

# Building Better Boards: *The IT Governance Value Chain*

Professor Michael Parent

*Electronic Commerce Seminar Series*  
ANU School of Accounting & Business Information Systems  
National Centre for Information Systems Research  
October 27, 2006

1

UQ BUSINESS SCHOOL



## Problem? What problem?

- IT = 1/3<sup>rd</sup> of all capital spending
- 20% of all IT efforts 'wasted' (Gartner)
- Most Boards pay scant attention until catastrophes occur

*Computerworld's Top Ten IT Project Failures during the 1990s EXCEEDED US\$1B!*

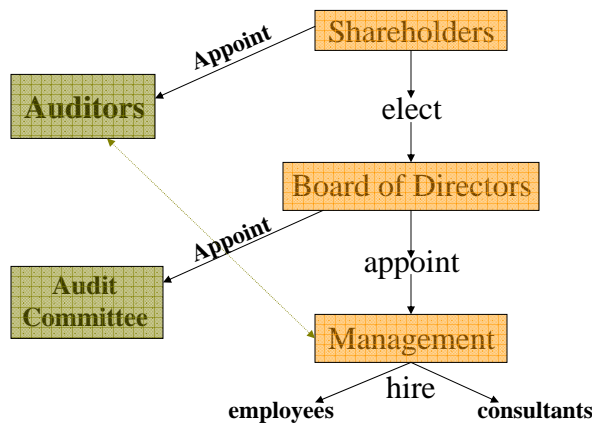
2

UQ BUSINESS SCHOOL



Governance is “...*decision-making in the exercise of authority for direction and control.*” (Shailer)

## Governance Framework for Accountability





## IT Governance

- A sub-set of overall corporate governance
- Increasingly regulated (SOX, AS8015)
- Oversight of decisions about *key* IT activities in the firm. Subsumes knowledge of:
  - The firm's strategy & strategic competencies;
  - The role and relative importance of IT in enacting this strategy;
  - Current / future technology trends

5



## IT Governance Defined

*The strategic alignment of IT with the business, such that maximum business value is achieved through the development and maintenance of effective IT controls and accountability, performance management, and risk management*

Webb & Pollard, 2006

6



## 3 Guiding Principles

1. The Board owns IT Governance
2. Trust but Verify
3. Risk = *probability X outrage*

7



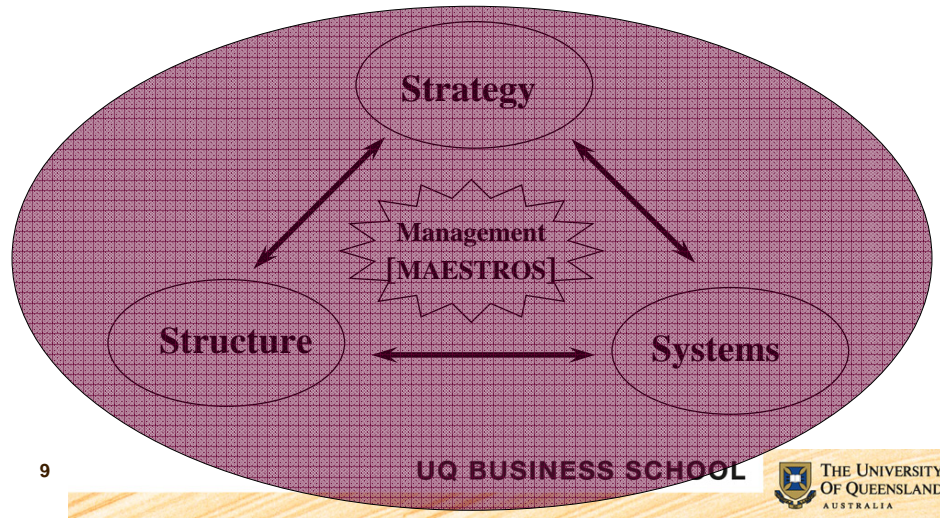
## The Board Owns ITG

- ITG is too important to delegate to managers in the organization
  - Audit Committee / Key expert (external director)
- Crises prompt knee-jerk reactions
- Better to have a program specified

8



## Trust but Verify



9

UQ BUSINESS SCHOOL



## IT Risk

$$\underline{\underline{RISK = PROBABILITY \times OUTRAGE}}$$

- When systems go bad, they go bad in a big, big way.
- *Outrage* is in part a function of the scope of the failure, but also its *visibility*.
- The internet has made everything visible

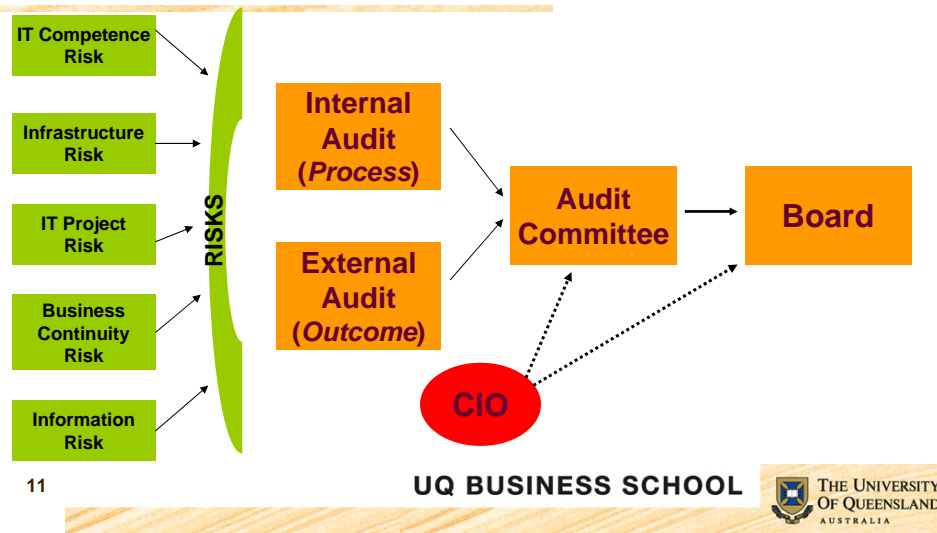
10

UQ BUSINESS SCHOOL





## The IT Governance Value Chain



## The IT Governance Value Chain

- Extension of Porter & Millar's (1985) work
- Posits that Directors *can & should* add value to the firm's activities through appropriately thorough oversight
- Presumes *active, ongoing* involvement by mainly by external directors (Audit Committee)



## A Director's Dashboard

13



## IT Competence Risk

IT Competence Risk

*Have I taken an executive course/seminar on IT in the past 2 years?*

*Do I regularly read at least one monthly column or article about technology?*

**RED** – no training, no reading.

**AMBER** – either a course or reading, but not both.

**GREEN** – ongoing commitment to learning about tech.

14

## 3 Sources

- Robert X. Cringely:  
<http://www.pbs.org/cringely>
- Walter Mossberg:  
<http://ptech.wsj.com>
- CEO Express portal  
<http://www.ceoexpress.com>

## IT Infrastructure Risk

**IT  
Infrastructure  
Risk**

*To what extent has  
management shown IT  
strategic 'fit'?*

*Does a coherent IT  
architecture plan exist?*

**RED** – no strategic fit demonstrated.

**AMBER** – plans & fit exist, but are ambiguous, not clearly executed

**GREEN** – clear plans, clear fit, CIO speaks native language, not 'Geek'.

## IT Project Risk

**IT Project Risk**

*How many IT projects have been successfully completed in the past 1-3 years? (IT project competence)*

*Do certified Project Managers (PMs) oversee IT projects (PMBOK)?*

**RED** – low (<50%) success rate or no new projects, few or no trained PMs.

**AMBER** – moderate (50-66%) success rate, moderate display of PM skills.

**GREEN** – High success rate, high degree of change management / PM skills.

## Business Continuity Risk

**Business Continuity Risk**

*Does a current (<1 yr) enterprise risk management (ERM) framework exist?*

*Has this framework ever been tested, an IT disaster initiated & solved?*

**RED** – no ERM (e.g., CoBIT, COSO, ITIL, ISO).

**AMBER** – an ERM exists, but has not been tested in the past year.

**GREEN** – ERM is in place, staff is trained, test has been conducted, and all deficiencies corrected.

## Information Risk

Information Risk

Does the organization have explicit privacy & security policies?

Does the organization have a Privacy Officer – a senior manager responsible for, and with sufficient authority to enforce these policies?

**RED** – no policy, no officer, no visible enforcement.

**AMBER** – policies exist but are not enforced (tacit understanding).

**GREEN** – clear policies, senior oversight.

## Final Thoughts I

- We have long-passed the days where, in the words of **Irving Olds**, Chair of U.S. Steel’s Board in the 1950s,

*“Directors are somewhat like parsley on a fish – decorative, but useless.”*



## Final Thoughts II

- Today, **Mitch Ratliffe's** 1992 impressions may still hold true:

*“A computer lets you make more mistakes faster than any invention in human history – with the possible exception of handguns and tequila.”*



## Final Thoughts III

- Directorship has become increasingly complex and legislatively proactive – what matters gets measured (and vice-versa).
- Directors are no longer expected to be benign acquiescers – they must:
  - Be aware
  - Show comprehension & foresight
  - Constantly monitor
  - Refuse to entrench
  - Eschew ‘common sense’ when it makes no sense
  - Be open to scrutiny from outsiders
  - Consider IT governance part of their portfolio



---

Thank You.

m.parent@business.uq.edu.au

mparent@sfu.ca