State of the Art: Risk Management

Jeff M. Spivey, CPP
President
Security Risk Management

Risk Management

Jeff Spivey, CPP
President
Security Risk Management, Inc.

State of the Art

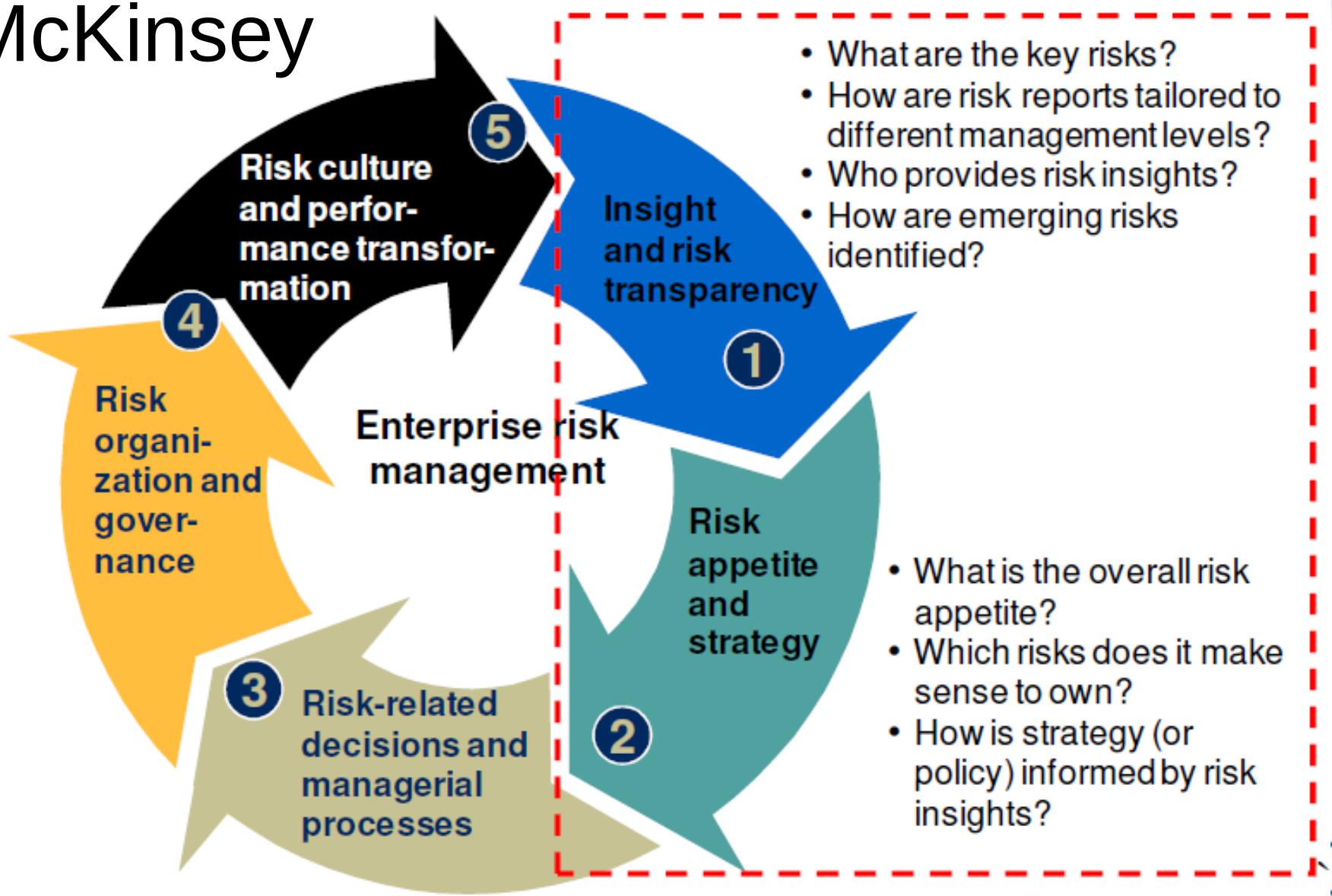
CSO Perspectives

CSO

Challenge the traditional assumptions about risk and risk management based on models inappropriate for the 21st century enterprise

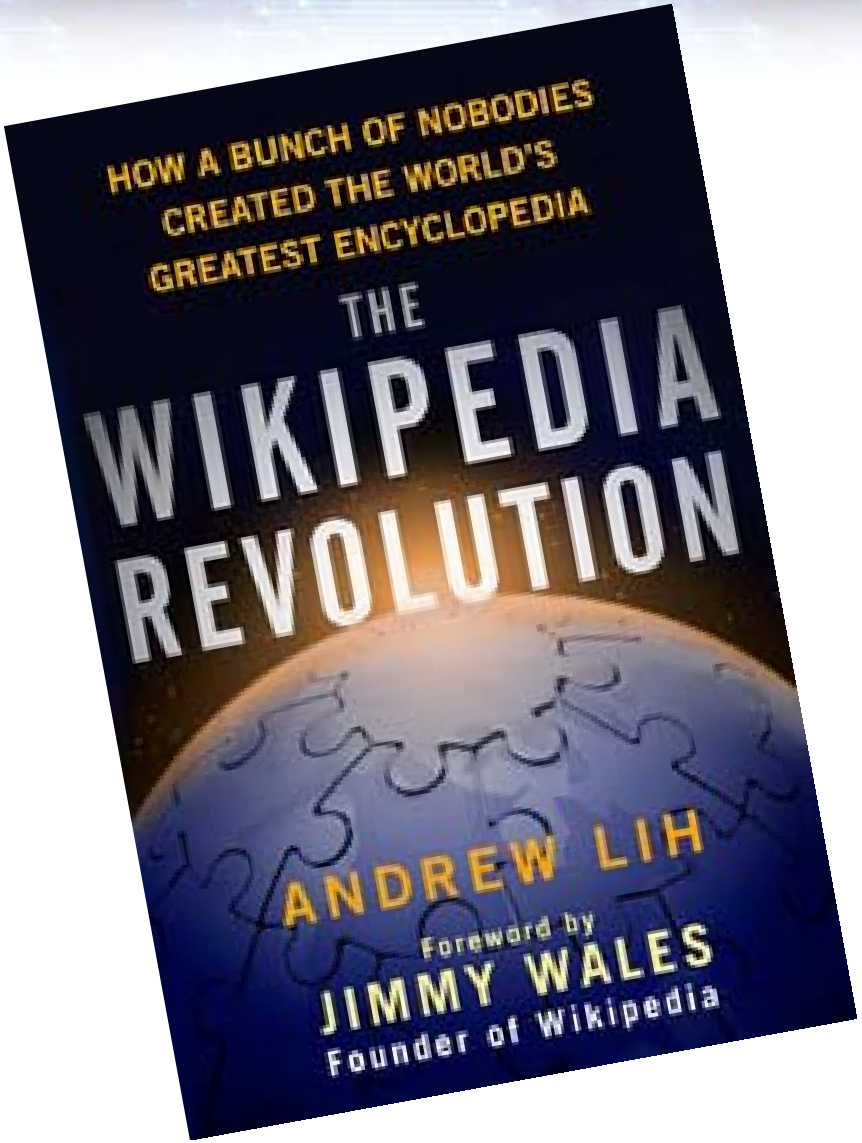
Awareness
Uncertainty
Horizon Scanning
Enterprise Risk Management
Holistic
Agility

McKinsey


Risk culture and performance transformation
5
Insight and risk transparency
1
Risk appetite and strategy
2
Risk-related decisions and managerial processes
3
Risk organization and governance
4
Enterprise risk management
• What are the key risks?
• How are risk reports tailored to different management levels?
• Who provides risk insights?
• How are emerging risks identified?
• What is the overall risk appetite?
• Which risks does it make sense to own?
• How is strategy (or policy) informed by risk insights?

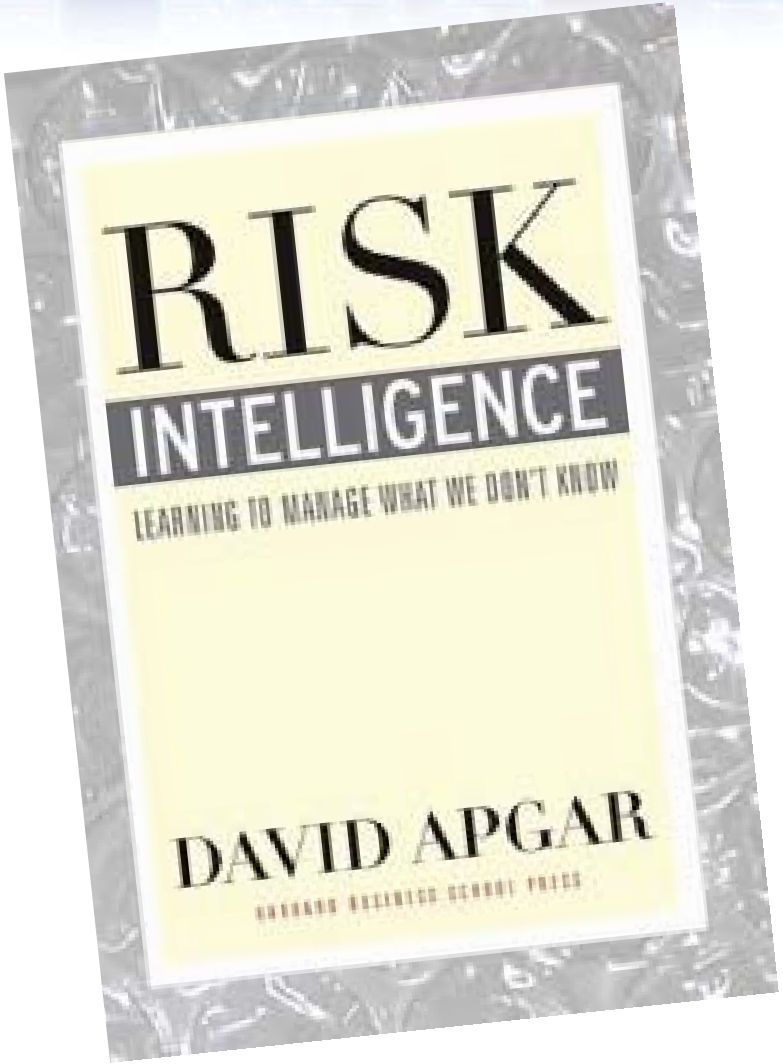
"Real Innovation in Technology Involves a Leap Ahead“

April 1, 2010


HOW A BUNCH OF NOBODIES CREATED THE WORLD'S GREATEST ENCYCLOPEDIA
THE WIKIPEDIA REVOLUTION
ANDREW LIH
Foreword by
JIMMY WALES
Founder of Wikipedia

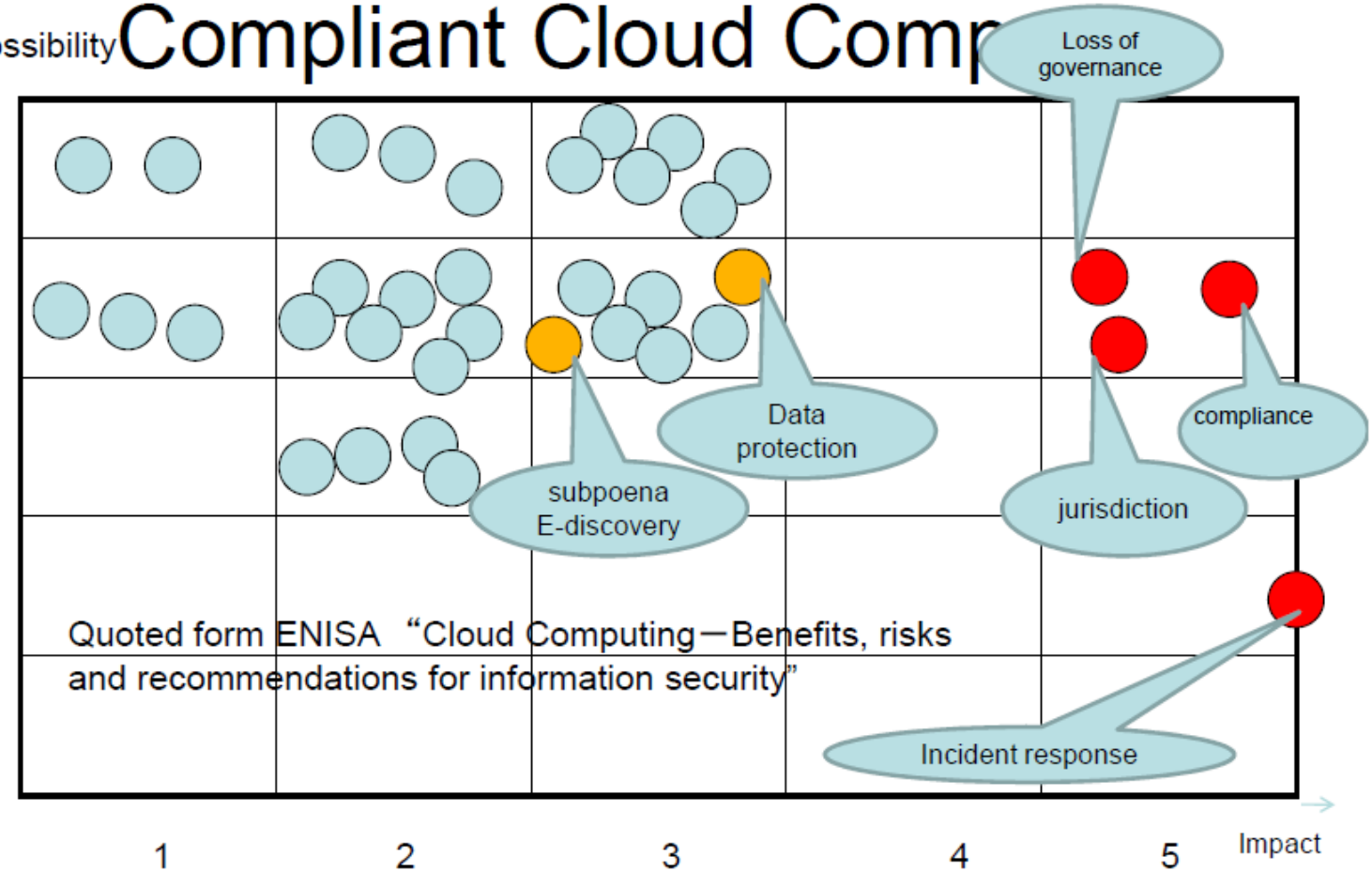
July 13, 2009

Justice Department is Creating Barriers to Companies Trying to Create New Technologies



Learning to Manage what we Don't Know

Risk analysis for Compliant Cloud Comp



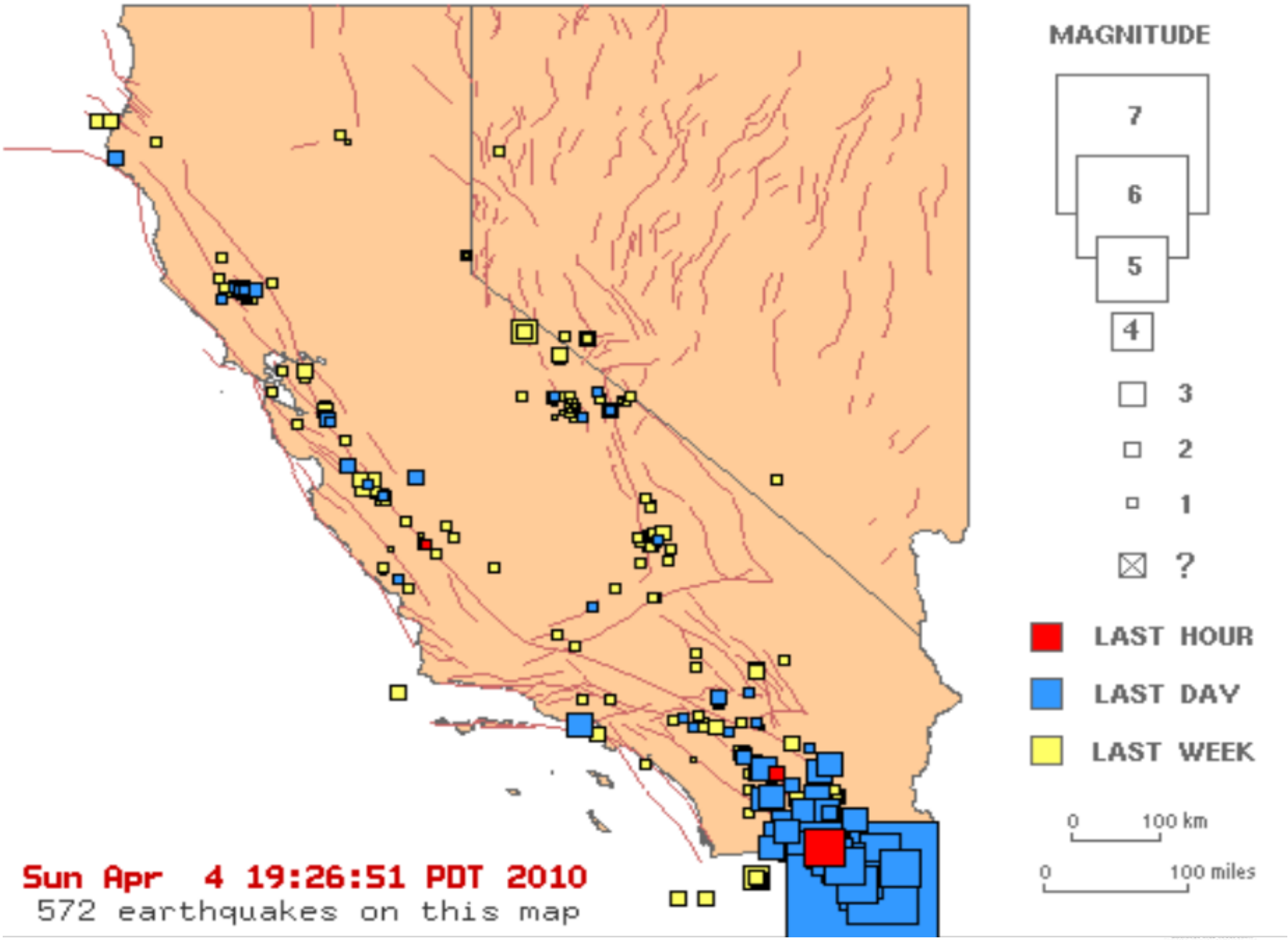
State of the Art

CSO Perspectives

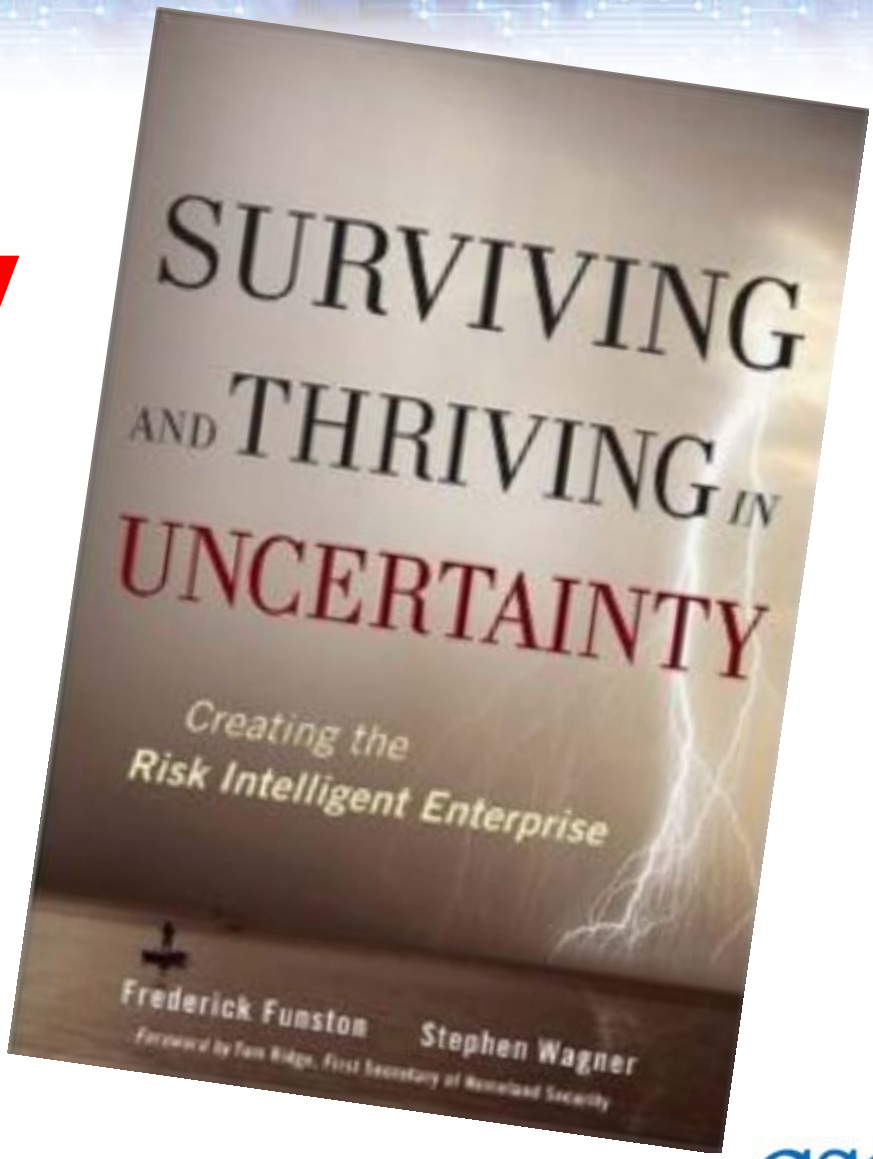
the Future

February 7, 2010

CSO


MAGNITUDE
7
6
5
4
3
2
1
?
LAST HOUR
LAST DAY
LAST WEEK
0 100 km
0 100 miles
Sun Apr 4 19:26:51 PDT 2010
572 earthquakes on this map

Uncertainty
& Complexity



conventional risk management has failed

New Era of Risk Management
New Congressional Report: A Call to Action for ERM Regulation

Yesterday the Congressional panel overseeing the Troubled Asset Relief Program (TARP) program released a scathing report of the regulatory failures that led to the current financial crisis, **Congressional Oversight Panel Special Report on Regulatory Reform**.

The report concluded **"The regulatory system not only failed to manage risk, but also failed to require disclosure of risk through sufficient transparency"**.

Steve Minsky, Logic Manager

SEC Ruling

The newly proposed SEC ruling goes beyond the executive level to target risk management competency at all employee levels that materially impact the company.

- Boards will soon be required by the SEC to report in depth on how their organizations identify risk, set risk tolerances, and manage risk/reward tradeoffs throughout the enterprise.
- Intended to address the current problem, isolation of the risk management process from both the front line and the board at most organizations.

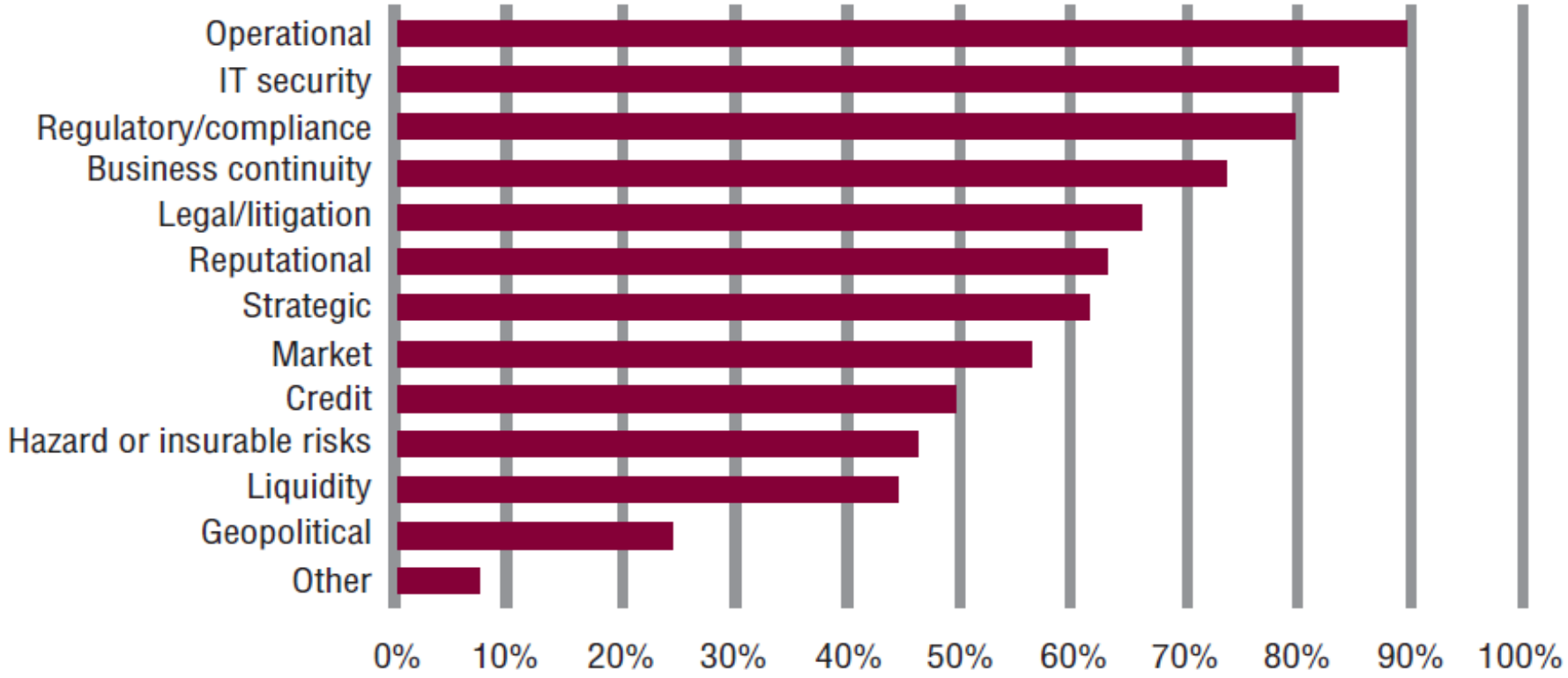
SEC Ruling

Figure 1—Shifts in Thinking: People, Processes and Strategy

	Operating Levers	FROM	TO
Strategy	Risk Management	Asset-based view	Enterprisewide view
	Governance	Passive and infrequent	Active board involvement
Processes	Budget Processes	"Not my domain"	Common language with peers
	Standards and Guidelines	Functionally focused	Common and shared widely
	Integration	Forced	Adaptive
	Business Case	Technical/jargon-filled or none	"C-suite" language
People	Roles and Responsibilities	Functionally defined	Multiple competencies
	Leadership	Command and control	Empowering and enabling
	Knowledge of the Business	Functional knowledge	Broad business understanding

Source: Booz Allen Hamilton

Figure 3—Risks Included in an ERM Program



Results may not total 100 percent as respondents were allowed to select more than one answer.

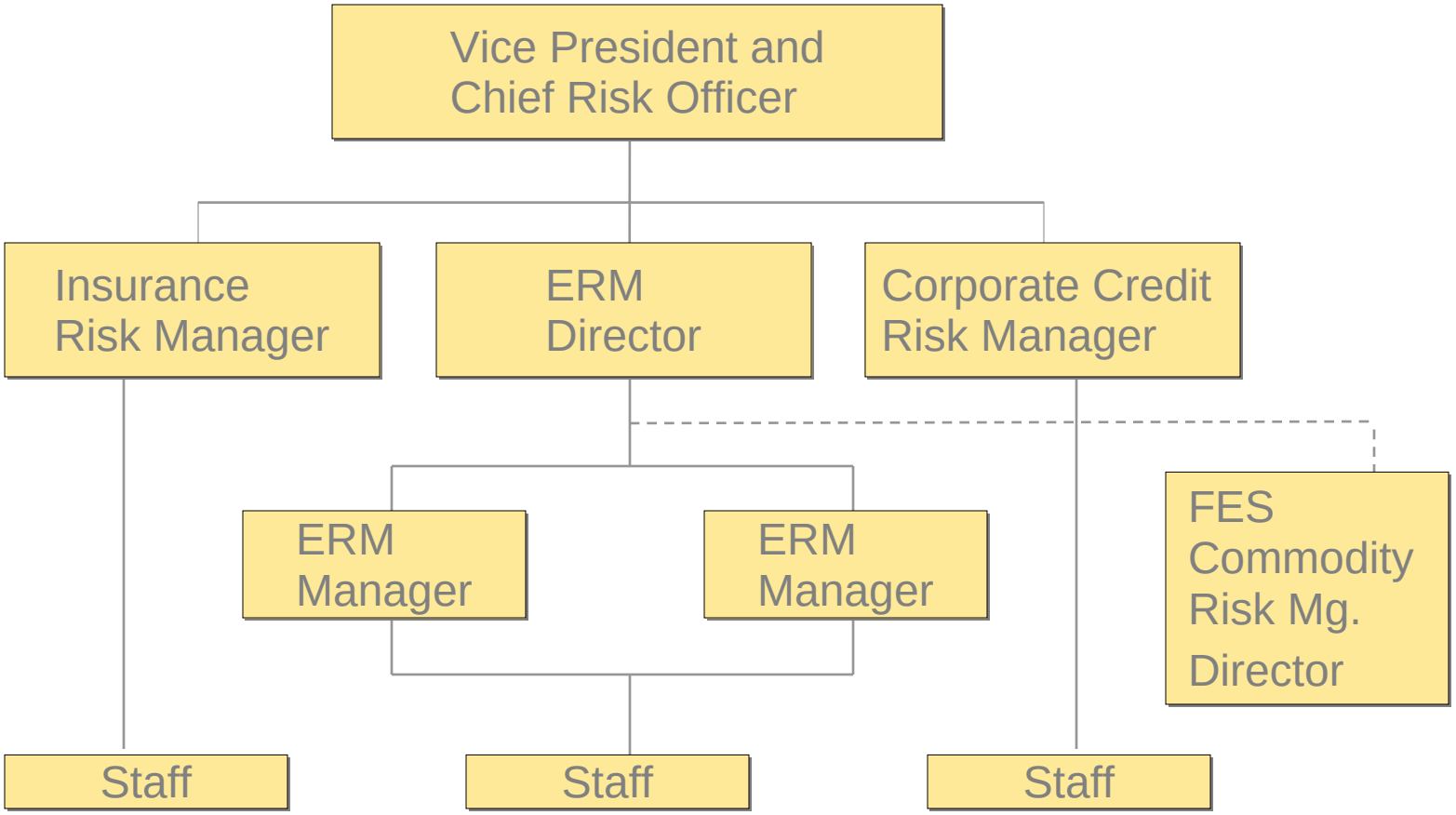
Role of ERM in the Convergence of Security

www.aesrm.org

CSO

Explain the difference between information security and information risk management

Justify the introduction of the risk office and the position of the chief risk officer


Vice President and Chief Risk Officer
Insurance Risk Manager
ERM Director
Corporate Credit Risk Manager
ERM Manager
ERM Manager
FES Commodity Risk Mg. Director
Staff
Staff
Staff

Why ERM Is Important

Every entity, whether for-profit or not, exists to realize **value** for its stakeholders.

Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

COSO

Today's organizations are concerned about

Risk Management
Governance
Control
Assurance (and Consulting)

ERM Defined:

"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

Why ERM Is Important

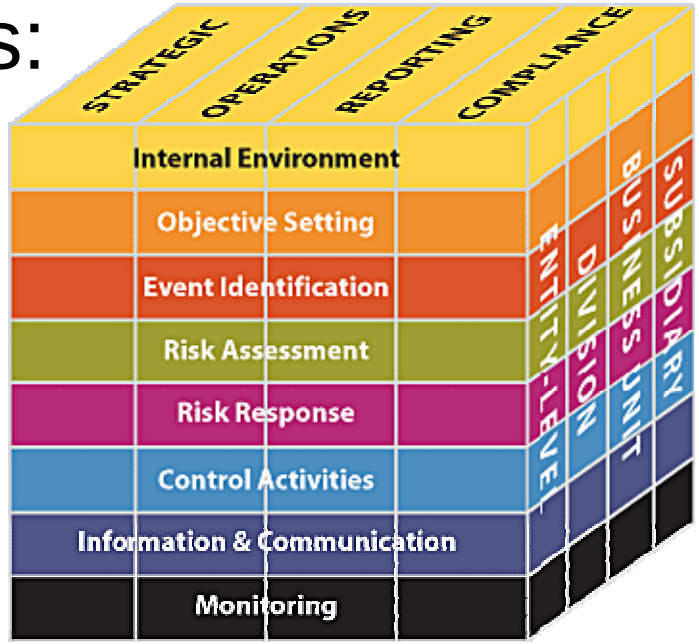
ERM supports value creation by enabling management to:

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

The ERM Framework

Entity objectives can be viewed in the context of four categories:

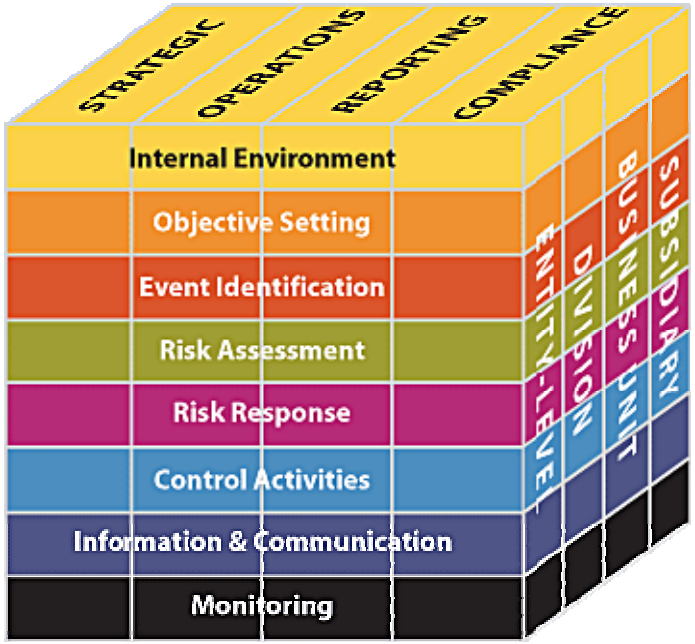
- Strategic
- Operations
- Reporting
- Compliance



The ERM Framework

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit processes



Internal Environment

Establishes a philosophy regarding risk management. It recognizes that unexpected as well as expected events may occur.

Establishes the entity's risk culture.

Considers all other aspects of how the organization's actions may affect its risk culture.

Risk tolerance…

the acceptable level of variation around objectives, is aligned with risk appetite.

IS a RISK AN OPPORTUNITY?

Manage and Capitalize on Business Risk

Enterprises achieve return by taking risks
Some try to eliminate the very risks that drive profit
Guidance was needed on how to *manage* risk effectively

Treating a RISK

REITA- E

Risk Intelligence

- Involves identifying those incidents, occurring internally or externally, that could affect strategy and achievement of objectives.
- Addresses how internal and external factors combine and interact to influence the risk profile.

Risk Intelligence

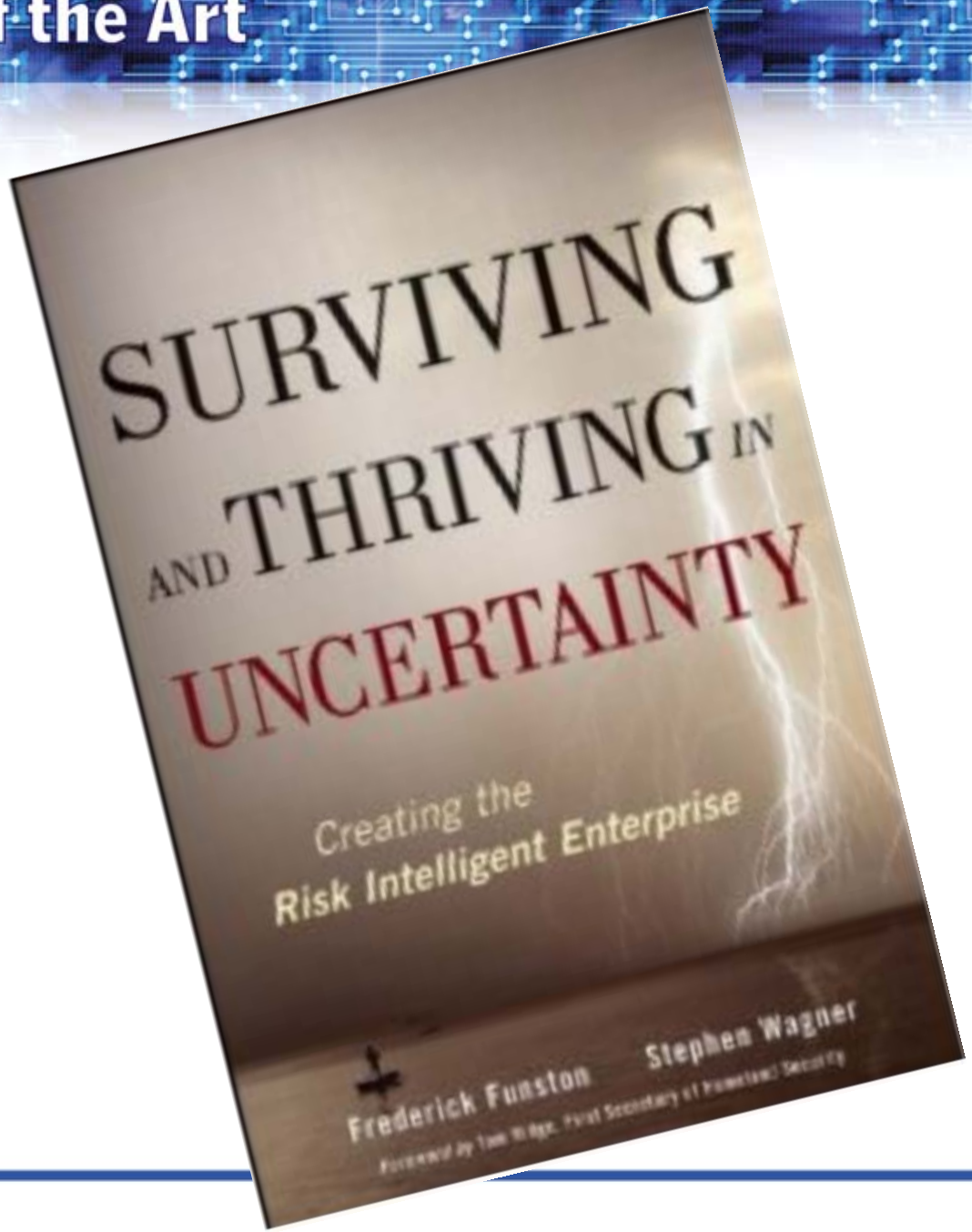
- Challenging basic business assumptions can help identify "Black Swans" and provide first-mover advantage
- Defining the corporate risk appetite and risk tolerances can help reduce
- The risk of ruin.
- Taking a longer-term perspective can aid in identifying the potential unintended consequences of short-term decisions.

Risk Intelligence

- Anticipating potential causes of failure can improve chances of survival and success through improved preparedness.
- Factoring in velocity and momentum can improve speed of response and recovery.
- Verifying sources and the reliability of information can improve insights for decision making and thus decision quality.

"Risk intelligence is dynamic. There is no set of rules to follow, no permanent certification, no way to insulate the organization from the forms that uncertainty and turbulence will take in the future. Rather, there is only a path to creating value and managing risks that enables better decisions

Fred Funston, Intelligent Enterprise


SURVIVING
AND THRIVING IN
UNCERTAINTY
Creating the
Risk Intelligent Enterprise
Frederick Funston
Stephen Wagner

These are important

Risk Culture
Risk Intelligence
(The Intelligent Enterprise)
Risk Tolerance
Exploiting Risks

Risk Management Innovation

Dave Snowden suggest there are three necessary conditions for innovation to take place.

- **Starvation** of familiar resource, forcing you to find new approaches, doing things in a different way;
- **Pressure** that forces you to engage in the problem;
- **Perspective Shift** to allow different patterns and ideas to be brought into play.

Thank You !

Jeff M. Spivey, CPP
JSpivey@srmsig.com
Jeff.Spivey@riskiq.com
704-521-8401