

January 2007

The power of principles

Considerations for integrating governance, risk and compliance*

Panel

- Bill Savage, The Hartford
- Tim Journy, MetLife
- Paul Horgan, PricewaterhouseCoopers
- Carlo di Florio, PricewaterhouseCoopers

How.*

Contents

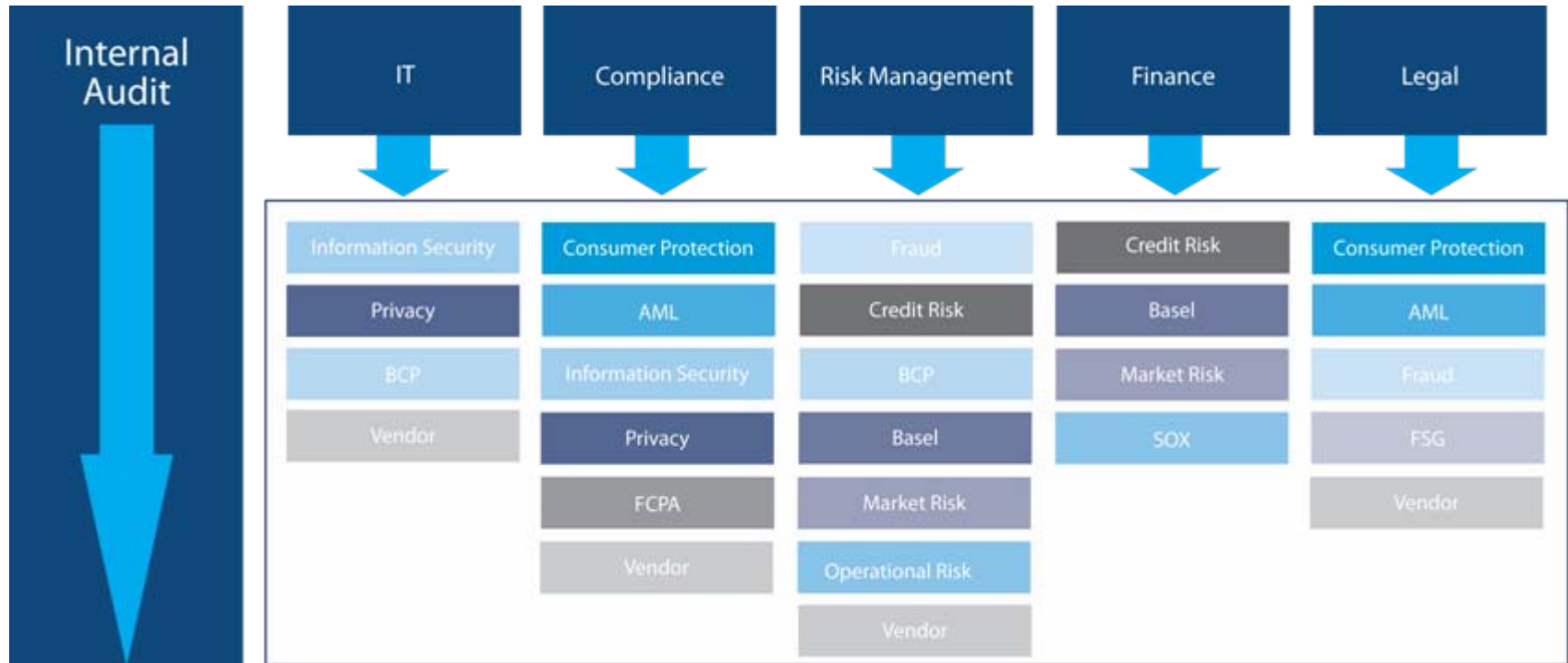
Situation

Point of View

Implementing iGRC

How.*

Lack of GRC coordination creates inconsistencies and redundancies in control activities and increases overall costs



- Individual functions and departments responsible for specific risks, regulations and control activities with their own independent infrastructure are commonplace
- Functions and departments that operate in silos impair GRC effectiveness by contributing to duplication of efforts, inconsistent processes, miscommunication, and “auditor fatigue”
- They also inhibit efficient allocation of resources to GRC functions, and by the rest of the enterprise that is responding to risk-related governance activity

Contents

Situation

Point of View

Implementing iGRC

How.*

Our Point of View

- Through thoughtful analysis and action, institutions can integrate GRC activities and leverage common people, processes, technology, and information (i.e., operating “levers”) either enterprise-wide, or:
 - Within a control function
 - Across control functions
 - Within a business unit
 - Across business units
 - For a single regulatory requirement
 - Across multiple regulatory requirements
- Changes should be made only if consistent with industry-accepted, risk-related corporate governance principles (e.g., COSO ERM), regulatory requirements and supervisory expectations
- Through better integration of risk-related corporate governance activities, companies can both enhance overall effectiveness and maximize efficiency
- Benefits from enhanced risk management program performance and efficiency enhancement should be defined, quantified and measured continuously to assure feasibility and maintain relevance

Opportunities for integration of activities exist

The opportunities for integration exist across functions that are performing similar risk-related corporate governance activities. The potential size of each opportunity depends upon the number, scope and scale of risk-related corporate governance functions, as well as the number, scope and scale of business units impacted by each function.

Common Governance, Risk and Control Functions

Common Activities	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	
	Event definition/scoping	X	X	X	X	X	X	X	X	X	X	X	
	Risk/Control ID & 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	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			

Using a Principles-based framework helps to identify integration gaps and target opportunities for enhancement

- Based on the functions and activities in scope, identify relevant standards and regulatory requirements applicable across risk-related corporate governance functions
- Tailor industry-accepted standards, as appropriate based on the scope and objectives of the analysis, into principles for evaluation
- Analyze target principles through four operating levers that are used to perform activities



<i>Illustrative 10 Key Principle Categories</i>	Levers
Objective Setting	People
Risk Appetite and Tolerance	
Structure, Roles and Responsibilities	Process
Policies and Procedures	
Communication and Training	Technology
Risk/Control Identification and Assessment	
Monitoring	Information
Testing	
Issues Management	
Reporting	

Effectiveness and efficiency can be realized through integrated governance, risk and compliance

Effectiveness

Role Clarity - Create clear roles between and among each component of the governance framework

Insightful, Actionable Management Information - Consistent reporting standards, dashboards

Enhance Risk/Return Evaluation - Target GRC investments to most material risks, develop control environment commensurate with risk profile

Regulatory Response - Pro-actively manage your response to the regulatory environment, and to the “next big initiative”

Efficiency

Maximize Coordination and Leverage- e.g. limit/merge duplicative assessments, promote process, data and technology platform consistency

Reduce burden on business unit resources - re-allocate resources back to revenue generation or other risk-related activities

Control the growth in GRC related expenses – develop scalable infrastructure that is utilized cross functionally

Contents

Situation

Point of View

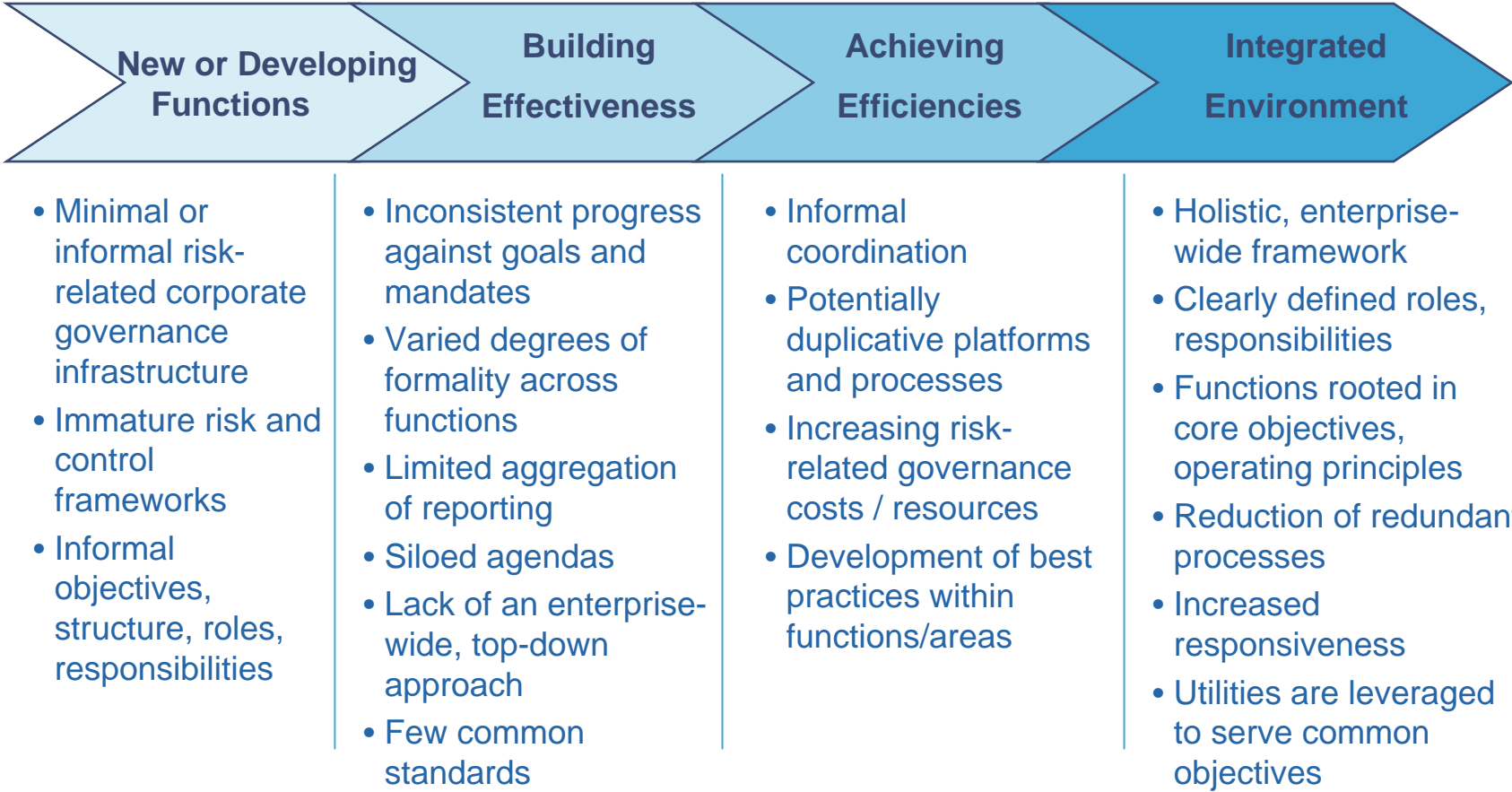
Implementing iGRC

How.*

Implementing iGRC

The road to integration will be influenced by the maturity of an organization's risk-related corporate governance structure and framework

Organizations will start at different places depending upon the maturity of their functions



The regulatory oversight within an industry will influence an organization's approach to establishing its principles and iGRC strategy

Several recent examples of integration initiatives in the marketplace

Strategic

Reduction of Overall Governance, Risk and Control (GRC) Expenditure

Performed detailed review of certain risk and control functions

Developed prioritized roadmap to streamline GRC infrastructure.

Implementation of Enterprise Risk Management

Established a common basis for the relationship between objectives and the company's means of achieving them.

Resulted in the reduction of duplicative effort and reallocation of resources to mitigate the risks to its most important objectives.

Tactical

Rationalization of Risk and Control Assessments (RCA)

Coordination of 17 assessment processes into one standardized RCSA process with common definitions and aggregated information.

Unified Risk and Control Dashboard

Aggregated and consistent reporting on risk and control information via a Management dashboard.

Dashboard will contain forward-looking and historical data that rolls up effectively to management.

Deficiency / Remediation Management

Integrated thousands of identified deficiencies into a single repository using a common data taxonomy and reporting. Management establishes an enterprise-wide view of all identified deficiencies.

Implement Standardized New Customer Account Processes

An enterprise-wide approach to opening new customer accounts integrating operational, finance, risk and compliance requirements, as well as regulatory expectations.

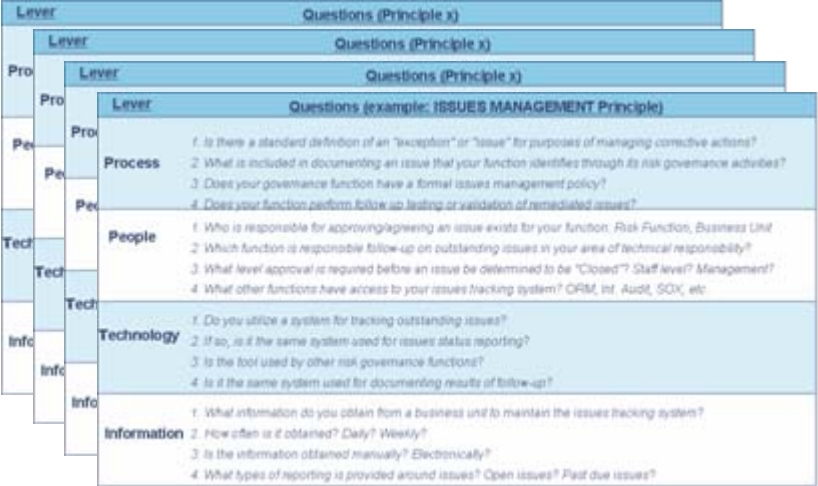
Example 1: Develop methods to obtain information

- Based on the principles established for evaluation, develop an approach to obtaining information about each principle from each function (e.g., through use of questionnaires, detailed interviews, documentation evaluation, detailed process mapping, etc.)

<u>Lever</u>	<u>Questions (example: ISSUES MANAGEMENT Principle)</u>
Process	<ol style="list-style-type: none"> 1. How are “issues” defined for the purpose of managing corrective actions? 2. What is included in documenting an issue that your function identifies through its risk governance activities? 3. How does the formal issues escalation process work in various functions? Is it based on risk? 4. How does your function perform follow-up testing or validation of management-remediated issues?
People	<ol style="list-style-type: none"> 1. What level is responsible for agreeing an issue exists for your function: Risk Function? Business Unit? 2. Which function is responsible for performing follow-up on outstanding issues? 3. What level approval is required before an issue is determined to be "Closed"? 4. What other functions have access to your issues tracking system?
Technology	<ol style="list-style-type: none"> 1. How are multiple issues-tracking systems coordinated? 2. What systems are used for issues status reporting? 3. Are these tools used by other risk governance functions? 4. How are they used for documenting results of follow-up?
Information	<ol style="list-style-type: none"> 1. What information do you obtain from a business unit to maintain the issues tracking system? 2. How is information obtained from a business unit? Daily? Weekly? 3. Is the information obtained manually? Electronically? 4. What types of reporting is provided around issues? Open issues? Past due issues?

Implementing iGRC

Example 1: Analyze information related to current cross-functional activities to determine where redesign could enhance effectiveness and efficiency



Principle and Lever Analysis of Potential Overlaps

- **Collect and analyze information**
- **Identify potential areas of integration and synergy**
- **Identify potential overlaps in process and technology**
- **Identify costs associated with systems, processes**

Cost Data	
% of functional budget dedicated to "principle"	%
Functional People-Hours Utilized	FTE*assumed unit cost
Third Party Vendor Fees	Fees
Total Costs (e.g., admin, operating, other) related to "principle"	Costs
Information System Costs related to "principle"	Costs

Example 1: Recommend areas for further in-depth analysis and study

Possible Recommendations:

- Evaluate the current risk-related governance committee structure, roles and responsibilities
- Enhance the process of setting and monitoring performance against enterprise-wide risk governance objectives
- Evaluate the integration of independent testing/validation
- Define risk tolerance and coordinate its application across risk-related corporate governance activities
- Establish a corporate policies and procedures framework anchored in risk tolerance
- Reduce the number of risk and control assessments (“RCA”), and develop a corporate utility to manage the process, tools and technology used to support RCAs
- Develop a consistent approach to tracking, reporting, and following-up on outstanding issues.

Potential Effect

- Effectiveness: Increases
- Efficiency: Increases
- Role Clarity: Increases
- Accountability: Increases

Contact Information

PwC Financial Services Advisory professionals focusing on Integrated Governance, Risk and Compliance issues are:

Miles Everson, Principal	miles.everson@us.pwc.com	(646) 471-8620
John Garvey, Partner	john.garvey@us.pwc.com	(646) 471-2422
John Campbell, Partner	john.w.campbell@us.pwc.com	(646) 471-7120
Jeff Lavine, Partner	jeff.lavine@us.pwc.com	(703) 918-1379
David Albright, Principal	david.albright@us.pwc.com	(703) 918-1364
Ellen Walsh, Partner	ellen.walsh@us.pwc.com	(646) 471-7274
Roger Coffin, Partner	roger.coffin@us.pwc.com	(646) 471-2545
Daniel Ryan, Partner	daniel.ryan@us.pwc.com	(646) 471-8488
Paul Horgan, Partner	paul.l.horgan@us.pwc.com	(646) 471-8880
Dennis Chesley, Managing Director	dennis.l.chesley@us.pwc.com	(646) 471-4009
Paul Mokdessi, Managing Director	paul.e.mokdessi@us.pwc.com	(312) 298-3347
Allan Cuttle, Managing Director	allan.cuttle@us.pwc.com	(646) 471-7573
Stephen Russell, Managing Director	stephen.j.russell@us.pwc.com	(203) 539-3079
Andrew Wilson, Managing Director	andrew.d.wilson@us.pwc.com	(646) 471-7839
Steve Crosby, Managing Director	c.steven.crosby@us.pwc.com	(646) 471-4875
Carlo Di Florio, Director	carlo.diflorio@us.pwc.com	(646) 471-2275
Rob Gormly, Director	robert.gormly@us.pwc.com	(646) 471-4221
Dietmar Serbee, Director	dietmar.d.serbee@us.pwc.com	(646) 471-7270
Dmitri Londos, Director	dmitri.londos@us.pwc.com	(646) 471-7063
David Sapin, Director	david.sapin@us.pwc.com	(703) 918-1391
Stephen Koslow, Director	stephen.w.koslow@us.pwc.com	(312) 298-3829

PRICEWATERHOUSECOOPERS 

How.*