

A tall, white lighthouse with a green band near the top and a dark lantern room, situated on a rocky pier extending into the ocean. The sky is clear and blue.

Deloitte.

Governance and Operational Risk

- The Heart and Achilles Heal of the
Financial Services Industry

Lawrence Lewis

November 9, 2009

Audit • Tax • Consulting • Financial Advisory •

Agenda

Introductions

Challenges in the FSI Industry

The Changing Role of the Risk and Finance Functions

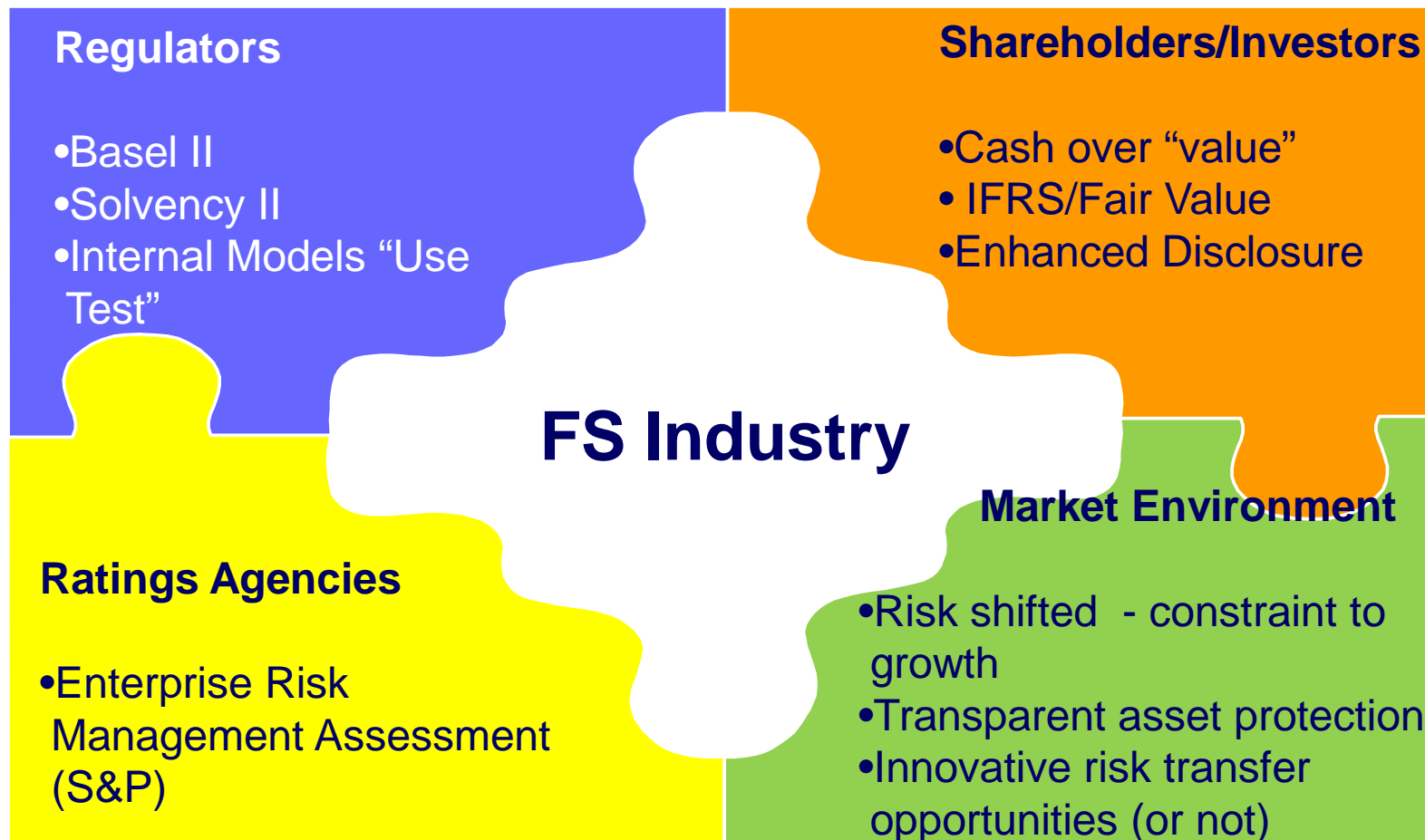
The need for Governance ERM Frameworks

The Risk Intelligent Enterprise

Conclusion

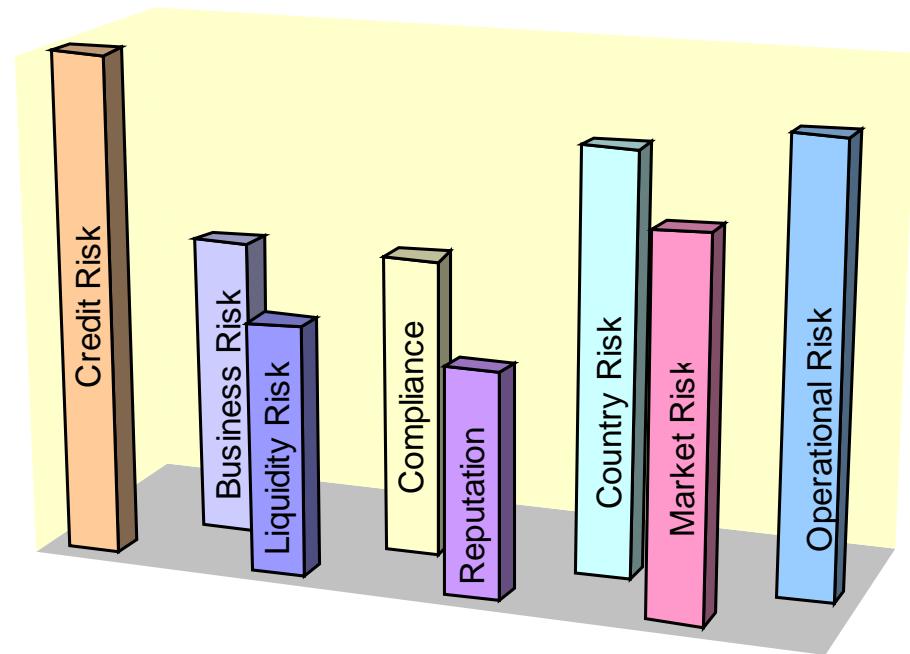
Challenges in the FS Industry

Risk Management in the FS Industry faces many new challenges that trigger change – both out of necessity and opportunity



Siloed Risk Management Based on Single Risks

Traditional approaches to managing risk focus on establishing well maintained and controlled processes around single risk factors.



While risks are often interrelated, they have historically been managed, to a large extent, as single impact events within various organizational silos.

.... the approach for evolving risk management capabilities is to build upon an institution's strengths and existing capabilities.

There are Lessons Learned from the Recent Market Turbulence

Senior Supervisors Group in its observations on risk management practices during recent market turbulence* identified factors that contributed to positive and negative performance at top institutions.

What worked:

Oversight:

- Breadth of cross-disciplinary discussions
- Active role in identifying/understanding risks
- Balance business and risk appetite

Risk measurement & reporting:

- Forward looking and adaptable approaches to risk measurement
- Wide range of risk measures to provide different views on risk
- Rigorous and independent internal processes to value complex/illiquid securities

Integrated risk management:

- Aligning treasury more closely with risk management processes and Finance
- Good interaction with business unit (BU) risk managers

Performance management:

- Appropriate BU incentives and internal pricing

What didn't work:

Oversight:

- Deficiencies in senior management oversight without appropriate focus on controls and risk mitigation activities

Risk measurement & reporting:

- Lack of forward looking scenario analysis planning that incorporates the business practices of the firm
- Over-reliance on single risk measures such as VaR and a lack of robust stress testing
- Static risk measurement techniques and inflexible risk measurement systems

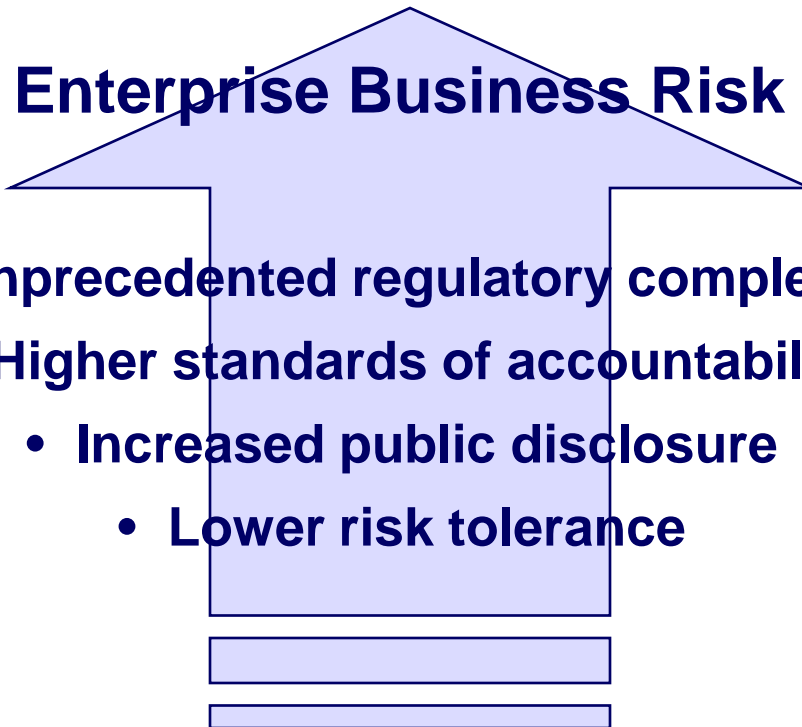
Liquidity management:

- Lack of pricing or planning for contingency funding

**Source: Senior Supervisors Group, Observations on Risk Management Practices during the Recent Market Turbulence,*

The Changing Role Of The Risk and Finance Functions

The Changing Business Risk Environment



Regulation

Sarbanes-Oxley

Basel II

SEC

NASDAQ

Governance

Board and Audit

Committee

Expectations

Capital Markets

Investors

Analysts

Lenders

Other

Competitive Pressure

Public Perception

Networked Economy

Risk and Finance Functions interrelated

Strategy

(Owned by CEO)

Where should we place our bets ?

- Market Assessment (economics, projections)
- Product Development
- Customer selection
- Competencies assessment

Financial Management

(Owned by CFO)

How should we allocate our financial resources ?

Capital Optimisation

- Risk-return trade off
- Risk tolerance diversification
- Portfolio Management
- Planning/Budget
- Capital Allocation

- Coordination of capital raising/structuring
- Monitoring and communication of capital adequacy

- Investment strategy
- Capital Efficiency Planning

- Risk Assessment
- Translation of risk appetite into limits
- Ongoing monitoring and control

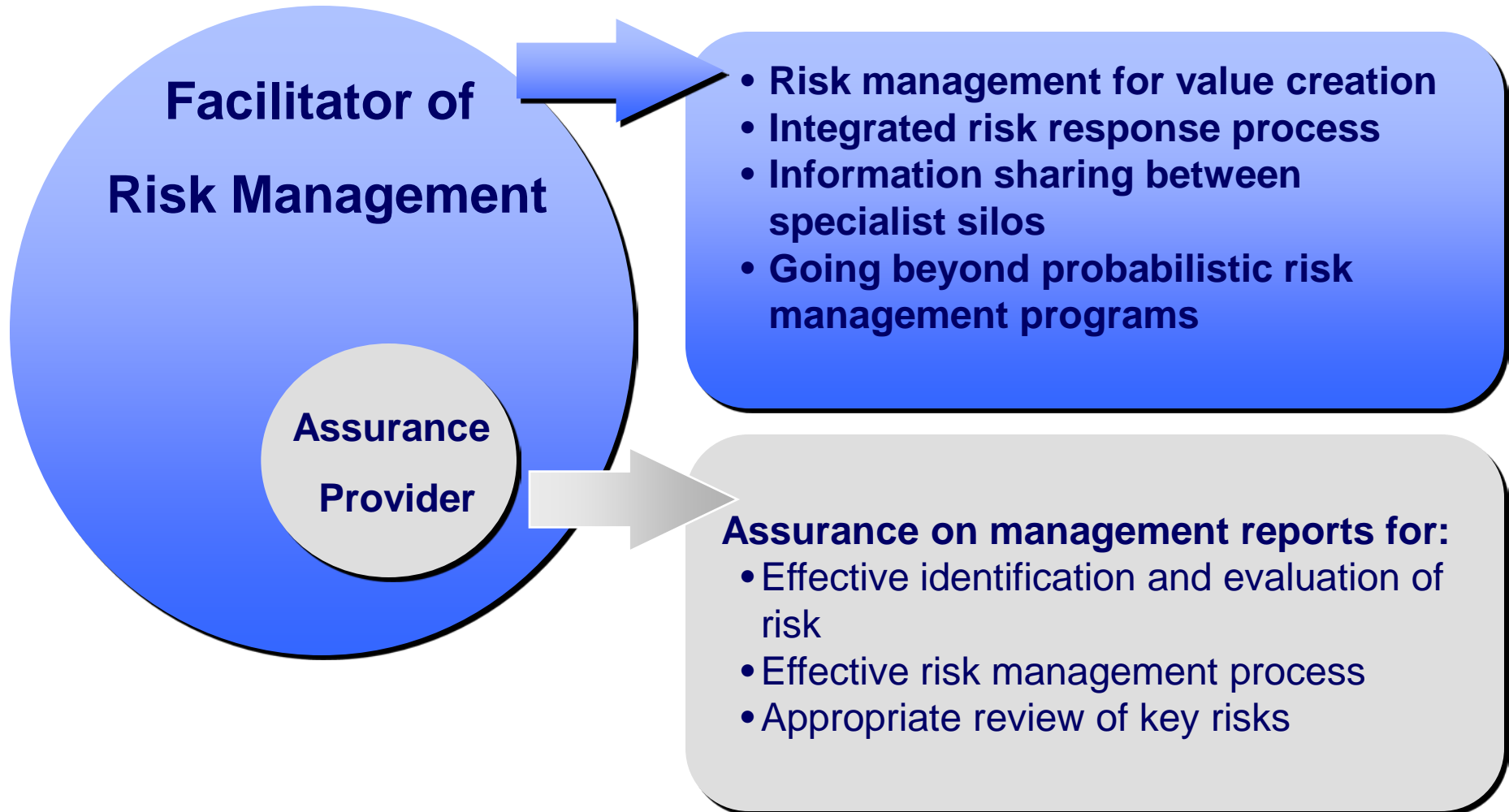
Risk Management

(Owned by CRO)

How much risk should we take ?

The convergence of Risk and Finance

From assurance provider.....To facilitator of risk management



ERM Framework to drive Governance

An ERM Framework Serves as the Guiding Vision for Risk Management

An ERM framework puts the activities of ERM in context by providing key principles and concepts, a common language, and clear guidance.

What is an ERM framework?:

- A conceptual tool to communicate the firm's risk vision;
- Defines the components of the risk management program;
- Sets out the risk methodology and interaction between components; and
- Categorizes risks and sets out a common terminology

Types of ERM Frameworks In Use:

- The COSO ERM framework is becoming more widely accepted in the U.S. and Canada
- Some organizations customize their ERM framework based on elements of COSO or other frameworks
- A framework must “fit” the organization by encompassing an approach that covers the entire organization and be flexible across jurisdictions and for a changing environment

Types and Sources of Framework in Use at Financial Institutions

Types:

1. Internal Control frameworks
2. Industry frameworks
3. Risk Management frameworks
4. Custom-built frameworks

Examples:

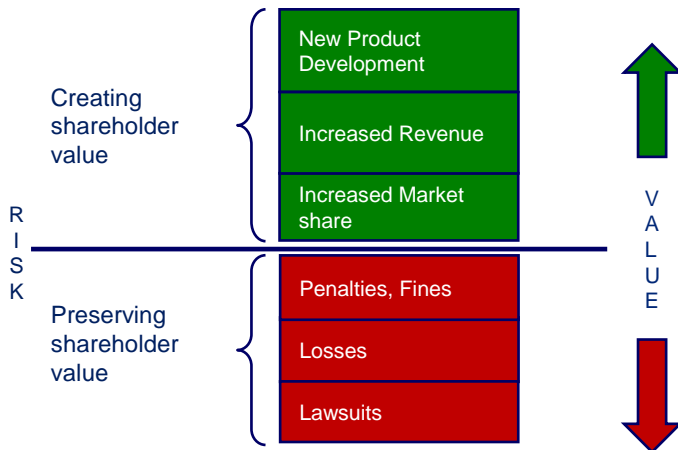
- ❑ COSO / COSO ERM
- ❑ COCO
- ❑ BASEL II / CSE
- ❑ COBIT
- ❑ LSE “Combined Code” (UK)
- ❑ AS/NZS 4360

The need for Risk Intelligence



Protecting and creating value

- Marketplace demand for board and executive accountability is intensifying
- Companies that do not effectively manage risk are being penalized by the capital markets
- Costs associated with managing risk and compliance activities are increasing



Managing in volatile times

- The recent financial crisis proves that even in a highly regulated environment, lack of effective risk management practices can have a major impact on organizations
- There is increased focus on timely and clear communications with stakeholders on how risks are being managed (board of directors, executive management, employees, bond rating agencies).
- Systemic risks and impacts on organizations have lead to significant losses in value.
- Trending for assessing future market demands and economic impacts is no longer reliable

Regulatory complexity

- Regulatory bodies and rating agencies have made it clear that greater disclosure lies ahead, guided by more specific requirements
- Regulatory examinations will most likely change, with increased focus on risk management oversight
- Global regulations are increasing in volume and complexity, increasing the importance of compliance and risk management

Benefits of improved Risk Intelligence

Risk Intelligence is a management approach that leverages risk for value creation and preservation

Characteristics of a Risk Intelligent Enterprise

- Risk management practices that encompass the entire business, creating connections between the so-called “silos” that often arise
- Risk management strategies that address the full spectrum of risks
- Risk assessment processes that augment the conventional emphasis on probability by placing significant weight on vulnerability
- Risk management approaches consider single events and take into account risk scenarios and the interaction of multiple risks
- Risk management practices that are infused into the corporate culture, so that strategy and decision-making evolve out of a risk-informed process
- Risk management philosophy that focuses not solely on risk avoidance, but also on risk-taking as a means to value creation

Competitive benefits of improved Risk Intelligence

- Improved ability to prevent, quickly detect, correct, escalate and respond to critical risk issues
- Reduced burden on business operations by standardizing risk management principles, language and decision-making
- Reduced cost of risk management by improved sharing of risk information and integration of existing risk management functions
- A means to improve strategic flexibility for both upside and downside scenarios. Better risk-reward decisions by quantifying impact on value
- The ability to provide a “comfort level” to the board and other stakeholders that the full range of risks is understood and managed
- The ability to manage expected risk exposure within acceptable risk appetite
- Preparedness for rating agency’s increased focus on risk management capability

Building a Risk Intelligent Enterprise

Risk Intelligent Enterprises adopt a balanced perspective of risk management supported by fundamental principles:

Nine Principles for Building a Risk Intelligent Enterprise

Governing Bodies Responsibility

Roles & Responsibilities

Common Definition of Risk

Common Risk Framework

Common Risk Infrastructure

Executive Management Responsibility

Objective Assurance and Monitoring

Business Unit Responsibility

Support of Pervasive Functions

The Risk Intelligent Enterprise



.... using the nine fundamental principles

Risk Governance

- A common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization
- A common risk framework supported by appropriate standards is used throughout the organization to manage risks.
- Key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization
- Governing bodies (e.g., Boards, Audit Committees, etc.) have appropriate transparency and visibility into the organizations risk management practices to discharge their responsibilities

Risk Infrastructure & Management

- A common risk management infrastructure that is used to support the business units and functions in the performance of their risk responsibilities
- Executive management is charged with designing, implementing and maintaining an effective risk program
- Other functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

Risk Ownership

- Business units are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management
- Certain functions have a pervasive impact on the business and not only provide support to the business units as it relates to the organization's risk program, but also enhance and enable success when strategically aligned and considered as essential elements of the program



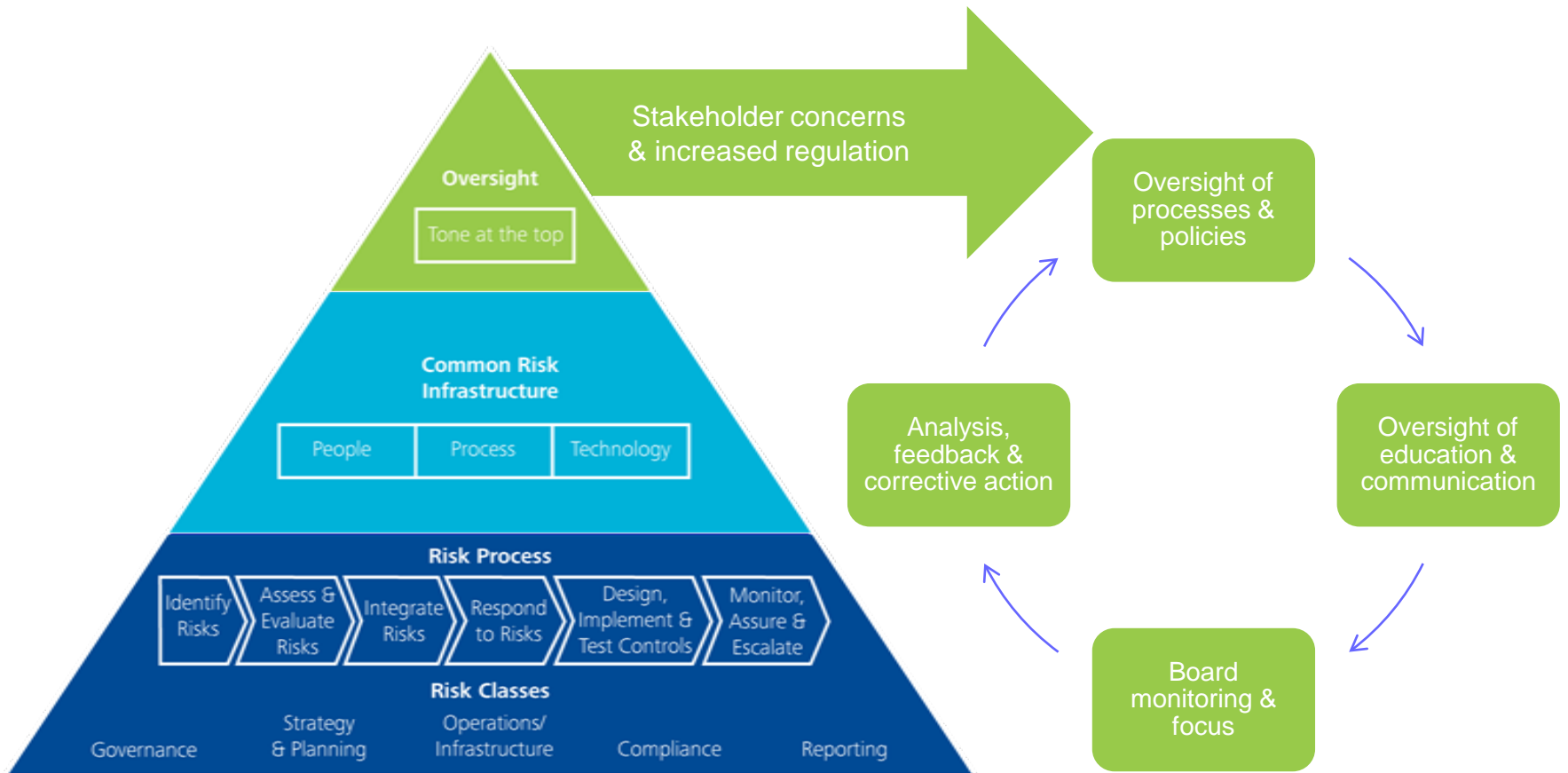
Assessing the maturity of risk management capabilities



Initial	Fragmented	Top Down	Integrated	Risk Intelligent
---------	------------	----------	------------	------------------

- | | | | | |
|--|---|---|--|---|
| <ul style="list-style-type: none"> • Ad hoc/chaotic • Depends primarily on individual heroics, capabilities, and verbal wisdom | <ul style="list-style-type: none"> • Independent risk management activities • Limited focus on the linkage between risks • Limited alignment of risk to strategies • Disparate monitoring & reporting functions | <ul style="list-style-type: none"> • Common framework, program statement, policy • Routine risk assessments • Communication of top strategic risks to the Board • Executive/Steering Committee • Knowledge sharing across risk functions • Awareness activities • Formal risk consulting • Dedicated team | <ul style="list-style-type: none"> • Coordinated risk management activities across silos • Risk appetite is fully defined • Enterprise-wide risk monitoring, measuring, and reporting • Technology implementation • Contingency plans and escalation procedures • Risk management training | <ul style="list-style-type: none"> • Risk discussion is embedded in strategic planning, capital allocation, product development, etc. • Early warning risk indicators used • Linkage to performance measures and incentives • Risk modeling/scenarios • Industry benchmarking used regularly |
|--|---|---|--|---|

Value and risk oversight process for boards



The Risk Intelligent Enterprise™

The Risk Intelligent Framework



The Risk Intelligent Framework



Governance: The risk culture of the organization. Management's philosophy on managing risk.

People: The right people, with the right training and appropriate levels of authority.

Process: The phases of identifying and responding to risk, expanded upon in the inner circle

Technology: Establishing the right systems to analyze and communicate risk information throughout the organization.

The Risk Intelligent Framework



Develop and Deploy Strategies:

Strategies are developed for creating and preserving value

Identify Risks: Identification of internal and external risks to the achievement of the entity's objectives. Risks are considered as scenarios and chains of events rather than as isolated incidents. This includes risks to both future growth objectives and risks to existing assets.

Assess and Measure Risks:

Consider (1) the extent to which potential events may have an impact on achievement of objectives and (2) the net exposure of the business after taking into account current risk mitigation and controls.

The Risk Intelligent Framework



Respond to Risks: The response plan considers all possible alternatives, including whether to avoid a risk, accept it (and mitigate where possible) and/or transfer it. Resources are prioritized and allocated, and the selected plan is executed.

Design & Test Controls: Control activities are the policies, procedures and systems that help ensure that management's risk responses are carried out. Controls must be periodically tested by independent functions to ensure they are designed appropriately and operating as intended.

The Risk Intelligent Framework



Monitor, Assure & Escalate: Monitoring is the periodic or continuous observation of the enterprise's portfolio of risk exposures in order to detect and give timely warning of change. Escalation is a procedure by which risks that exceed or are about to exceed specified thresholds or triggers are elevated to the appropriate level of authority for resolution on a timely basis.

The Risk Intelligent Framework



Sustain & Continuously Improve: Risk intelligence should be sustainable and depends on the capability of people, processes and systems to act in an integrated, coordinated and timely manner. Improvement of effectiveness and efficiency is always possible, so risk management processes should be continuously reevaluated and improvements implemented.

The Board's role

Some boards of directors are subjected to
“The Mushroom Treatment”

Keep them in the dark...

- Put risk on the agenda
- Inventory the current risk structure
- Summon the management team
- Discuss risk scenarios
- Check organizational appetite — and diet
- Get reasonable assurance and independent reassurance



Executive management's role

“We manage risk every Friday”

Everyone has responsibility for risk. But if you're a member of the executive team, this obligation is ratcheted even higher. You are tasked with tone, direction, design, and metrics.

Inherent in your executive role is leadership and authority. And you need to exercise it:

- To get people thinking about risk taking for reward
- To push risk management through all the layers of the organization
- To set expectations
- To ensure accountability
- To engage the board
- To drive change
- To establish a Risk Intelligent culture



Business units and supporting functions' roles

If you own the business unit, you own the risk

So everyone's responsible for risk. But who "owns" it? In our view, the business units hold the title and deed.

If you are accountable for the success of a business unit, you have primary responsibility for the day-to-day management of the risks associated with that unit.

What does ownership entail? Among other things, risk owners have the responsibility to:

- Identify, measure, monitor, control, and report on risks to executive management;
- Promote risk awareness;
- Reprioritize activities as dictated by effective risk analyses



Conclusion

In the recent past, financial services was perceived as paragon of sophisticated risk management...then the subprime crisis swept billions from corporate balance sheets.

What did we learn?

- 1) The potential interaction of multiple risks was underestimated or disregarded.
- 2) Probabilistic modeling was overemphasized; shortcuts were taken; scenario planning was underutilized; transparency into potential issues was absent.
- 3) Risk managers were isolated in silos.
- 4) Warnings were ignored; those who delivered them were dismissed as naysayers or criticized for not being team players.
- 5) A short-term perspective with a single-minded focus on making the quarterly numbers predominated.

Conclusion

6) Companies lacked a comprehensive approach to firm-wide risk management; authority and responsibility were poorly controlled and defined.

7) Risk management often focused on compliance rather than performance, leading to inadequate assessments and responses.

All were significant breakdowns, to be sure, yet it would be an even greater failure if companies responded by turning risk averse. Risk taking for reward is a fundamental precept of capitalism, ingrained in the financial services industry and should be encouraged. But the pursuit of organizational success must be handled skillfully.

In other words,

It's time to be Risk Intelligent

Deloitte.