



FINANCIAL SERVICES A D V I S O R Y

K P M G L L P

Global Advisory

## Tuning Risk for Return

Jonathan Rosenoer

- June 25, 2008
- ADVISORY

***"All of life is the management of risk,  
not its elimination."***

Walter Wriston

## The rise of extreme events

- IT-driven extreme events are occurring with increased frequency and severity.
- These events may be a power law phenomenon
  - ❑ They do not exist as random anomalies that occur to others and can be disregarded
  - ❑ They are likely a function of the new role of IT as the principal factor of production, the inter-networking of systems across enterprise boundaries, and feedback dynamics.

# Industrial age tools are not proving sufficient for today's business risks

- Controls review
  - Focus on existence and quality of control process, **not direct testing** of effectiveness
- Audit
  - Not a proxy for a holistic risk management process
  - Do **not provide total assurance** or guarantee
- Regulation
  - Highly prescriptive and rules-based industrial age regulation **focus on discrete violations and correction**
  - Compliance functions siloed and replicated throughout companies.

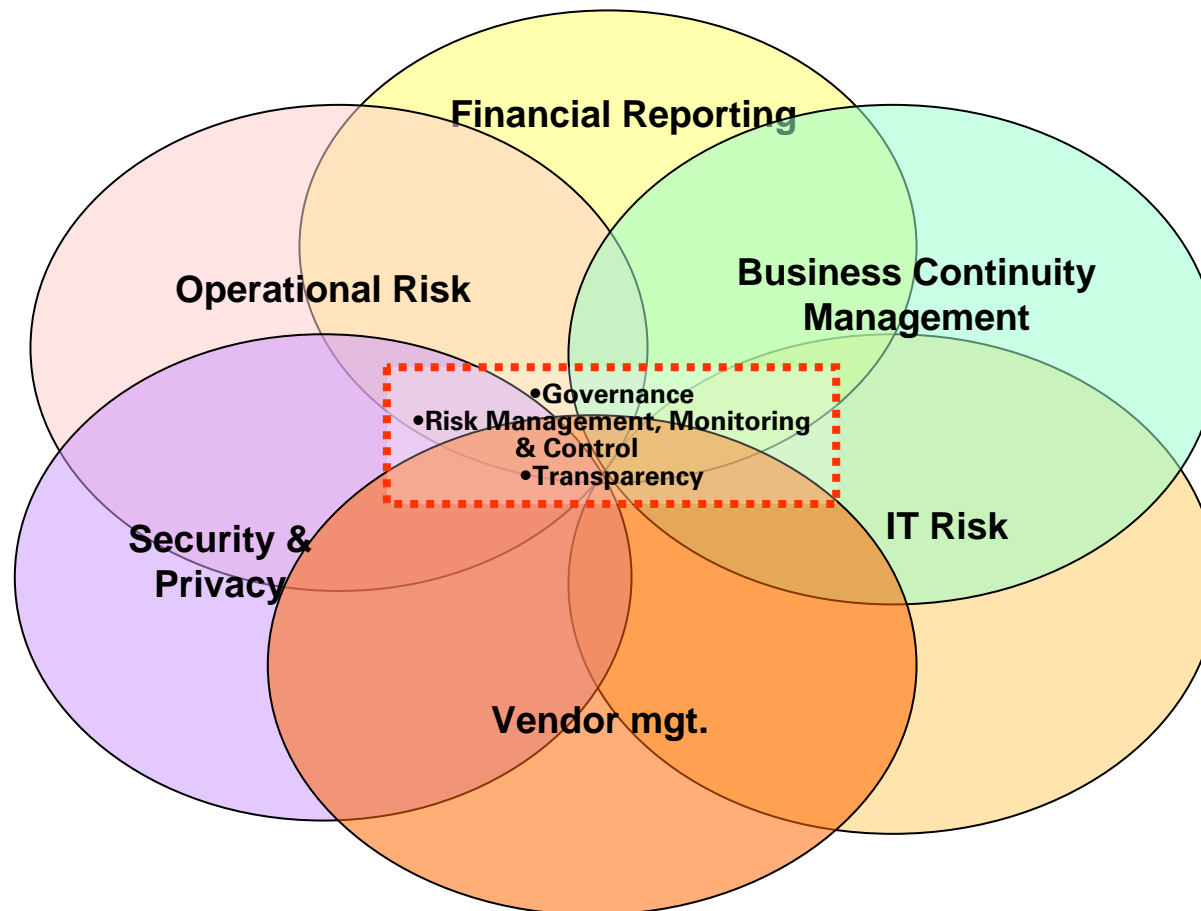
# Structure is needed to minimize and control the risk posed by extreme events.



The Square-Cube Law states that while the surface of an object is measured as a square of its dimensions, its volume varies as a cube of its dimensions.

In the case of buildings, this means you cannot blindly scale up a 10-story building from a one-story building. If suitable supports are not used in the taller building, it will collapse because it generates many times more stress.

# Regulators and credit ratings agencies are establishing principles and making the case for change



# Needed: A future vision and roadmap

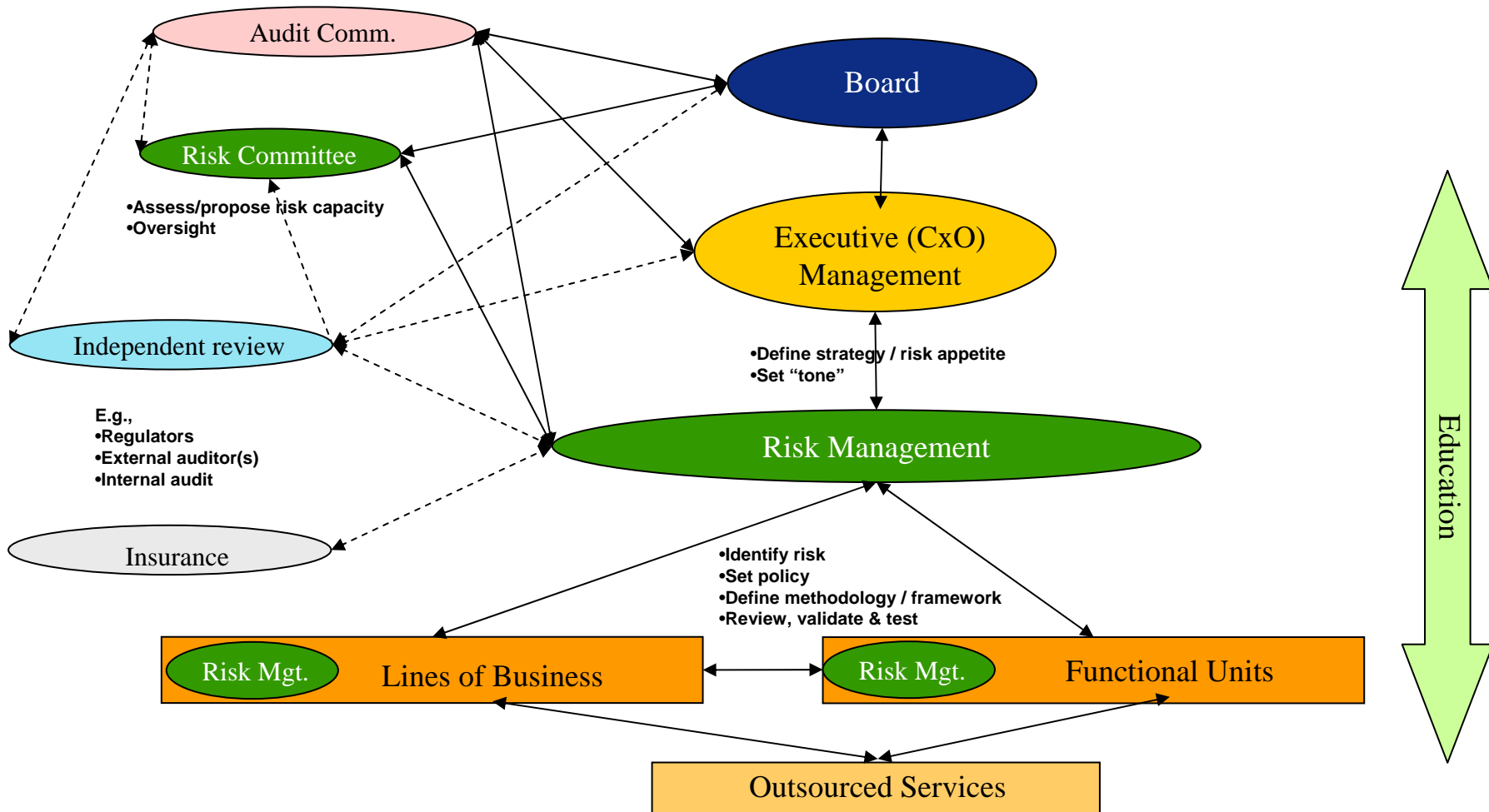
Governance, Risk & Compliance (GRC)	Implicit	Explicit	Synchronized	Optimized
<b>Governance &amp; Objectives</b>	Siloed approach to GRC	Internal alignment; transparency; separated risk-assuming and risk-monitoring functions	Integrate and consolidate regulatory compliance spectrum; incorporate requirements into product development process	Integration with strategic planning
<b>Process &amp; Controls</b>	Independent	Appropriate controls and risk limits; documentation of process and controls	Removal of redundancies & overlaps, adaptive and self-healing systems	Business process transformation
<b>Risk Management</b>	Informal	Integrated; homogenization of risk types and control elements at BU and group level; loss event data capture & analysis; Key Risk Indicator creation, monitoring, & testing; risk limits and tolerance defined	Risk strategy normalized; Capital analysis embedded in mgt.; active portfolio mgt. of all risk types; alignment of risk profile with risk appetite; sufficient risk funding available in light of risks; identification of opportunities: incentives for improved risk management	Value creation; dynamic and predictive risk management and control
<b>Information &amp; Data Management</b>	Ad hoc	Asynchronous	Harmonized, consistent, & timely	Information lifecycle management
<b>People, Org &amp; Culture</b>	Organization Silos	Internal cooperation	Inter-network collaboration & alignment	Adequate and pervasive risk culture
<b>Measures &amp; Metrics</b>	Reactive	Documented	Risk adjusted performance measures: management ensures return on risk exceeds cost of capital	Risk ownership and risk-reward thinking by business owners
<b>Continuous Improvement</b>	Firefighting	Unilateral	Mutual	Embedded

## Benefits

- Governance & compliance
- Reduced reputation risk
- Cost take-out
- Enhance customer satisfaction
- Maximize spend effectiveness & risk adjusted return
- Increase operational effectiveness
- Re-deploy capital towards innovation & growth
- Reduce capital charges
- Increase shareholder value
- Risk culture, common language, education

- Getting down to basics and avoiding stumbling blocks

# Governance is a primary requirement; execution can be challenging

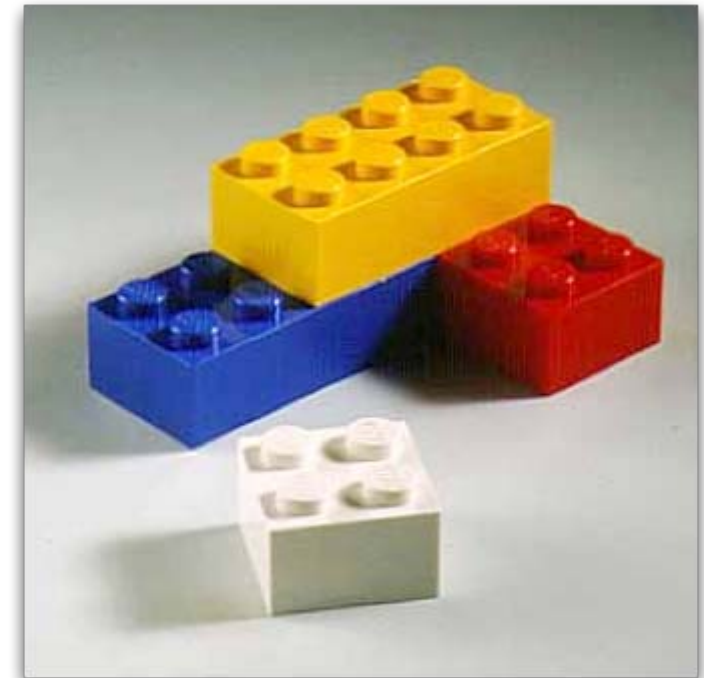


# Framing the exercise raises difficult questions

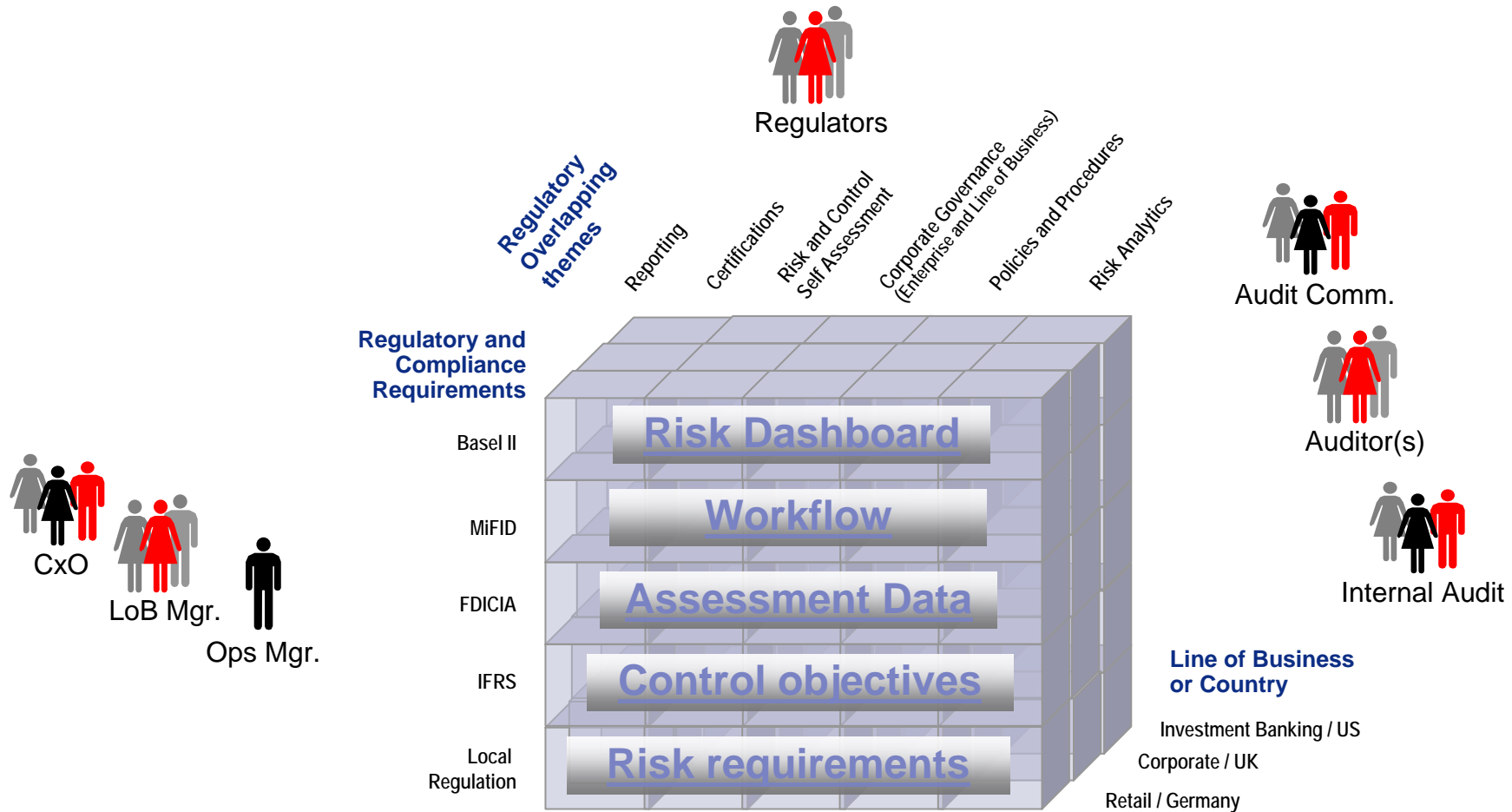
- What is, and who owns, the problem?
- What do regulators, ratings agencies, and the markets expect?
- How will change be funded?
- What is the impact on business owners?
- To buy or to build?
- How can the risk management be leveraged for competitive advantage?
- Are there external sources that can help better to understand risk?
- How do capital costs vary with individual products and services?
- Is risk priced appropriately?
- ...??

# Tactical building blocks are sometimes needed

- Risk education, culture, and language
- “Single view of organization”
  - ✓ Legal entity data
- Business risk identification
  - ✓ “Single view of process”
  - ✓ Homogenization of risk types and control elements at BU and group level
  - ✓ Internal data creation, acquisition, and management
  - ✓ Reference data
  - ✓ External (industry) event data
- Workflow orchestration



# A goal state: harmonized, consistent, and timely information

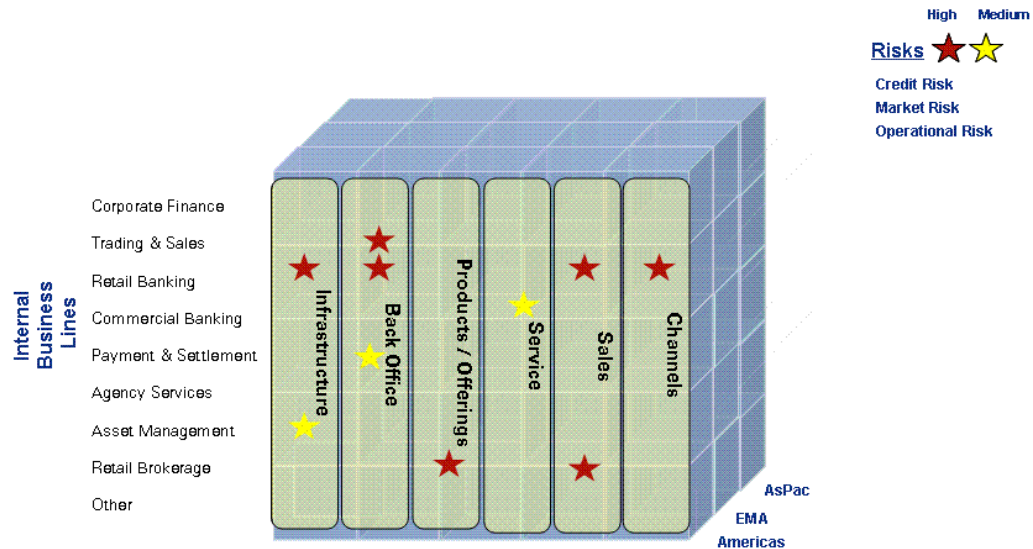


- Gaining focus and traction

# Risk identification and evaluation

Identify and prioritize hot spots across the enterprise.

- Create visibility
- Size exposures
- Focus attention on high risk areas
- Control spending



# Risk modeling and quantification is a cornerstone of enterprise-wide risk management

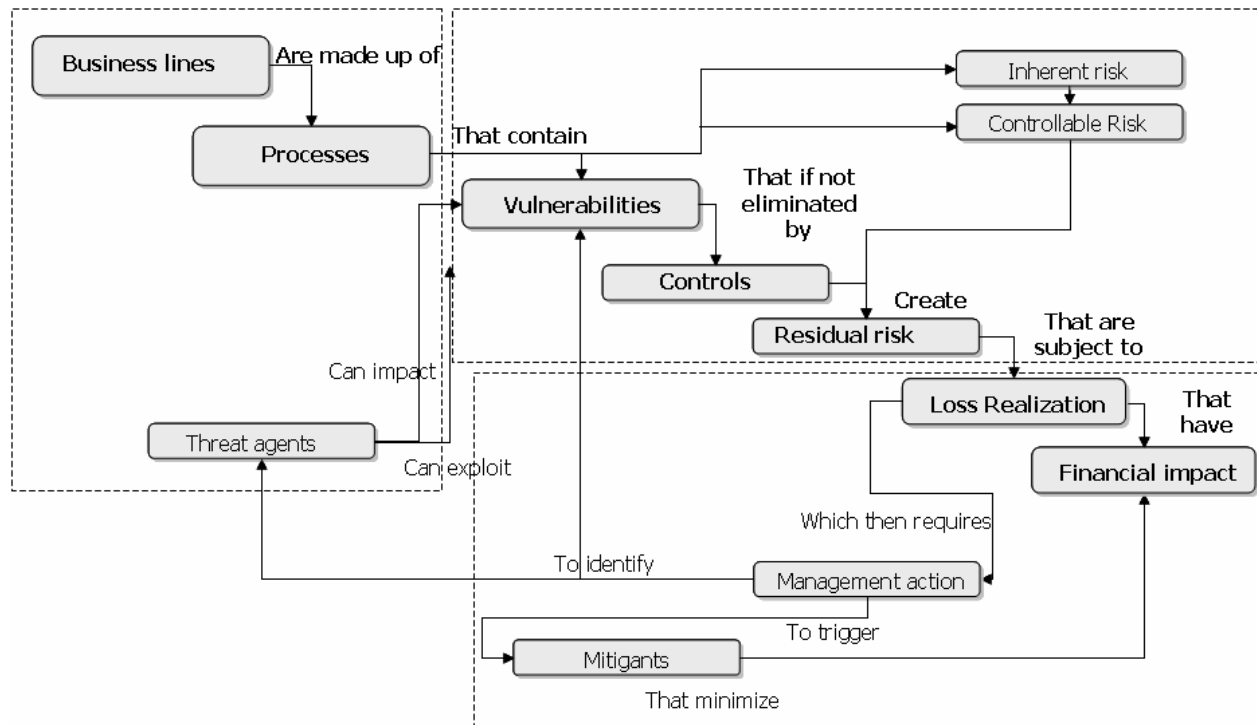
Risk modeling enables managers to understand risk exposure over 3 dimensions:

- ✓ *Analytic*: What is the overall quantified risk exposure?
- ✓ *Diagnostic*:
  - How effective are technologies, controls, and mitigants?
  - What is the ROI for change?
- ✓ *Predictive*: What are the key causes and indicators of risk?

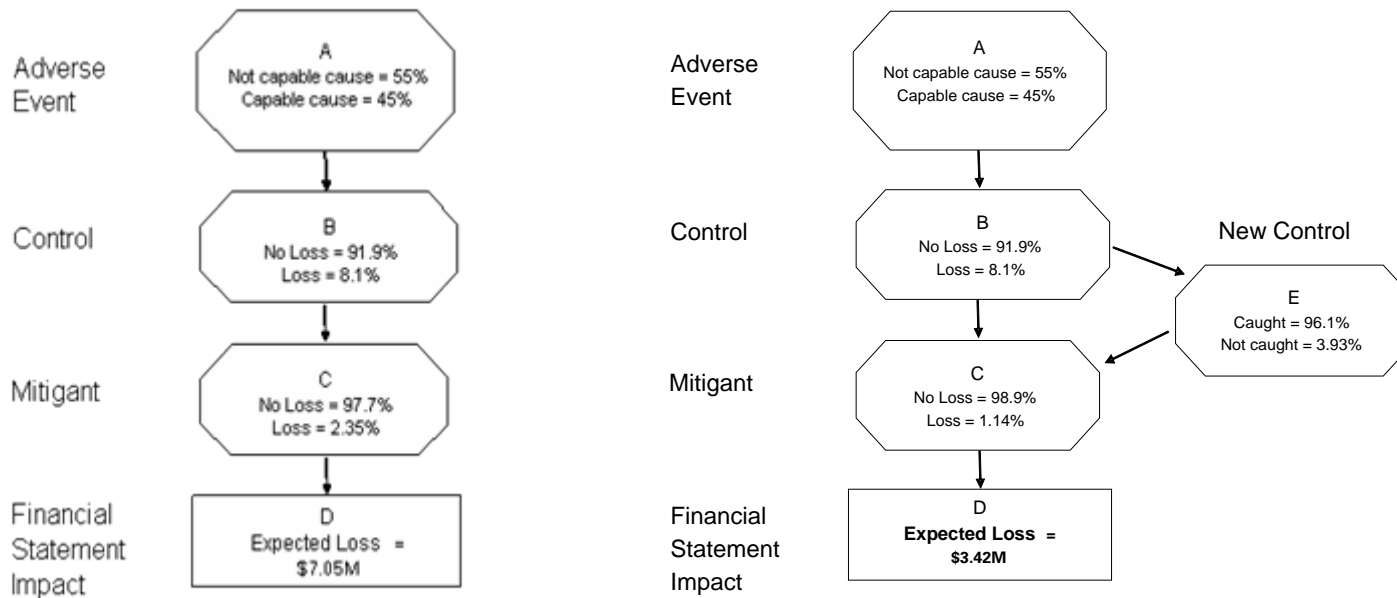
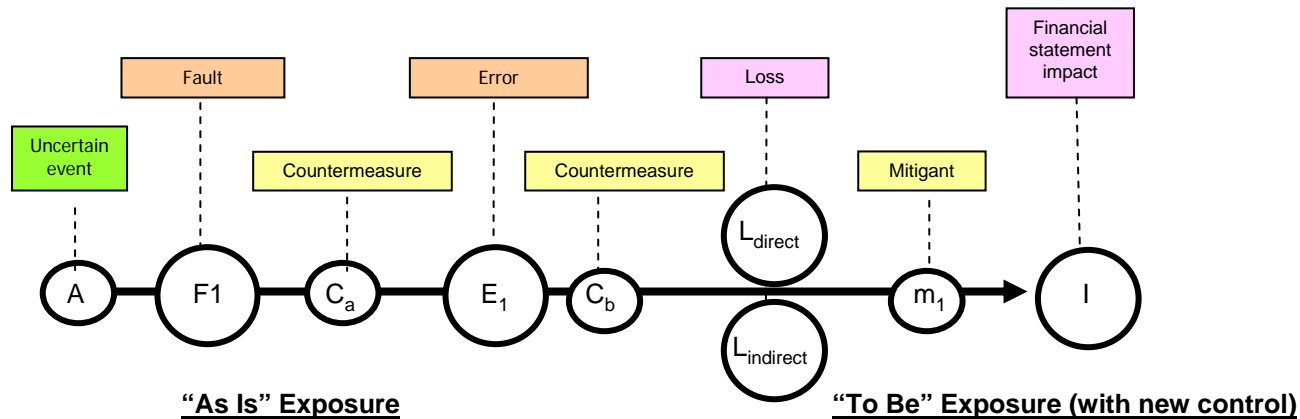
# Effective management of Operational Risk requires understanding the relationship between risk reduction options and business impact.

Operational Risk can be quantified by:

- Identifying business processes of interest
- Identifying applicable event drivers, and
- Estimating the effectiveness of controls, countermeasures, and mitigants (e.g., insurance), as well as their combined economic impact on business process.



# A transparent, risk-driven ROI calculation can assist managers to understand risk and where best to make changes



- Dynamic and predictive Enterprise-wide Risk Management

"Cutting through complexity to find a solution runs through four predictable stages:

**[--D]etermine a goal,**

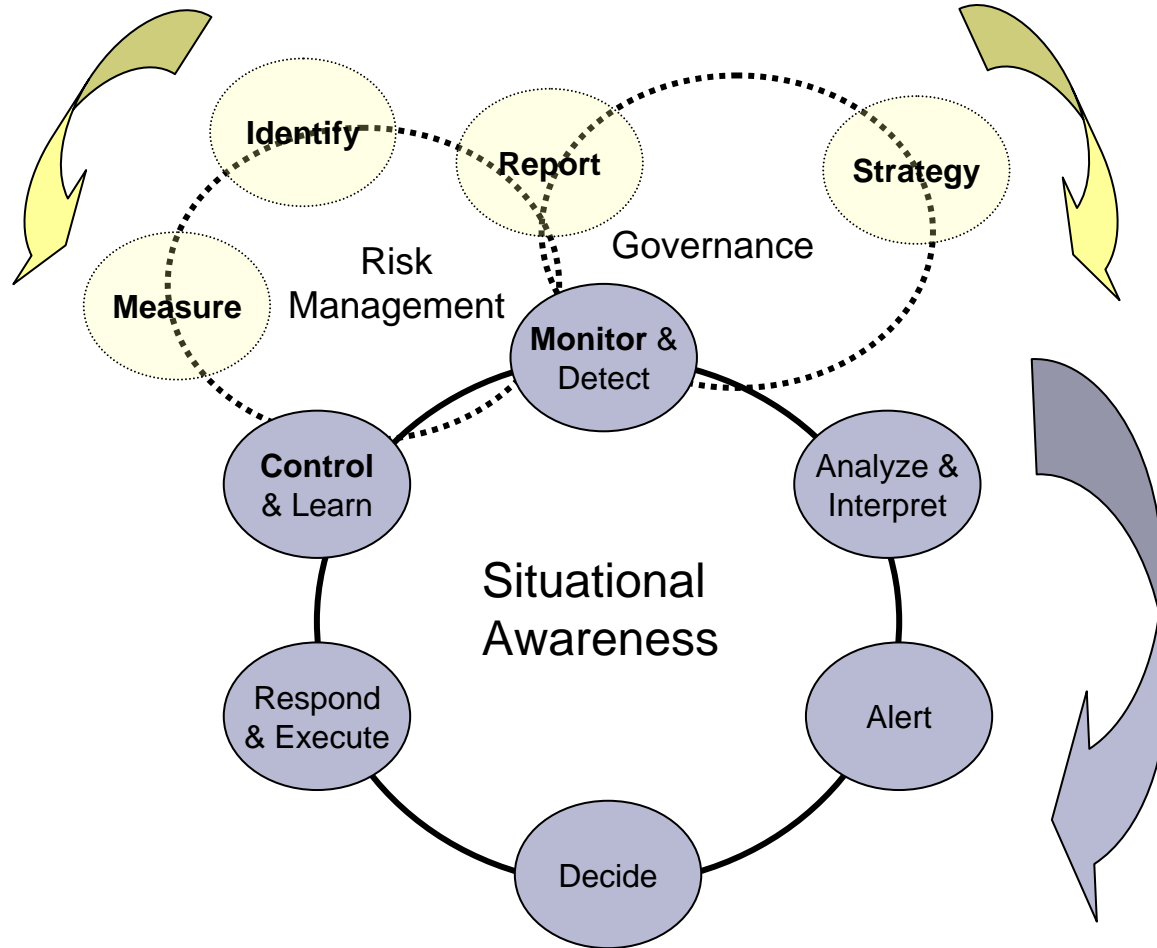
**[--F]ind the highest-leverage approach,**

**[--D]iscover the ideal technology for that approach, and in the meantime,**

**[--M]ake the smartest application of the technology that you already have...."**

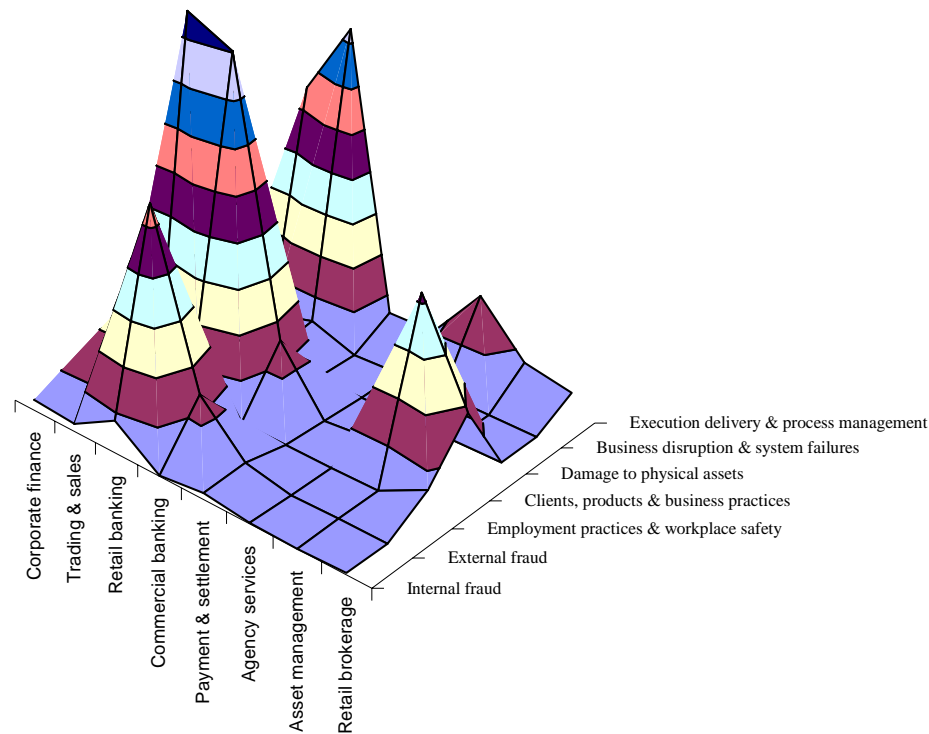
Bill Gates

# Risk management is a process

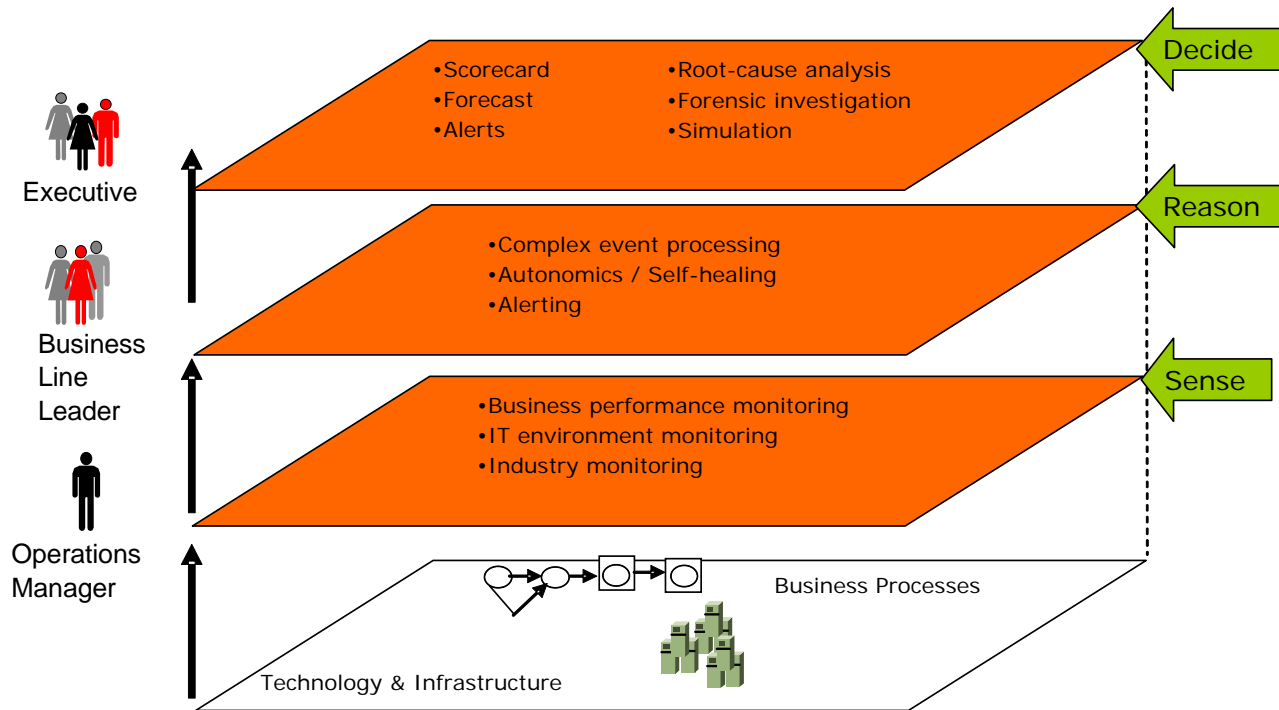


# C-level executives need to be able to monitor enterprise-wide risk, watch it vary over time, and investigate problem areas.

By quantifying and harmonizing the range of enterprise risk types, integrated risk information can be presented in graphical form, such as a risk surface.

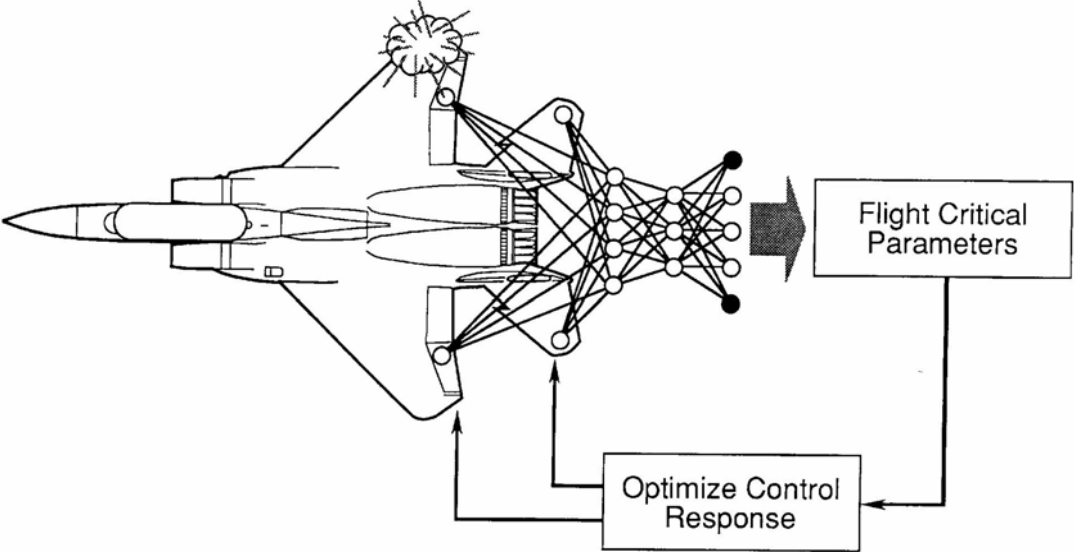


# Other stakeholders have needs and requirements



# Self-managing and healing features should be part of the architecture, to provide resiliency and enhance flexibility

## A self-managing and healing system



- The benefits of effective risk management



# With risk as a key parameter, executives can model and optimize enterprise value add for a range of key business decisions

