



The Summit on

Auditing and Governance

INTEGRATING COMPLIANCE AND CONTROLS IN THE POST-SOX ERA

Coordinated Governance: A Winning Relationship Between Internal Audit and the Organization's Other Risk and Control Functions



Coordinated Governance: A Winning Relationship Between Internal Audit and the Organization's Other Risk and Control Functions

Bonnie Howard – Chief Auditor, Citigroup, Inc.
Dick Anderson – Partner, PricewaterhouseCoopers, LLP

December 5, 2006



What's happened to companies in today's Risk and Control environment

- Issues
 - **Sox required Testing**
 - **Concern about Risks**
 - **Higher Compliance Fines**
 - **Desire for More Assurance**
- Corporate Reaction
 - **Create an Internal Control function**
 - **Create an ERM function**
 - **Expand the compliance group**
 - **Expand Internal Audit**

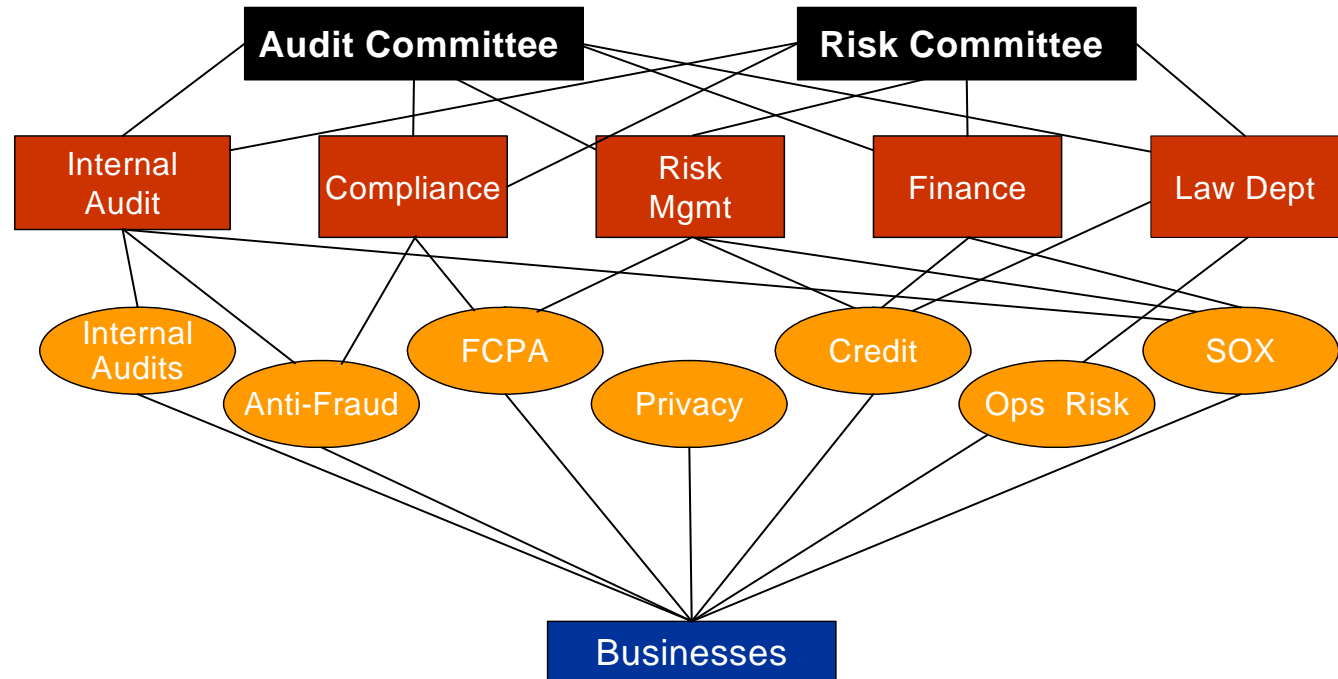


Result: A Group of Separate Risk and Control Functions

- Separately developed mandates and missions
- Separate processes
- Lack of coordination
- Duplicative efforts
- Competition for attention
- Different schedules, reporting formats

Oversight of risk and compliance activities are experiencing:

- Cost and resource explosion
- Business and Board overload
- Competition for scarce resources
- Premium pay for resources





Today's environment from the standpoint of businesses

- Significant increase in risk and compliance operating expenditures
 - **Slope of the expense curve can't continue**
- Lack of clarity around roles and responsibilities of various risk and control functions
 - **Especially in relation to each other**
- People apparently duplicating efforts



Who should drive the solution?

- First, given the magnitude of the costs and issues, *someone* in the organization will have to address this issue
- Internal Audit can:
 - **Champion the effort and help shape the right response, or**
 - **Take a “wait and see” attitude and ride along**
- Does Internal Audit have an opportunity to drive the governance processes?



How best to approach this issue?

Start at the top! You need:

- Top level support and agreement on the issue and objectives
- Principles or ground rules
 - **Organizational structures may be off the table**
 - **Unique role in internal audit (and other functions) must be recognized**
- Define who the players are
 - **Many organizations haven't really defined their governance players**
 - **You need the right players in the game**
- Recognize the maturity of your governance and risk and control environment
 - **Different approaches work at different points**



Case Study I: High level solution

- Major organization realizing that they need:
 - **Common view on risks but not ready for ERM**
 - **Coordination of risk and control groups**
 - **Organization is not ready to get into structural and reporting lines**
 - **Needed to get moving**
- Solution: Form a “Common Risk Analysis Committee”



Objectives of the Committee

- Common Risk Analysis Steering Committee – Overall Objectives
 - **Agree on a common risk management concept for various functions across the Company who deal with risk (“risk management functions”)**
 - **Maintain independence/objectivity of each risk management function**
 - **Rationalize and harmonize approaches to risk across the Company**
 - **Increase information sharing across the risk management functions**



Case Study I: High level solution

- Common Risk Management Concept
 - **Utilize common risk definitions and risk analysis framework across the company**
 - **Facilitate risk identification**
 - **Consider how the company could measure/assess risk dynamically**
 - **Facilitate ongoing discussion of the company's control processes**



Case Study I: High level solution

- Maintain Independence/Objectivity
 - **Recognize the right of any risk management function to disagree and disengage**
 - **Recognize the need to protect objectivity of the various risk management functions**



Case Study I: High level solution

- Rationalize and Harmonize Approaches
 - **Share planning schedules and strategies**
 - **Modify risk management timing/approaches as appropriate**
 - **Eliminate duplication by leveraging work done by other risk management functions**



Case Study I: High level solution

- Increase Information Sharing
 - **Evolve the “Steering Committee” into a standing “Risk Management Committee”**
 - **Increase the amount and types of information being shared**
 - **Foster an “information sharing” mindset among risk management functions**



Case Study II: Complex organization with mature risk and control functions and normal level of coordination

- Looking for logical – not necessarily all – integration opportunities
- Taking it in steps:
 - **Integration across capabilities**
 - **Linkage to business units**
 - **Operating changes**
- Starting with a pilot program and learning as you go



Case Study II: The phases are straightforward, but scoping can be difficult

- Step 1: Identify the principles framework for a detailed assessment
- Step 2: Establish the scope of the assessment
- Step 3: Analyze how “operating levers” are used to apply one or more principles
- Step 4: Prioritize, selecting one principle in one business unit for a pilot program
- Step 5: Integrate across capabilities, embed in business units and make operating changes
- Step 6: Expand pilot across another principle or business unit

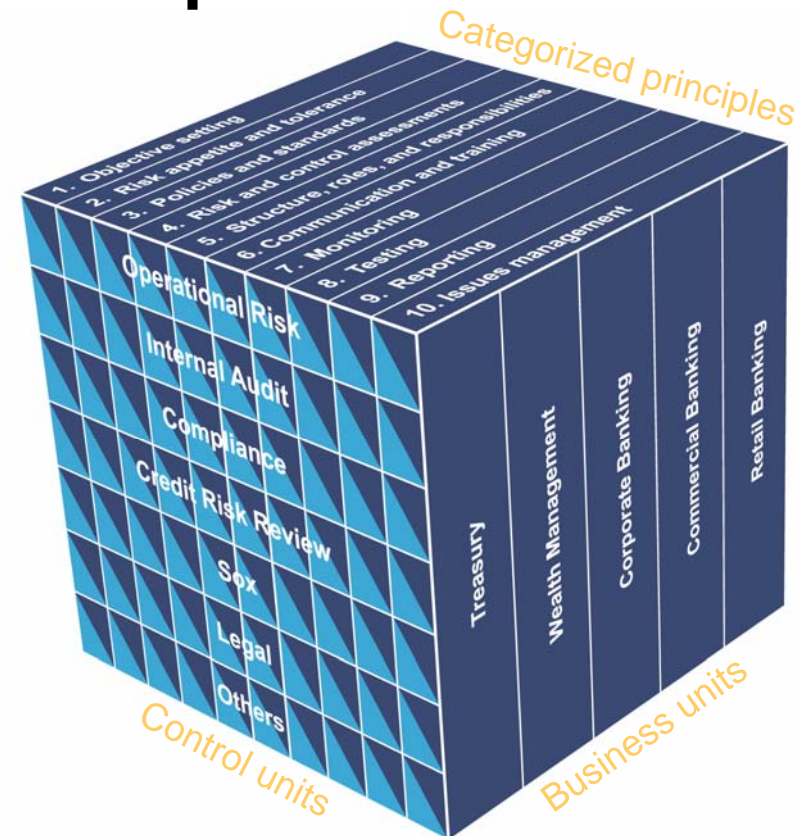


Case Study II: Example Principles

- Objective setting
- Risk appetite and tolerance
- Policies and standards
- Risk and control assessments
- Structure, roles and responsibilities
- Communications and training
- Monitoring
- Testing
- Reporting
- Issues management

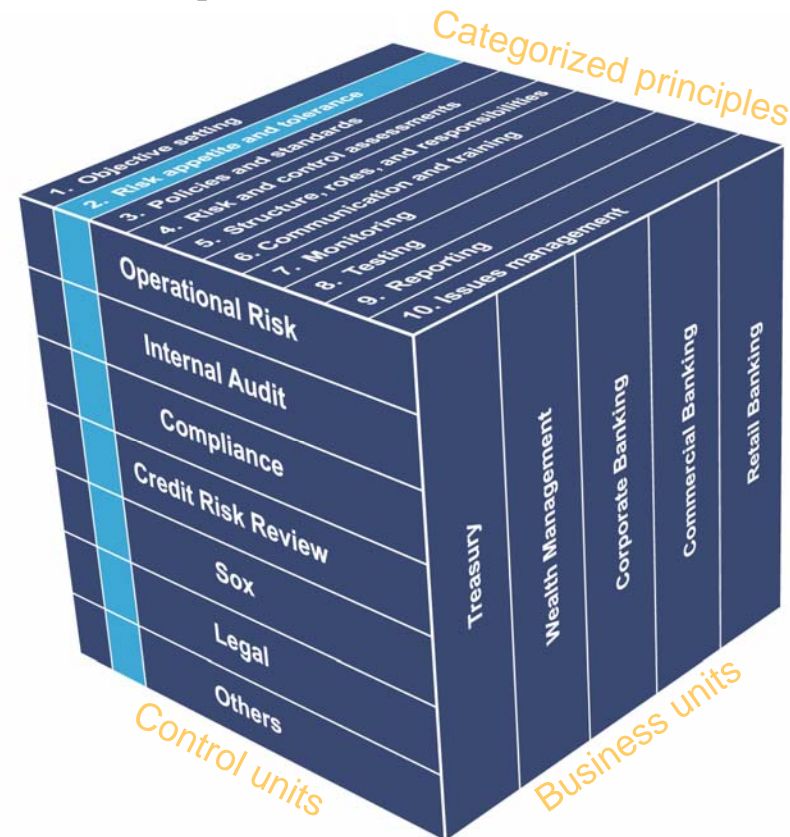
Case Study II: Scoping alternatives – baseline analysis across all business units and principles provides comprehensive roadmap

- Execute moderate depth analysis across all or a subset of all risk and compliance activities across all ten categorized principles
- Analysis yields areas for potential integration and roadmap to integration
- Provides the most comprehensive output
- Enables gaining the greatest efficiency in the shortest time frame



Case Study II: Scoping alternatives – deep dive into single principle across all existing risk/compliance activities and business units optimizes individual processes

- Execute deep dive analysis across existing risk and compliance activities of a single or small set of categorized principles
- Typically, analysis yields areas of integration and optimization for individual processes across the enterprise. Does not yield roadmap to integration
- Can also be used to optimize an activity, such as risk and control self assessment. Can be conducted on the processes, data, or both



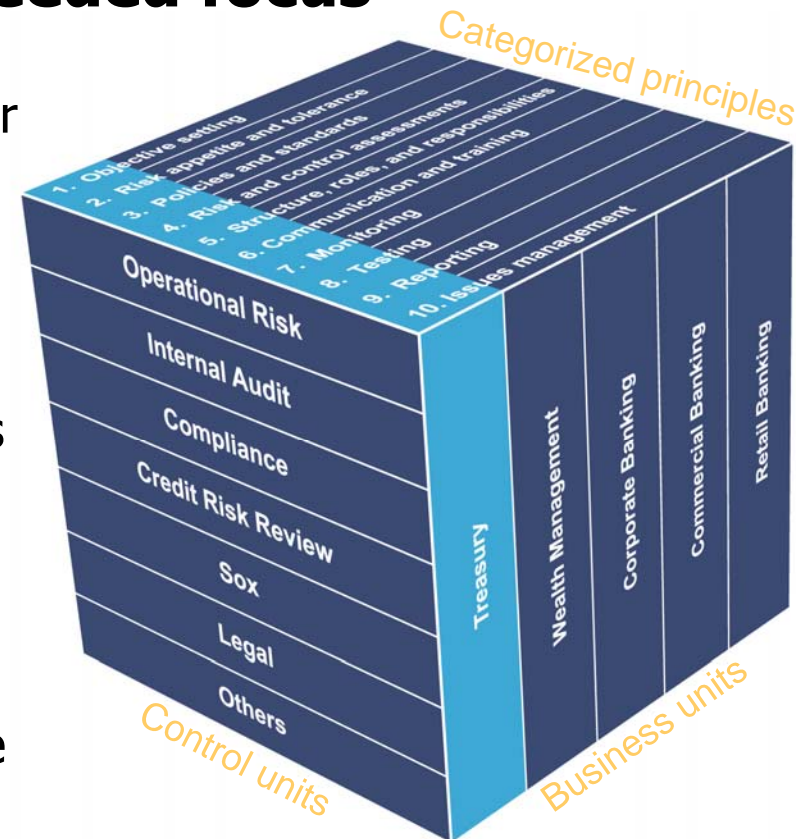


Deep dive analysis of one principle

- “Operating levers” to be researched:
 - **Processes**
 - **Technology**
 - **People**
 - **Information**
- Questions:
 - **Can they be “standardized?”**
 - **Can they be integrated/optimized?**
 - **How be data be shared?**

Case Study II: Scoping alternatives – deep dive into one business unit across all principles and activities provides needed focus

- Execute deep dive analysis across all or a subset of all risk and compliance activities and principles for a single business unit
- Analysis typically yields roadmap for business unit to be more efficient in its existing risk and compliance activities. Does not address overlap, duplication, or inefficiencies across business units
- Approach used to assist IT organizations, for instance, to organize themselves more efficiently





Case Study III: Complex Global Organization with Mature Self-Assessment Process

- Situation:
 - **As self-assessments matured...**
 - multiple and duplicative control “touchpoints” on business units (Compliance, Audit, Self-Assessment, others)
 - “Bottoms up” and “Kitchen Sink” approach – all levels of importance
 - Goals and benefits not clear
 - Costly
 - Stress and overload
 - **But ... controls became stronger and there were less ‘surprises’ – overall benefits were clear**
 - **How to do less but keep the benefits?**



Case Study III: Complex Global Organization with Mature Self-Assessment Process

- Five major steps to improve coordination:
 - **Role definitions to increase understanding and collaboration – “three layers of control”**
 - **Cross functional forums meet quarterly in all businesses, regions and countries: clear accountability to drive efficiency and effectiveness**
 - **One point person in each major business – ‘go to’ person**
 - **Agree reliance and coordination to eliminate unnecessary duplications where appropriate**
 - **Communication and training – reinforce business responsibility for control and encourage collaboration, problem solving and transparency among the control functions**



Case Study III: Complex Global Organization with Mature Self-Assessment Process

- “Project Touchpoint” goals:
 - **Reduce unnecessary, multiple control touchpoints**
 - **Develop a seamless and non-duplicative control environment**
 - **Enhance working relationship between businesses and control functions**
- Testing Coordination and Reliance Guideline
- Detailed review of all self assessments and control testing
- Identify and eliminate duplications
- Most duplications and excessive testing are in self-assessments – were able in some cases to reduce self-testing by over 50%
- Touchpoint process itself strengthened the relationship between business units and control functions.



Case Study III: Complex Global Organization with Mature Self-Assessment Process

- Challenges
 - **Change expectation that all issues will be self-identified; shift to focus on important risks**
 - **Must have senior leadership – tone and sponsorship from the top**
 - **A cultural change – permeate businesses and daily interactions**
 - **Takes time**
- But benefits can be significant !



Q&A

The Summit on
Auditing and Governance

INTEGRATING COMPLIANCE AND CONTROLS IN THE POST-SOX ERA

