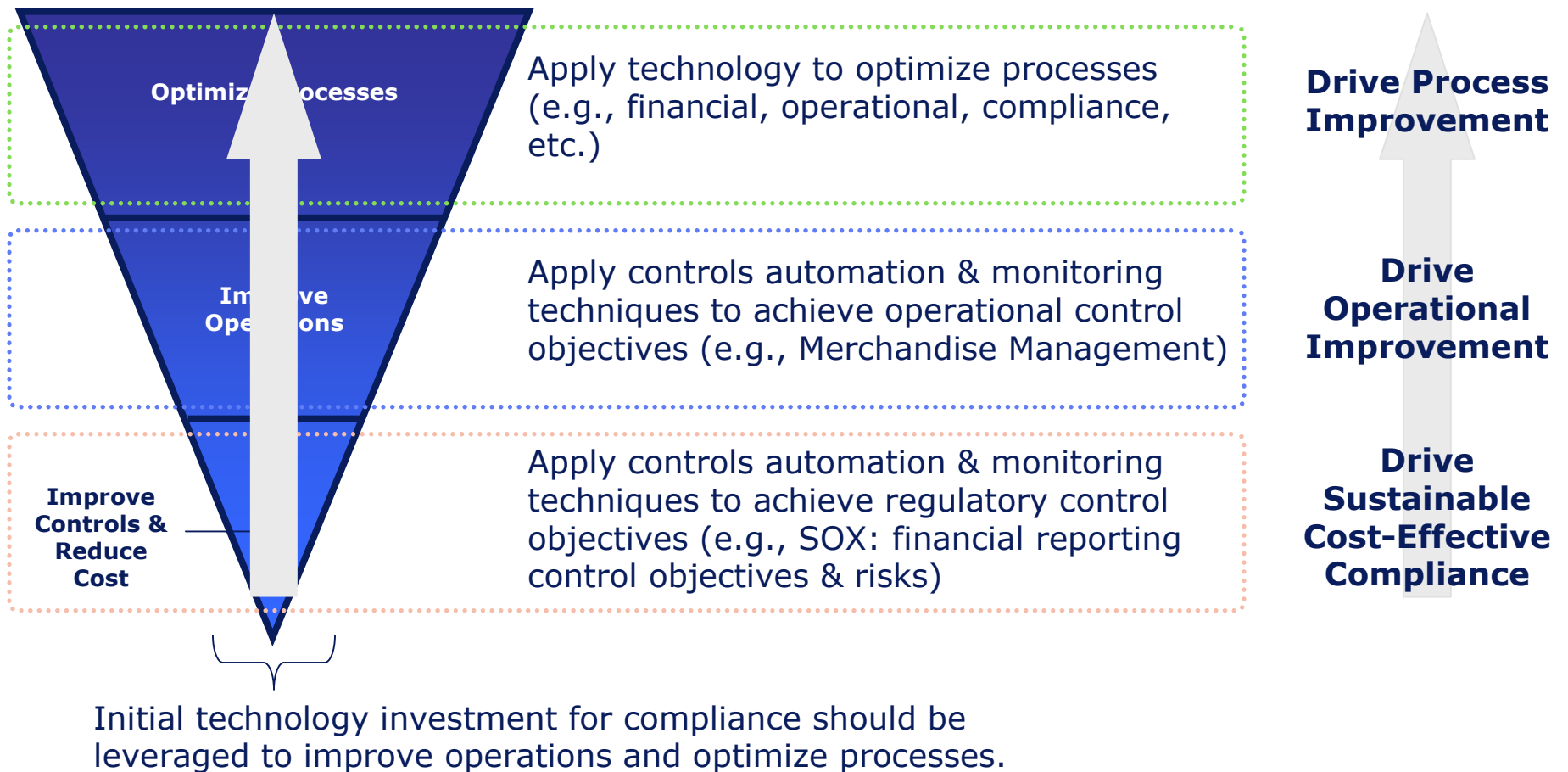
Technology can help companies with their governance and oversight responsibilities.

To achieve these goals, companies will need to:

- Assess their current technology environment
- Identify opportunities for automation and monitoring
- Identify opportunities to leverage existing investments
- Identify new technologies that will integrate with and extend existing infrastructure
- Make sure their systems are being used efficiently and effectively
- Prioritize technology solutions to meet their greatest needs

# Moving up the Value Chain

To move up the value chain, companies should leverage technology-enabled control capabilities used to achieve financial control objectives, to address operational control objectives and process improvement opportunities.



# Implementation Considerations

# Implementation Considerations

---

- Install vs. Implement
  - ‘Get it running’ vs. ‘Fully realize value’
- KIS – Keep it simple
  - Generally start with a success and build
  - Don’t under estimate the planning and prototype phase
- Proof of Concept / Phased Go-Live
  - Smaller groups of users
  - Controlled scenarios

# Implementation Consideration

---

- Plan and Prototype
  - Thoroughly plan the solution in advance
  - Prototyping has proven to be very valuable
- Vendor support
- Linkage across system landscape

# Implementation Considerations

---

- System set up and linkage
  - Differences in landscape
  - Even though related applications, the connectors are interfaces
- Change control and management
  - QA/Development vs. PRD systems
  - Do not use SAP transports
- In-scope for SOX?
  - Reliance of audit functions

# Implementation Considerations

---

- **Distributed support vs. Centralized support model**
  - Who ‘owns’ the system?
    - Security?
    - Internal audit?
    - Controls function?
    - SAP COE/Support team?
  - What access is given out broader?
    - Are super users in the system or provided information?
- **Solution Documentation**
  - Vendor provided vs. Client specific

# Closing Thoughts/Q &A

---

- Companies should consider adopting an integrated approach to efficiently manage governance, risk, and compliance
- Internal Audit is the enabler of high quality information for good governance, effective compliance and improved risk management
- Internal Audit plays a critical role in helping management achieve and sustain compliance with laws, regulations, standards and policies
- The impacts and implications of governance, risk and compliance are broad and pervasive and will be a significant driver of priorities and investments over the next few years