PwC Advisory
Performance Improvement
Integrated Governance, Risk, and Compliance

September, 2007

A Principles Based Approach to Integrating GRC

How to get back to business through the sensible integration of governance, risk and compliance*

*connectedthinking

PRICEWATERHOUSECOOPERS

Agenda

Situation:
- It is time to drive efficiency and improve performance

Perspective:
- Anchor GRC integration in principles

Implications:
- Execute along three avenues

Agenda

Situation:
- It is time to drive efficiency and improve performance

Perspective:
- Anchor GRC integration in principles

Implications:
- Execute along three avenues

Situation

Why GRC Is Relevant?

- **Accelerating rate of change**
  - Rapid technological advances in recent years
  - Requires management to be more anticipatory
  - Requires a GRC approach that effectively aligns risk and rewards
- **Greater complexity**
  - Accelerated rate and volume of change demands increased flexibility
  - Extended business models and increased geographic diversity increase the complexity of managing the business
  - Increased number of regulatory regimes
- **Increased transparency**
  - Stakeholders learn about unmanaged risk almost immediately
  - Management has little time to remedy the impact of a risk management failure
  - Places a premium on the ability to identify, evaluate and manage risks

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Situation

Companies have responded by expanding or building GRC oversight functions

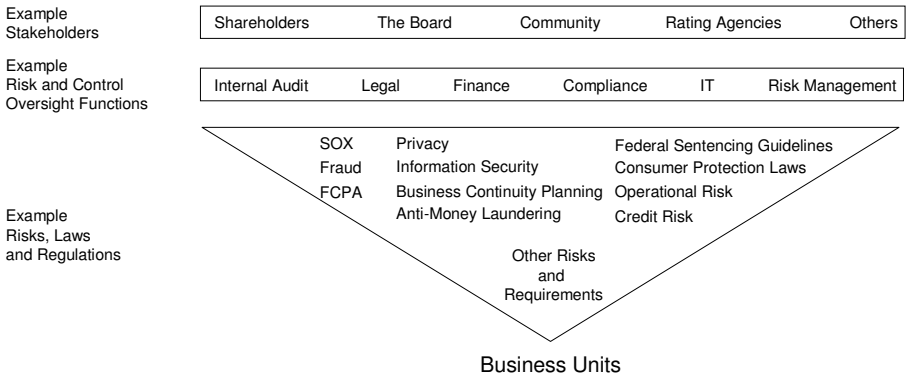
Increasing Stakeholder Demands	New Risks & Requirements	Response
• Shareholders • The Board • Customers • Employees • Community • Rating agencies • Others	• Increased regulation • Less tolerance for risk management failure	• Expansion of existing oversight functions • Creation of new oversight functions • Layering of oversight processes over existing processes and functions

Result: Multiple independent GRC oversight functions and committees, each focused on a specific GRC challenge

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Situation

The management of business units are being diverted from their core mission of revenue generation



© 2007 PricewaterhouseCoopers LLP. All rights reserved

Situation

Opportunities for integration of activities exist

	Illustrative	Internal audit	Regulatory compliance	Operational risk	SOX (bus and IT)	Anti-fraud	Legal	Records management	Information security	Business continuity planning	Credit / market risk	IT problem management
		Common governance, risk and control functions										
Common activities	Event definition/scoping	X	X	X	X	X	X	X	X	X	X	X
	Risk/control assessment	X	X	X	X	X			X	X	X	X
	Control monitoring		X	X		X		X	X	X	X	X
	KPIs/KRIs		X	X		X	X	X	X	X	X	X
	Control testing/validation	X	X		X	X			X	X	X	X
	Advisory		X	X	X	X	X	X	X	X	X	X
	Policy and procedure	X	X	X	X	X	X	X	X	X	X	X
	Incident management	X	X	X	X	X	X		X	X	X	X
	Deficiency management	X	X	X	X	X	X	X	X	X	X	X
	Reporting	X	X	X	X	X	X	X	X	X	X	X
	Change management		X	X	X	X			X	X	X	X
	Records management	X	X	X	X	X	X	X	X	X	X	X
	Communications	X	X	X	X		X	X	X	X		X
	Training	X	X	X	X				X	X	X	

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Situation

Oversight capabilities are stretched to the breaking point

- AMR Research estimates that in 2007 organizations will spend nearly $30 billion on compliance
- Many companies recognize that they cannot cost effectively sustain this approach
- Others are concerned about the impact that future growth will have on an already fractured system

A solution is to integrate GRC efforts and resources to seize future business opportunities while remaining adaptable to addressing new risks and compliance obligations

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Agenda

Situation:
- It is time to drive efficiency and improve performance

Perspective:
- Anchor GRC integration in principles

Implications:
- Execute along three avenues

Perspective

Use a principles-based approach to integrating governance, risk and compliance

Advantages of using a principles-based approach
- Focuses the organization on principles rather than organizational silos
- Focuses management attention on *what* needs to be done rather than on *who* reports on it or *where* it occurs
- Helps ensure business effectiveness, regardless of the function, risk or regulation being addressed
- Allows for taking an incremental approach to integration
- Should result in a more efficient allocation of resources – management resources can be reallocated to revenue generating roles

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Perspective

Begin by using an accepted set of principles

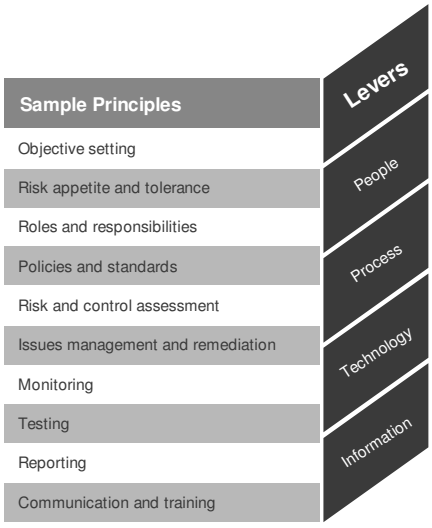
Sample Principles
Objective setting
Risk appetite and tolerance
Roles and responsibilities
Policies and standards
Risk and control assessment
Issues management and remediation
Monitoring
Testing
Reporting
Communication and training

Using a principles-based framework cuts across organizational hierarchies that mask potential integration points behind reporting lines

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Perspective

Examine operating levers to identify logical integration points



- Operating levers are the methods used to execute principles and to identify logical points of integration
- Management should systematically evaluate the way the levers are used to apply each principle
- Logical integration points should be identified
- An essential consideration is finding those areas where differentiation should be preserved

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Perspective

Identify variations in how principles are applied – and preserve variations where it makes sense

- Understand the root causes of the differences in how principles are executed
- Distinguish those differences that are valuable and necessary from those that have evolved from ineffective and inefficient silo practices

The purpose of integration is to combine processes and information while preserving variations in how principles are applied when it makes sense to do so

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Perspective

Example: The “testing” principle

- Testing activities are often executed in multiple organizational units, spanning various businesses and control functions
- Viewing testing through the lens of all four operating levers can eliminate redundancies and disconnects, enabling improved efficiency and performance
- The natural inclination is to think about testing in terms of the ***people*** lever
- However, when evaluating testing in terms of the other operating levers, a more comprehensive view emerges

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Perspective

Example: The "testing" principle

- ***Process***
  - Testing processes are often inconsistent.
  - Often results in:
    - A lack of common standards for test scoping, test execution and deficiency identification
    - Redundant testing of the same environment, but for different purposes
- ***Technology***
  - Multiple systems are often used (or in some cases no technology is used)
  - Often results in:
    - Wasted spend or leaves the organization dependent on heavily manual efforts
- ***Information***
  - The actionable product of people, process and technology
  - Often results in:
    - Uncoordinated and or redundant information
    - Inconsistent understanding of operating environments
    - Inability to efficiently satisfy new or evolving demands

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Agenda

Situation:
- It is time to drive efficiency and improve performance

Perspective:
- Anchor GRC integration in principles

Implications:
- Execute along three avenues

Implications

Determine the scope of integration that is best

- Integration should occur at sensible points designed to move the organization toward a GRC platform that is focused on balancing growth, risk and return
- Begin with a single principle, oversight function, or business unit and carefully determine the scope of the integration based on the organizations objectives and capacity for change

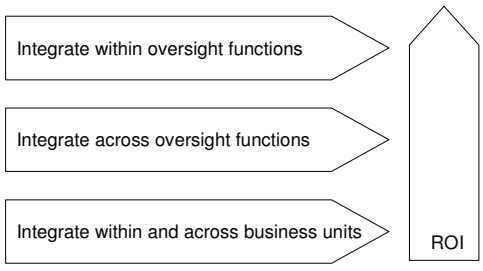
Take small steps, demonstrate value, and then move on to the next step

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Implications

Execute along three avenues

Once the scope of the integration effort is defined, integration can be executed along the following three avenues



© 2007 PricewaterhouseCoopers LLP. All rights reserved

Implications

Integrate across oversight functions

Principle: Risk and Control Assessment

- The issue:
  - Use of multiple systems to assess and control operational risk
  - Policies were loosely enforced and interpreted differently across risk and control assessment units
  - Corporate level risk and control assessment reports took months to compile
  - Reporting was often unreliable
  - Maintenance of multiple systems and processes was expensive
- Action taken:
  - The iGRC framework was used to identify common principles and to examine all four operating levers
  - A standard risk and control assessment program was implemented across the organization
- Results:
  - Risk and control assessment report accuracy, consistency and coherence were substantially improved
  - The time frame for producing risk and control assessment reports was reduced from months to weeks
  - Greater ability to compare assessment outcomes and allocation of resource

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Implications

Integrate within oversight functions

Principle: Issues Management and Remediation

- The issue:
  - The operational risk department used multiple disparate databases across geographies and businesses to capture and report deficiencies
  - Often resulted in a single deficiency being reported several times
  - A lack of clarity as to responsibility for correcting deficiencies
- Action taken:
  - The company integrated deficiency databases and created a standard process by which to report and record deficiencies
  - The process included the establishment of ownership for each issue identified
  - Instituted a common reporting structure to disseminate information to business and corporate management
- Results:
  - Improved efficiency
  - Improved clarity of ownership
  - Reduction in the number of senior management members involved in deficiency oversight committees

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Implications

Integrate within and across business units

Principles: Objective Setting and Roles and Responsibilities

- The issue:
  - At an international company, risk management and compliance oversight committees existed across the organization in business units, within functional areas and within internal audit.
  - Use of disparate databases and manual processes to consolidate and report risk management and compliance issues
  - Reports used differing taxonomies, were slow to produce and were heavy on data and light on analysis
  - The goal was to create reports based on enterprise-wide control metrics that would aggregate information from all oversight functions, identifying the most important issues and the appropriate response strategies
- Action Taken:
  - The company created a prototype for one business unit
  - Developed uniform methodologies for entering and maintaining information
  - Disparate desktop systems were migrated to a single database system capable of supporting all users
- Results:
  - Resulted in a consistent, more coherent basis for management to assess its risk management and compliance priorities
  - Eliminated reporting redundancies, reduced workloads, accelerated reporting timelines and enabled risk-based decision making

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Implications

Summary

- **Accelerating rate of change, increasing complexity, and greater transparency** ---demands that management act now to build a sustainable, efficient GRC capability that enables companies to balance growth, risk and return
- **The principles-based approach to iGRC** provides the means to achieve this goal in incremental steps, enabling companies to integrate within an oversight function, across functions, or within and across business units
- **Allows management to get back to business** focusing on what creates and preserves value

© 2007 PricewaterhouseCoopers LLP. All rights reserved

Questions and Answers

© 2007 PricewaterhouseCoopers LLP. All rights reserved

A Principles Based Approach to Integrating GRC

How to get back to business through the sensible integration of governance, risk and compliance*

© 2007 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, other member firms of PricewaterhouseCoopers International Ltd., each of which is a separate and independent legal entity. *connectedthinking is a trademark of PricewaterhouseCoopers LLP.

PRICEWATERHOUSECOOPERS