

# ***Enterprise Risk Management & Governance***



**Dr. Robert Charette**  
**President**  
**ITABHI Corporation**

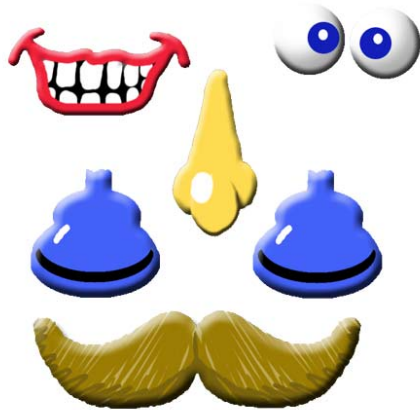
# Corporate Landscape

1. *Do more with less*
2. *Be more innovative & entrepreneurial*
3. *DON'T do anything that might get the CEO or CFO (or CIO) thrown in jail*



# ***Enterprise Risk Management***

***Totality of an organization's risk spectrum (i.e., risk "gestalt") is assessed and managed as a whole***





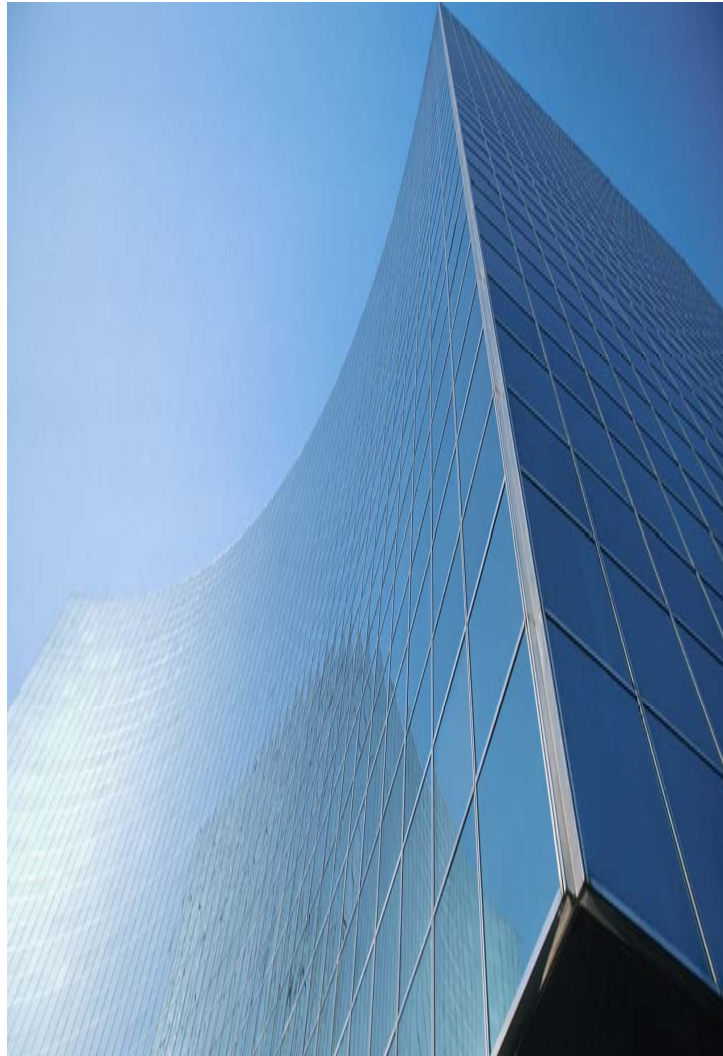
# ***ERM Approach***

- **Manage risk as a system**
  - “System” includes organization & operating environment
  - Borderless, seamless and continuous flow of information
  - Focus on radically improving:
    - Situational awareness (white, grey & black space risks)
    - Quality/timeliness of decision making
    - Quality of risks taken
  - Improve risk management efficiencies across organization
    - Don't over or under manage risks
- **Use common approach to:**
  - Assess total amount of business risk exposure
  - Determine responsibility for risk aversion & exploitation
  - Understand individual, collective and cumulative effects of different types of risk on business decisions
- **Three integrated aims**
  - Loss & Cost Control
  - Innovation & Entrepreneurship
  - Stewardship & Responsibility



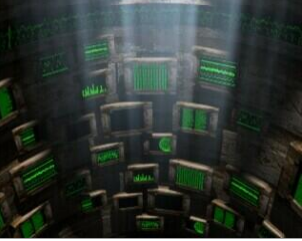


# ***ERM Focus***



- **Strategic Risks**
- **Operational Risks**
- **Financial Risks**
- **Insurable Risks**
- **Governance Problems**





# ***ERM Components***



- **Management of risk**
  - “Top-down” – strategic, financial, insurable risk-oriented
  - Sets risk appetite, tolerance, behaviors
  - Attacks systemic risks through innovation
- **Risk management**
  - “Bottom-up” – operational, financial risk-oriented
  - Creates information for decision making
  - Execution focused
  - Aims to avoid predictable surprises
- **Centralizing decision mechanism**
  - Chief Risk Officer
  - Decision point process





# ***Enterprise Governance***

*“Corporate governance is the system by which business corporations are directed and controlled.”*

Cadbury Report 1992





# ***Governance Requirements***

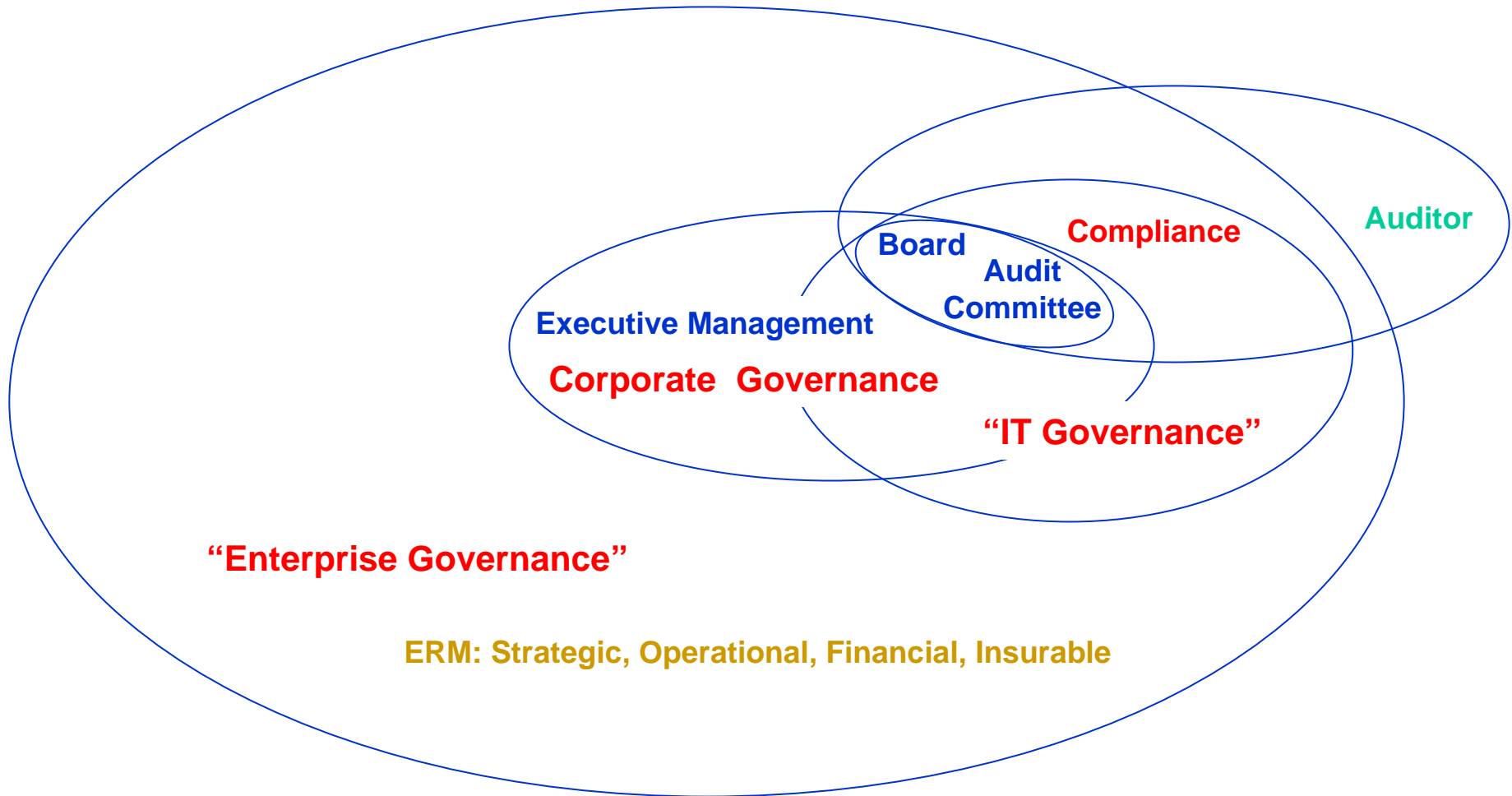
- **Due Care**
- **Validity**
- **Transparency**
- **Completeness**
- **Disclosure**
- **Timeliness**
- **Restrictiveness**
- **Verification**

**AU/NZ 4690**  
**UK Company Code**  
**Basel II**  
**Sarbanes-Oxley**  
**COSO Internal Controls**  
**OECD Principles**





# Governance Troika



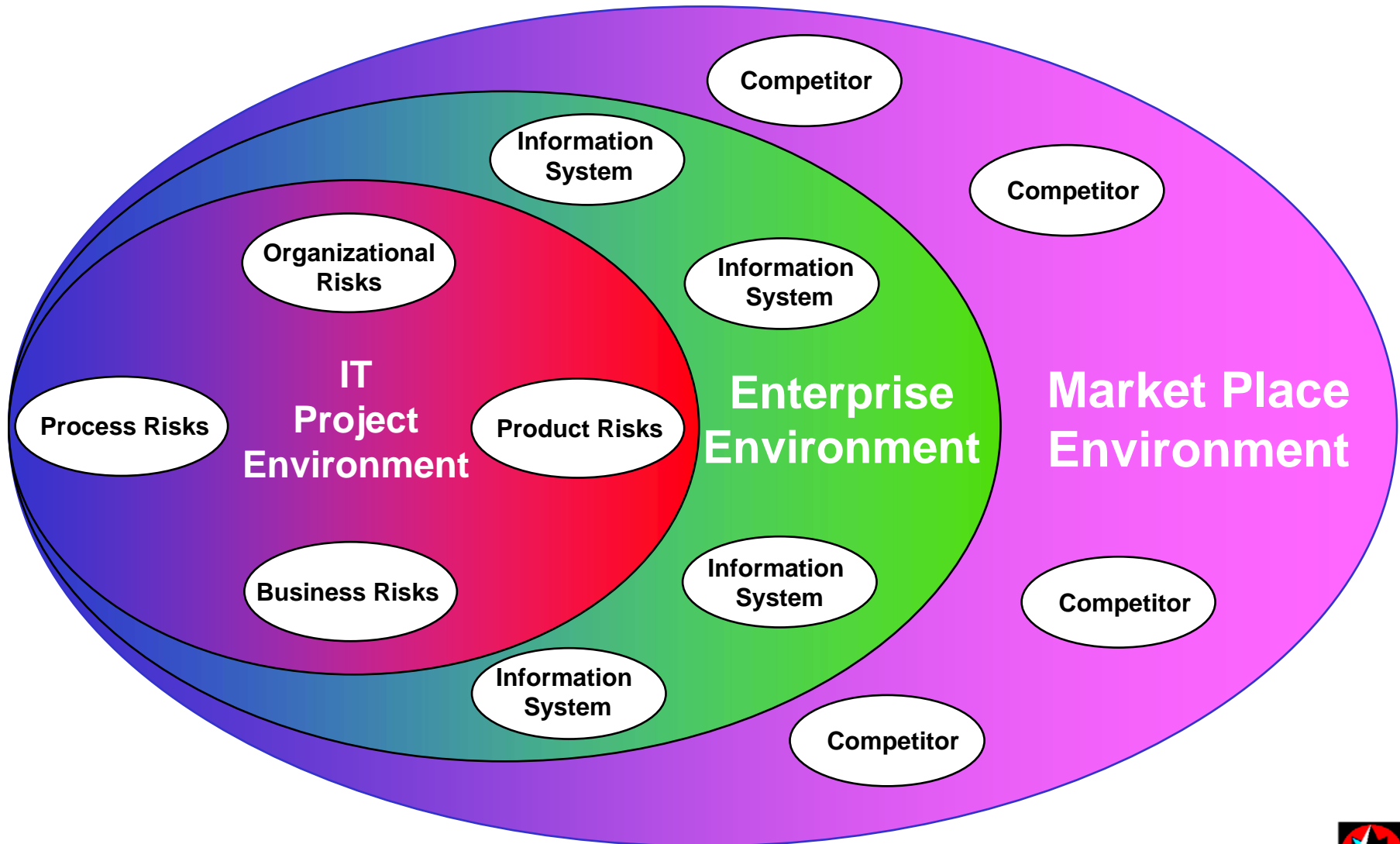
# ***Rules vs. Principles***



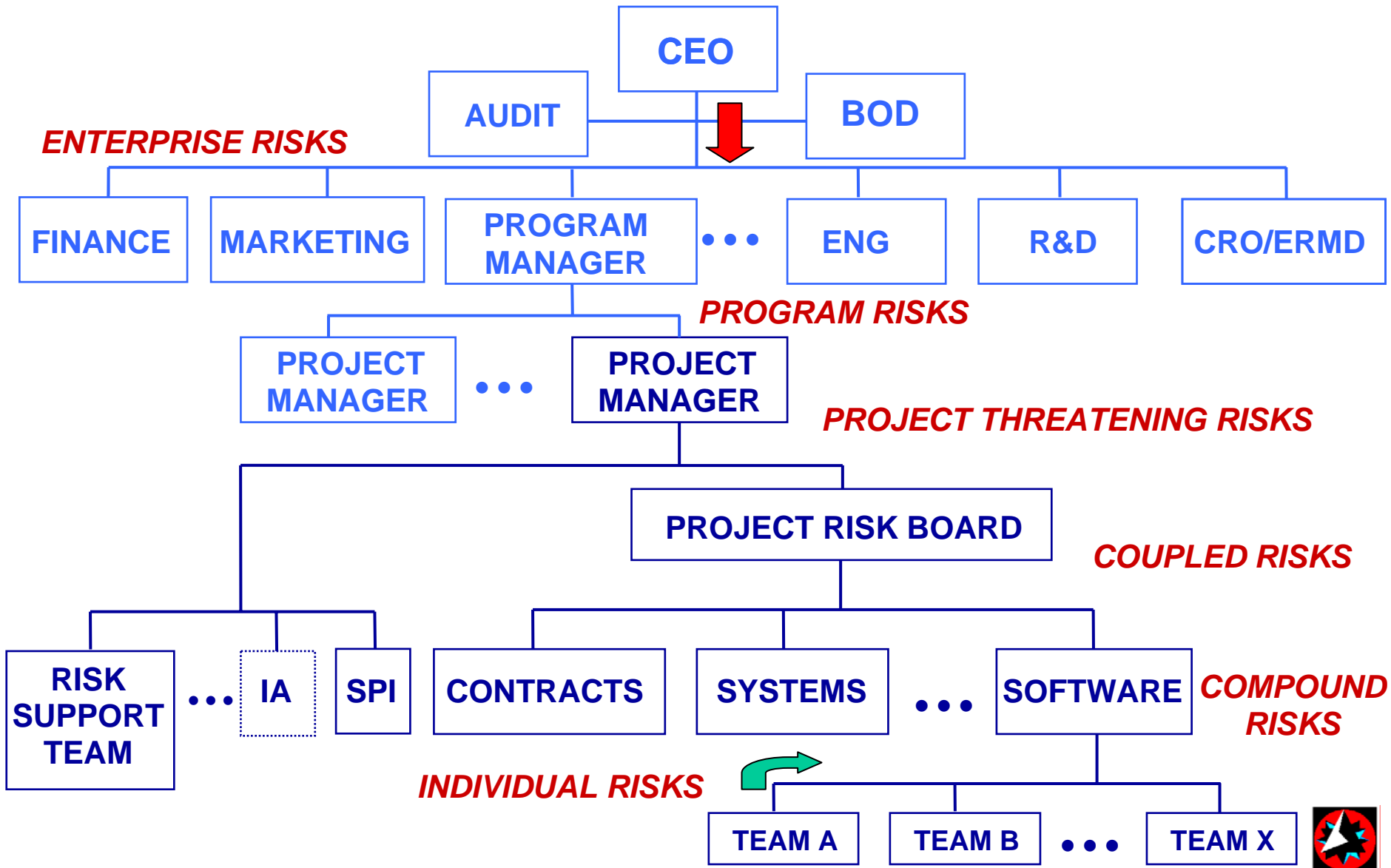
- **US Approach**
  - Comply or jail
  - Procedure-focused, consequence-centric
  - Controls an add-on
  - Same basic controls for everyone
  - Trust you only so far
  - 100,000 + pages
- **UK Approach**
  - Comply or explain
  - Objective-focused, risk-centric
  - Internal “controls” culturally embedded
  - Controls tailorable to situation
  - Trust you to do the right thing
  - 14 pages



# ***ERM&G Interactions***



# Managing ERM&G





# ***Measurement Impacts***



- **ERM & G information must encompass broad range of specific and general measures**
  - Each risk area (strategic, operational, financial, insurable, governance) has own needs
  - Information has to be interconnected and usable
  - Context information critical
- **IT linked directly into business (individually/collectively)**
  - IT/Strategy alignment
  - IT/Financial alignment
  - IT/Operational alignment
  - IT/Insurance alignment
  - IT/Compliance alignment
- **Governance impacts IT processes and management**
  - Proof of effective internal controls
  - Timeliness/accuracy of control information critical
  - Costs of internal controls
- **Tensions Between ERM & Governance**
  - Innovation vs. compliance
  - “Cultural measures” needed?



# Summary



- **ERM & G's growing practice**
- **Direct impacts on**
  - What needs to be measured
  - How it is to be measured
  - How measures are interconnected and interpreted
  - Timeliness of measures
  - Costs of measurement
- **Dynamic environment**
  - Governance requirements
  - Emerging enterprise risks
  - Perceptions of risk

