PricewaterhouseCoopers'

2008 Banking & Capital Markets Conference*

November 19, 2008 | New York City

*connectedthinking

PRICEWATERHOUSECOOPERS

Creating a sustainable risk and compliance organization in an environment of increasing regulatory mandates and demands for transparency

Carlo di Florio
Principal, Financial Services Advisory Practice
PricewaterhouseCoopers LLP

Paul Mokdessi
Managing Director, Financial Services Advisory Practice
PricewaterhouseCoopers LLP

Agenda

- Current Situation
- Regulatory Considerations
- A Framework for Response
- Examples of Industry Practices
- Key Takeaways

Agenda

- Current Situation
- Regulatory Considerations
- A Framework for Response
- Examples of Industry Practices
- Key Takeaways

Most C-level executives face a dilemma of unprecedented industry conditions…..

- Unprecedented market conditions
- Significant failures of several institutions
- Greater operating model complexity
- Accelerated rate of change

…….and operational constraints and heightened expectations

- Increased regulatory oversight
- Uncertainty surrounding future regulatory landscape
- Increased visibility and demands for transparency
- Budget pressure

"Well-managed organizations rely on their leadership to articulate strategy, the range of outcomes that are acceptable to maintain and increase franchise value, and the structure through which organizations pursue their strategy and increase the firm's value as a going concern. Imbedded within these responsibilities is the task of determining in which businesses to engage and to what degree, and hence the kinds and levels of risks the firm will accept. **The responsibilities necessarily include the task of creating an infrastructure to take on appropriate exposures that will achieve targeted returns and simultaneously to identify, measure, and manage the associated risks**."

*Regulatory Observations on Risk Management Practices during the Recent Market Turbulence, March 6, 2008

For many financial service firms, performance measurement, operational and risk management practices did not enable avoiding losses

- Inadequate forecasting models
- Inconsistent risk limits and disaggregated exposures
- Siloed management structures and operational processing

The historic approach of independent governance risk & compliance (GRC) oversight functions and committees has not been working effectively

Increasing stakeholder demands

+

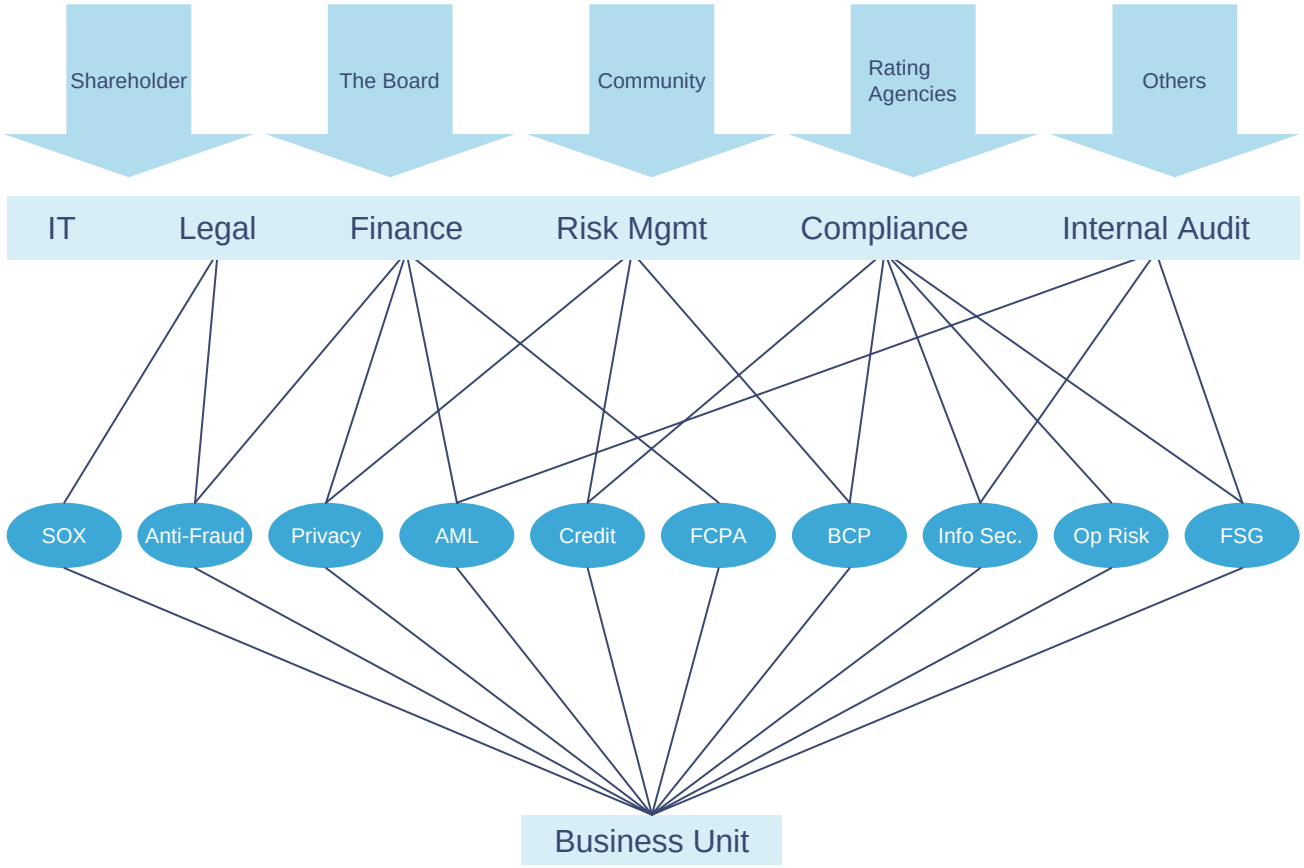
Expansion of Risk and Control Oversight Functions

+

Expanding Risks, Laws and Regulations

=

- Distracted attention
- Inconsistent monitoring and review
- Risks falling through the cracks
- Business Fatigue



Financial institutions are realizing that they cannot sustain this ineffective and costly approach to managing risks

- AMR Research estimates that in 2008 organizations will top $32 billion on compliance spend – most clients are reporting that they cannot cost effectively sustain this approach
- The costs of the risk management and compliance functions themselves are only a fraction of the true cost of risk and compliance activities – The true cost of implementation in the businesses is multiple the cost of risk and compliance central groups themselves
- Siloed approach is impeding standardization, scalability and speed to market
- Credit crisis and many “lessons learned” reviews have highlighted the inadequacy of the current approach at many firms in terms of organization, reporting lines, risk appetite, risk monitoring and overall infrastructure
- In the current environment, new regulation is inevitable and this will carry additional cost as well

What some of our financial institution clients are experiencing

Stakeholders	GRC Challenges
Board & Audit Committee	• Difficulty in exercising their role of effective oversight into corporation's risks • Lack of visibility into potential landmines • Difficulty in understanding breadth and implications of regulatory expectations
Senior Management	• Lack of a consistent or defined view on the level of risk the company is willing to accept • Need better information and articulation of critical emerging risks and control issues • Current risk information not sufficient to be a key factor in driving key corporate decisions
Risk and Compliance Leadership	• Multiple and/or uncoordinated risk/control assessments • Independent GRC oversight functions and committees, each focused on a specific GRC challenge • Difficulty in responding to the next regulation in a coordinated fashion

What some of our financial institution clients are experiencing

Stakeholders	GRC Challenges
Business Unit Management	• Business often views risk management as a bureaucracy that provides limited insight or tools • Experiencing “assessment fatigue”, and is distracted from its core revenue generating activities • Suffering losses or breakdowns in controls but feels like they spend a lot of money to identify and prevent breakdowns • High volume/complexity of management reports that don’t distill what’s important • Business has only informal or ad hoc approaches to managing risk • Previous cost cutting actions have often been “slash and burn” headcount reductions that are reversed when the growth cycle returns
Internal Audit	• Businesses that feel over-audited or that audit focuses on the wrong areas • Disjointed remediation and tracking of issues • Lack of automated controls and/or too much time spent on evidence collection • Risk and compliance information not suitable for driving intervention • Challenges in proper internal valuation and validation of securities & portfolios

Agenda

- Current Situation
- Regulatory Considerations
- A Framework for Response
- Examples of Industry Practices
- Key Takeaways

Key implications

In our interactions with regulators and our clients, it is clear that the regulatory backlash to the credit crisis is building and that this will have significant implications in a number of areas, including the cost structures of risk and compliance functions. These consequences will likely show up in areas such as increased reporting, more focused supervisory exams, more critical reports, findings and mandates for remediation. There is also likely to be a rise in enforcement actions and litigation. There has been a stronger focus on sound and internally coordinated enterprise risk management practices (particularly those put forward by the Senior Supervisory Group and the BIS).

In this environment, real operational process improvements that result in better information on risk and compliance profiles should also result in cost reduction if carried out intelligently. Cost reduction should be a by-product, not the primary goal.

Some Key Implications
More regulation, greater regulatory scrutiny and costs are coming
Financial institutions will need to deal with these challenges in the backdrop of very difficult economic times and severe pressure for cost cutting, notwithstanding the substantial risk management challenges that must be managed on a day-to-day basis for the foreseeable future. Any attempts to cut costs will need to be made in a careful manner.
Much better enterprise risk oversight will be required
Regulators will expect a unified view of the major risks facing the enterprise. They are starting to ask for evidence that the Board, Senior Management, and risk and control functions have similar views of the core enterprise risks facing the organization, and a unified mechanism for determining internal capital adequacy.
Accountability for specific compliance mandates can not be delegated
Regulators will encourage efforts to integrate, but will expect individual control functions to perform their expected role- for example, AML assessments need to produce specific information on AML risks.

Key implications

Some Key Implications
Greatly expanded supervision of liquidity risk management
The June, 2008 BIS guidance has expanded the supervisory powers over liquidity risk management. To limit the damage liquidity shortfall can have, on individual companies and systemically, a more integrated framework consisting of tolerance, risk identification, stress testing, reporting and disclosure will be necessary at each financial institution.
More compliance training will be expected
The regulatory expectation of across-the-board awareness of risk will require a great deal more spend on employee training, especially on compliance related issues
Global organizations are expected to have similar approaches to risk management across their entire organization
Home regulators will expect head office to lead globally, and demonstrate an affinity for local rules interpretations
The race is on
Firms will be held up to the best practices of their competitors- in other words, the bar is going up for demonstrating leading practice
An integrated regulatory model will be supportive of an integrated GRC model
A move towards a more integrated objectives-based regulatory scheme in the US would be supportive of integrating risk and compliance activity with an approach that focuses on results and core principles.

Agenda

- Current situation
- Regulatory Considerations
- A Framework for Response
- Examples of Industry Practices
- Key Takeaways

Deep reflection is needed as to the effectiveness of risk management & compliance in its current form

- The financial markets crisis has caused inter-related challenges for companies:
  - Valuations and risk
  - Dealing with investigations and disputes
  - Developing proper liquidity management capability
  - Capital adequacy
  - Dealing with new levels of regulatory oversight
- Many organizations are now re-considering everything from organization, governance, roles, level of review, reporting and the like. Our conversation with the regulators has only reinforced the view that they are expecting significant changes

The challenge is how to enact those "changes" without triggering a new cost spiral

We recommend organizing around a core set of common principles as opposed to the existing silos

Core GRC principles

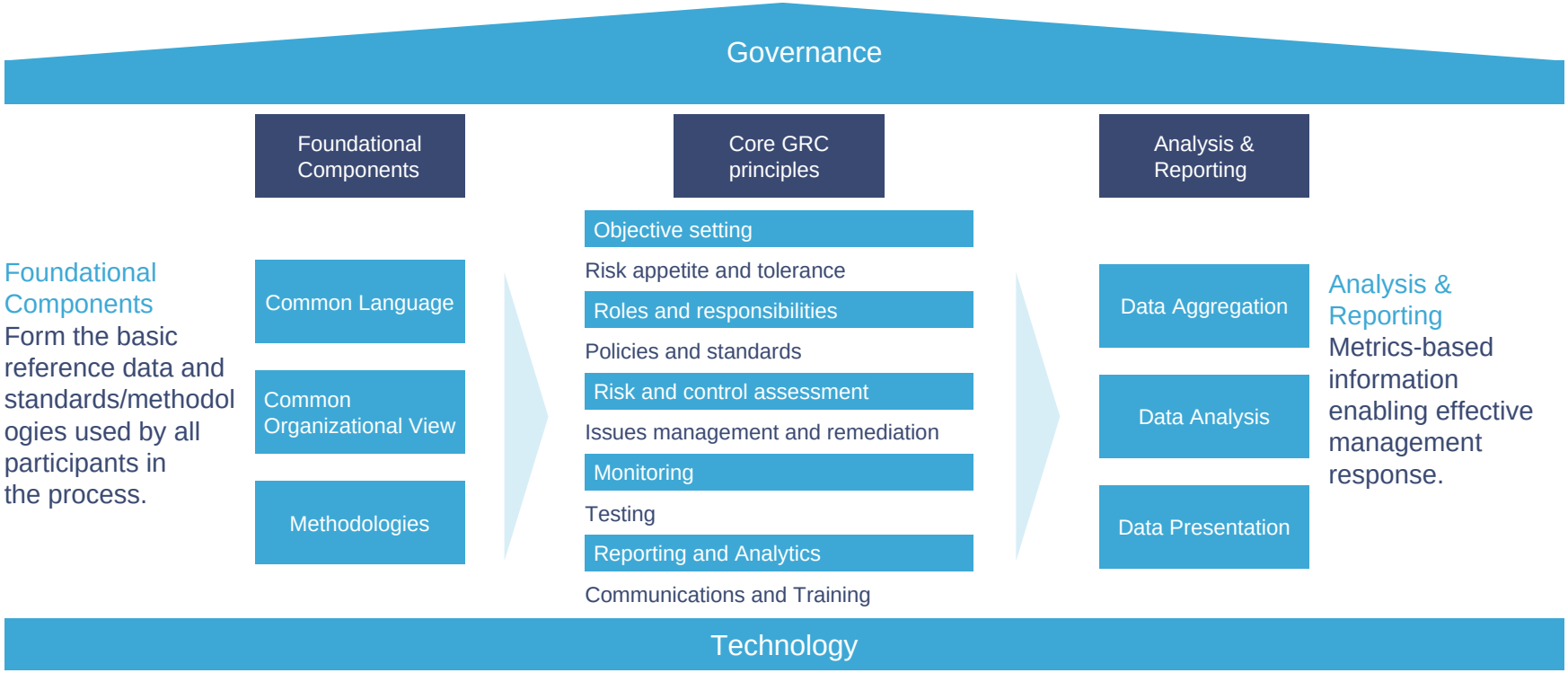
- Objective setting
- Risk appetite and tolerance
- Roles and responsibilities
- Policies and standards
- Risk and control assessment
- Issues management and remediation
- Monitoring
- Testing
- Reporting and Analytics
- Communication and training

Advantages of using a Core Principles approach:

- Establishes a common understanding of risk across the organization (e.g. business units, control functions, risk oversight functions, senior management, the board)
- Anchoring around principles allows the organization to focus on the core set of practices and utilities needed 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
- Better aligns with regulatory focus on objectives-based approach

Progress is being made through agreement on these principles, alignment of the organization and the execution of pragmatic, incremental steps

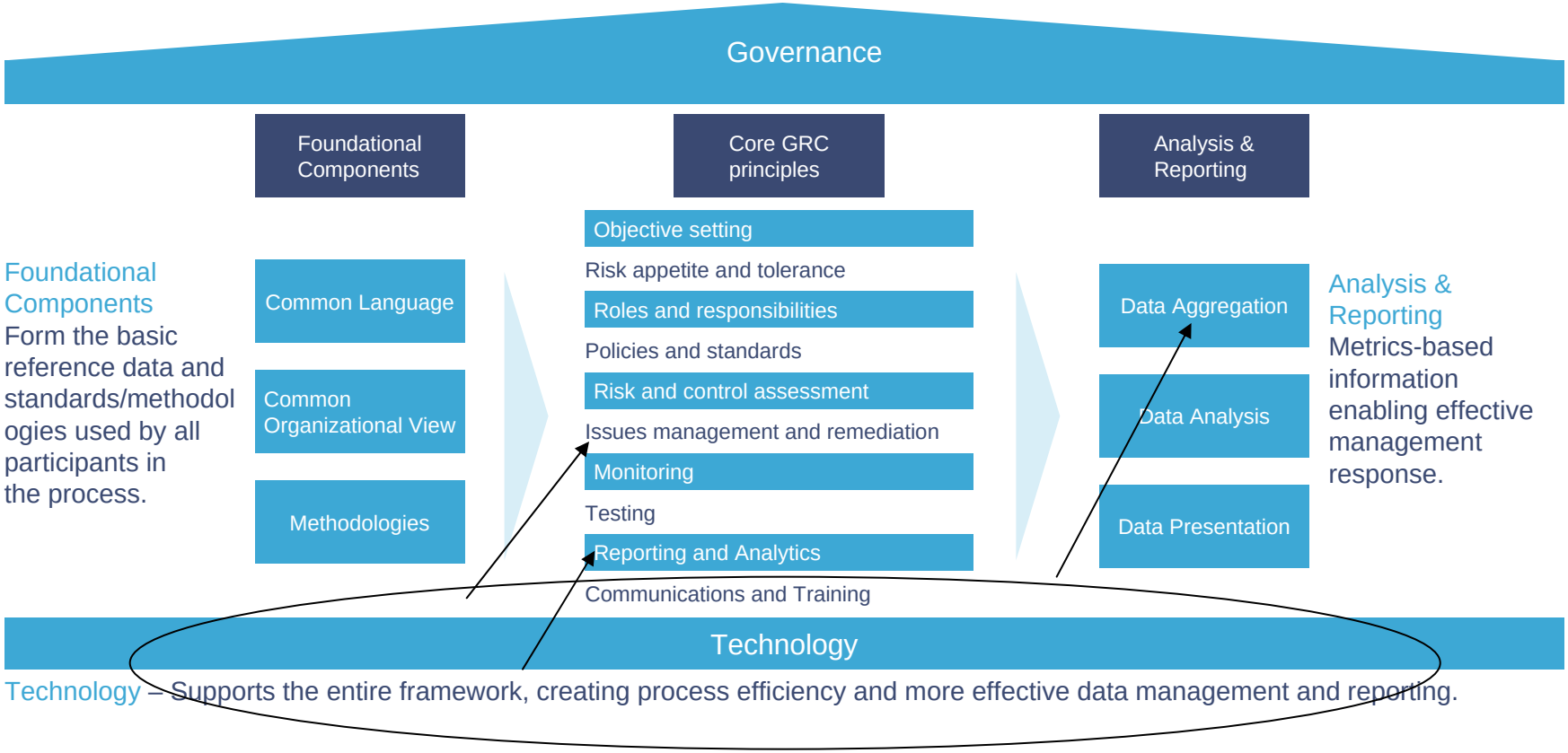
Governance – Provides leadership, consistency and accountability over the entire process. Critical roles (e.g. Internal Audit) are preserved as centers of excellence leveraging shared processes to drive greater effectiveness and efficiency.



Technology – Supports the entire framework, creating process efficiency and more effective data management and reporting.

Technology is emerging as a key enabler – We are seeing technology being leveraged to reduce cost, enhance risk information access and improve efficiency

Governance – Provides leadership, consistency and accountability over the entire process. Critical roles (e.g. Internal Audit) are preserved as centers of excellence leveraging shared processes to drive greater effectiveness and efficiency.



Technology – Supports the entire framework, creating process efficiency and more effective data management and reporting.

Look for improvements along three practical avenues

Three approaches	Questions to ask
Integrate within an oversight function	• Have you identified the unique and distinct mandate for each oversight function? • Have you aligned your risk assessments to specific business objectives? • Do you have a standardized way of approaching the requirements of new regulation?
Integrate across oversight functions	• Do you know the full costs of each oversight function? Or, of each core GRC principle (e.g. risk reporting)? • Does the organization have a consistent language and taxonomy of risk descriptions/libraries ? • Are there multiple and distinct issues and control deficiency repositories? • Has the organization conducted an inventory of its risk and control assessments?
Integrate within and across business units	• Does senior management have concise documentation of its top risks, and identified risk ownership among business leaders? • Can the business align its risk profile against acceptable risk tolerances? • Can business leadership justify its spend on controls, or show that the spend has reduced control failure?

Agenda

- Current situation
- Regulatory Considerations
- A Framework for Response
- Examples of Industry Practices
- Key Takeaways

We are seeing some sophisticated financial institutions making advances in integrating their risk management and compliance activities

	Examples of recent responses		
Core GRC Principles	Financial Institution A	Financial Institution B	Financial Institution C
Risk appetite and tolerance	Implementing a shared risk language anchored in policies	Developing a risk tolerance model for multiple risk classes	
Roles and Responsibilities	Created a costing model to evaluate and limit multiple responsibilities for CSA	Established a Risk Governance structure	Developed a Risk & Compliance Council to tackle common issues
Policies and Standards	Streamlined corporate policies and procedures framework		
Risk and Control Assessment		Rationalized 15-20 separate risk assessments under a common platform and process	Developed one risk assessment standard and methodology for consistent scoring across multiple assessments
Issues management and remediation	Developed a shared issues repository for audit and risk issues	Integrated deficiency databases and created a standard reporting mechanism	Centralized issues tracking and exceptions management process
Monitoring	Implemented global lower-cost monitoring hubs on a shared services basis	Unified monitoring of compliance action plans	Developed KRI across all businesses with Op Risk's sponsorship
Testing	Developing a central testing utility for financial and audit controls	Integrated independent testing/validation processes, technologies and repositories	A testing "czar" has been appointed for RCSA, Audit and AML
Reporting and Analytics	Mining data through electronic discovery tools for Regulatory reporting, investigations into subprinme, etc.	Created a dashboard of multiple assessments across all BUs	Risk dashboard with a common set of compliance and risk analytics
Communication and Training			Shared compliance and risk-awareness training program

Examples of achieved benefits

Benefit	Value Proposition	Examples
Cost Control	Less spend on risk, compliance and control activities. After an initial phased investment, one institution is estimating an estimated 10-20% reduction in spend in 2009	Example: Establish a standard BU risk assessment methodology that integrates several assessments (SOX, business continuity, vendor mgmt, new product, model validation), creating risk reporting across enterprise, with a practice view to meet regulatory requirements
Improved Business Leverage	Reduced process fatigue due to coordinated activities by control groups. Business freed up to focus on revenue-enhancement.	Example: Businesses will be assessed a minimal number of times by the internal risk, compliance and control groups. Results in higher quality input and more time to spend on revenue generating activities.
Better Coordination	Control functions and business risk management improve their coordination and sharing of information Better able to focus their joint efforts on the areas of most critical risks	Example: A metrics-driven control health check of individual businesses will be the product of a coordinated effort that provides an improved ability to focus resources where risk and control concerns exist.
Improved Regulatory Response	Positions a better response to regulatory expectations of a broader analytical underpinning for risk assessment, monitoring and capital adequacy activities	Example: The risk impact of a new regulation (e.g. identity theft red flags rule) was better evaluated by reviewing output from existing BU assessments, and incorporating into subsequent risk reviews
Better Visibility into Risk/Control Effectiveness	Senior management will have better information and articulation of critical emerging risks and control issues	Example: Implementing risk reporting which integrates data across all key control groups linked to critical risks will provide a consolidated view of risk for management.

Agenda

- Current situation
- Regulatory Considerations
- A Framework for Response
- Examples of Industry Practices
- Key Takeaways

Key Takeaways

- It is possible to significantly improve risk management and compliance effectiveness and lower costs
- The last decade has seen an unprecedented increase in risk management spend
- The costs of the risk management and compliance functions themselves are only a fraction of the true cost of risk and compliance activities
- The credit crisis has caused deep reflection as to the effectiveness of risk management & compliance in its current form
- Moving quickly is imperative

Key Takeaways

- A fundamental re-think of the existing frameworks is needed
- Financial institutions are beginning to organize around a core of common principles as opposed to the existing silos
- Progress is being made through agreement on these principles, alignment of the organization and the execution of pragmatic, incremental steps
- Technology is emerging as a key enabler
- Modern sourcing practices for risk and compliance services are being applied to reduce costs
- Where successful, senior management has committed to this new way of thinking and the accompanying cultural changes

For further information, please contact

Paul Mokdessi paul.e.mokdessi@us.pwc.com

312-298-3347

Carlo di Florio carlo.diflorio@us.pwc.com

646-471-2275

www.pwc.com/2008bcm

PRICEWATERHOUSECOOPERS