



International ICT Expo 2007

IT Security & Governance

Leroy Yau, Director of ISACA HK Chapter
16 April 2007

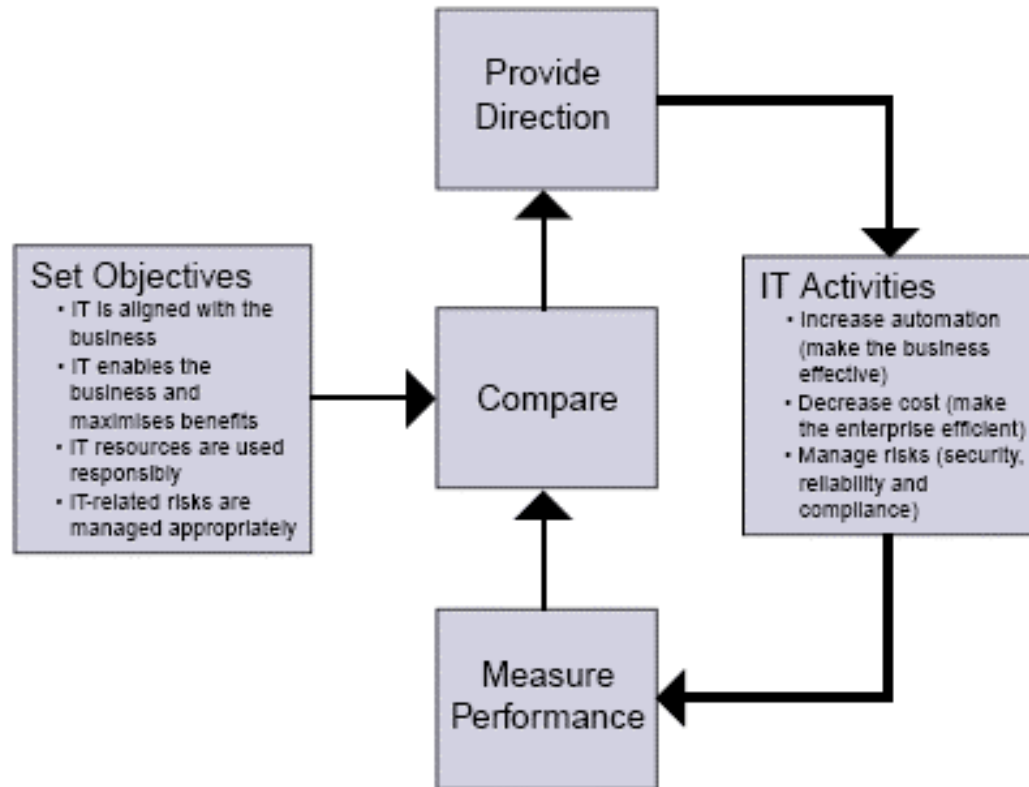
- IT Governance Overview
- Convergence with IT Governance

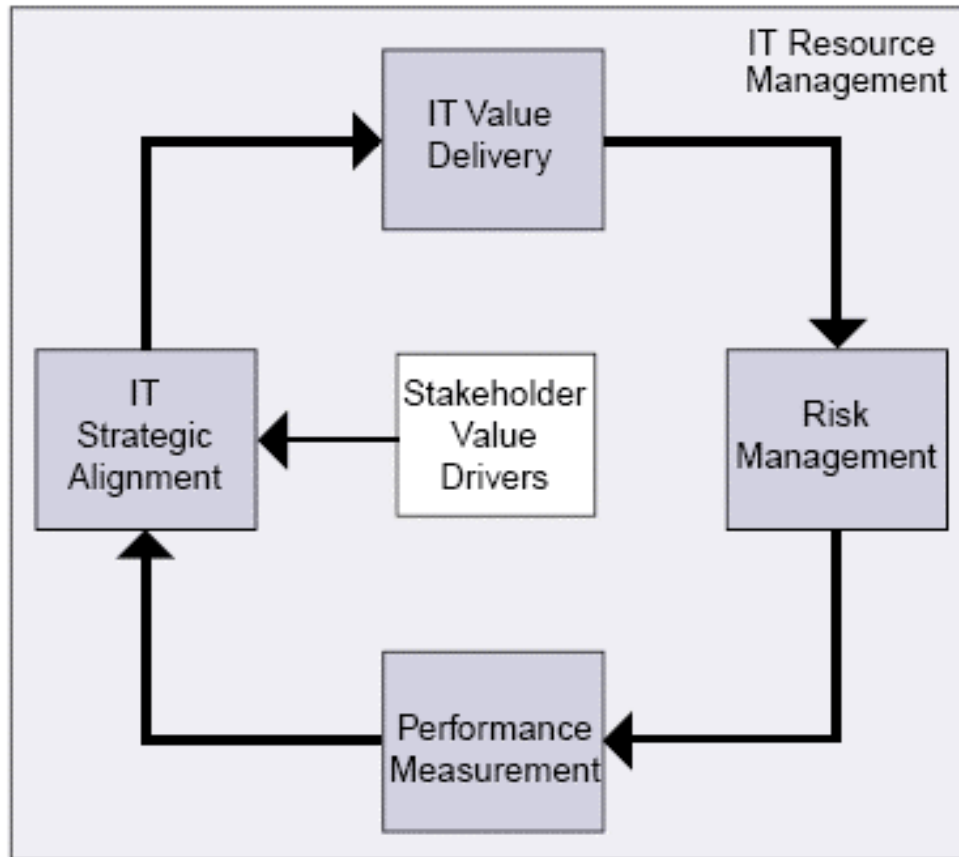
- Aligning IT strategy with the business strategy
- Cascading IT strategy and goals down into the enterprise
- Providing organizational structures that facilitate the implementation of strategy and goals
- Creating constructive relationships and effective communications between the business and IT, and with external partners
- Insisting that an IT control framework be adopted and implemented
- Measuring IT's performance

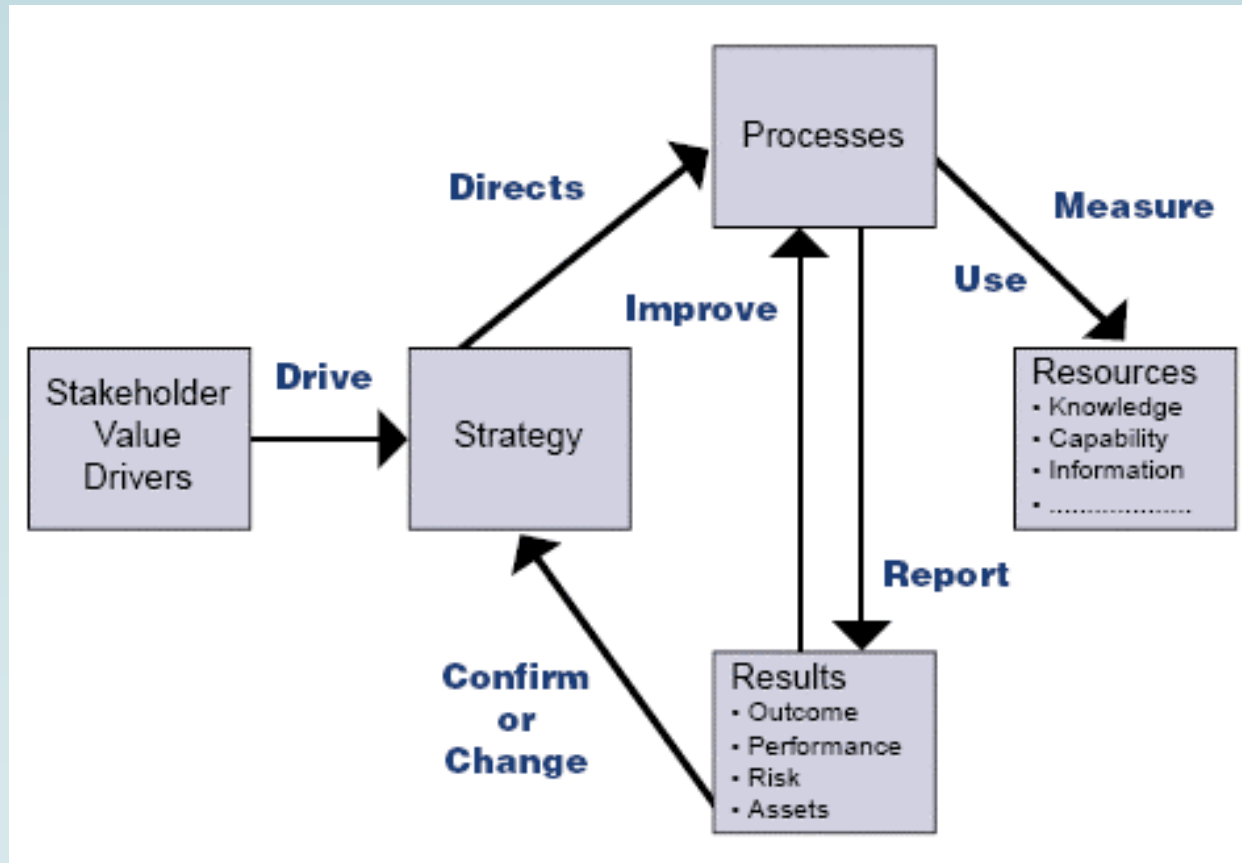
- Take advantage of IT's enabling capacity for new business models and changing business practices
- Balance IT's increasing costs and information's increasing value to obtain an appropriate return from IT investments
- Manage the risks of doing business in an interconnected digital world and the dependence on entities beyond the direct control of the enterprise
- Manage IT's impact on business continuity due to increasing reliance on information and IT in all aspects of the enterprise
- Maintain IT's ability to build and maintain knowledge essential to sustain and grow the business
- Avoid the failures of IT, increasingly impacting the enterprise's value and reputation

What is IT Governance?

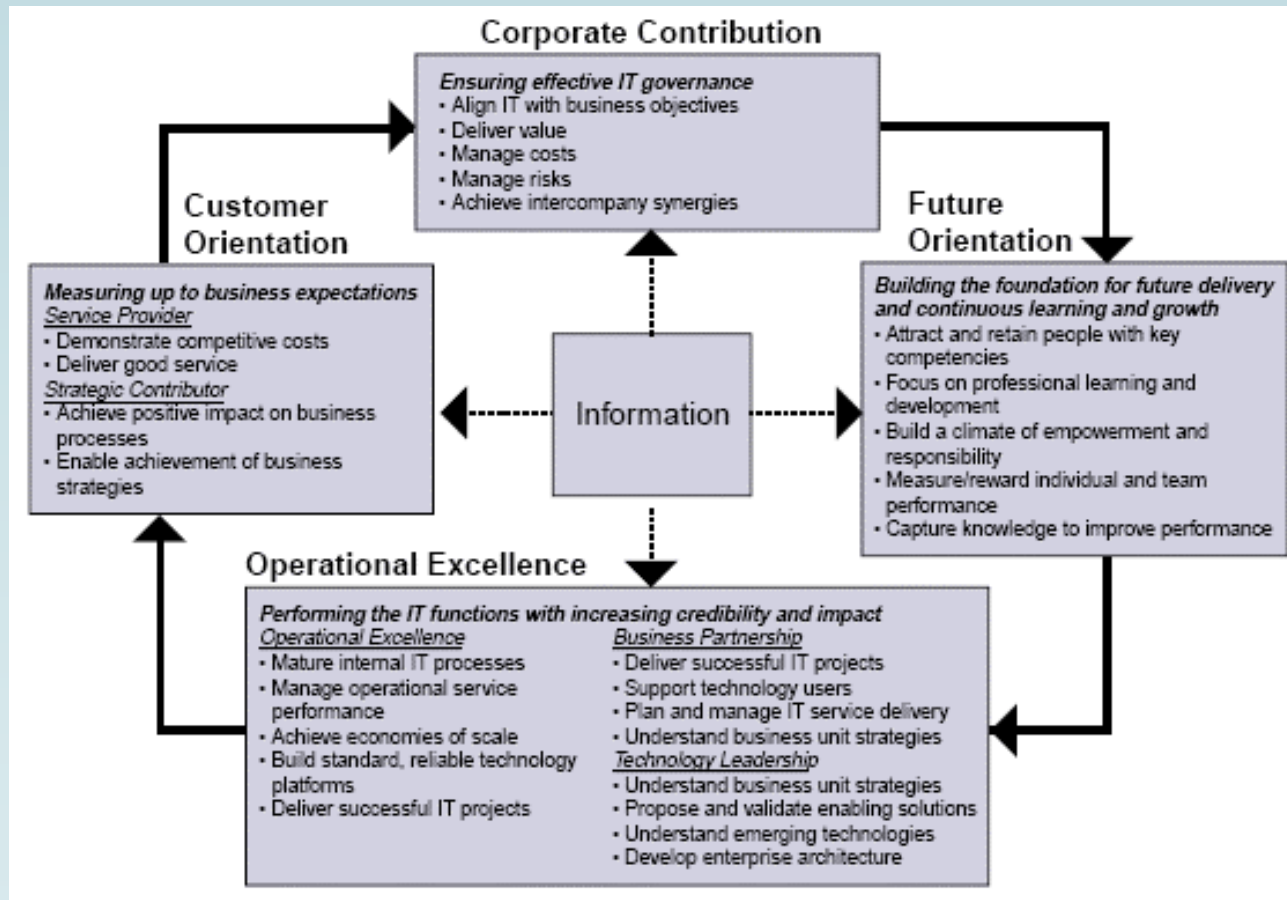
- IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives







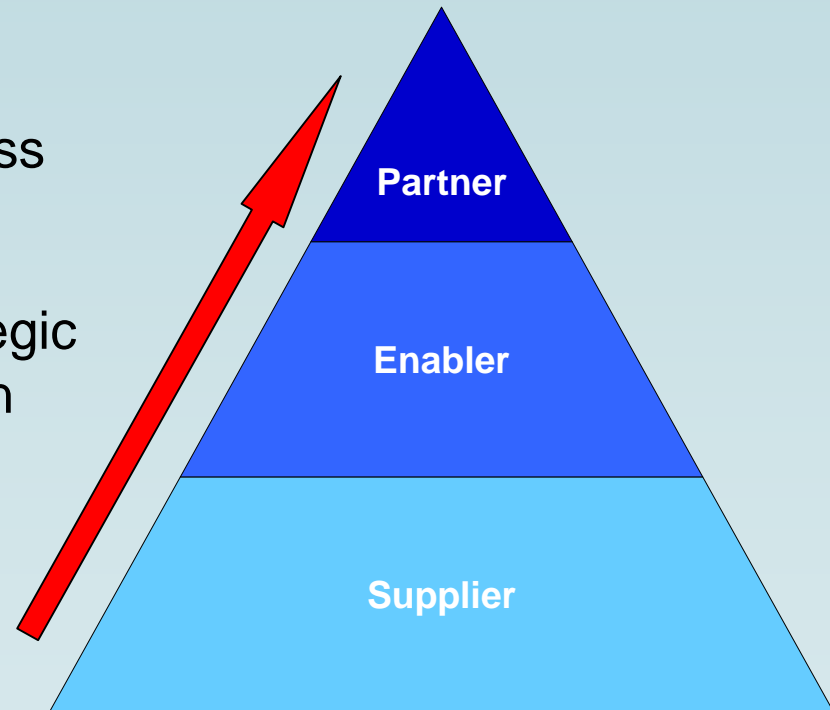
Sample IT BSC Measures



Drives or “is” the business

Contributes in part to strategic
areas of the organization

Supporting
the organization



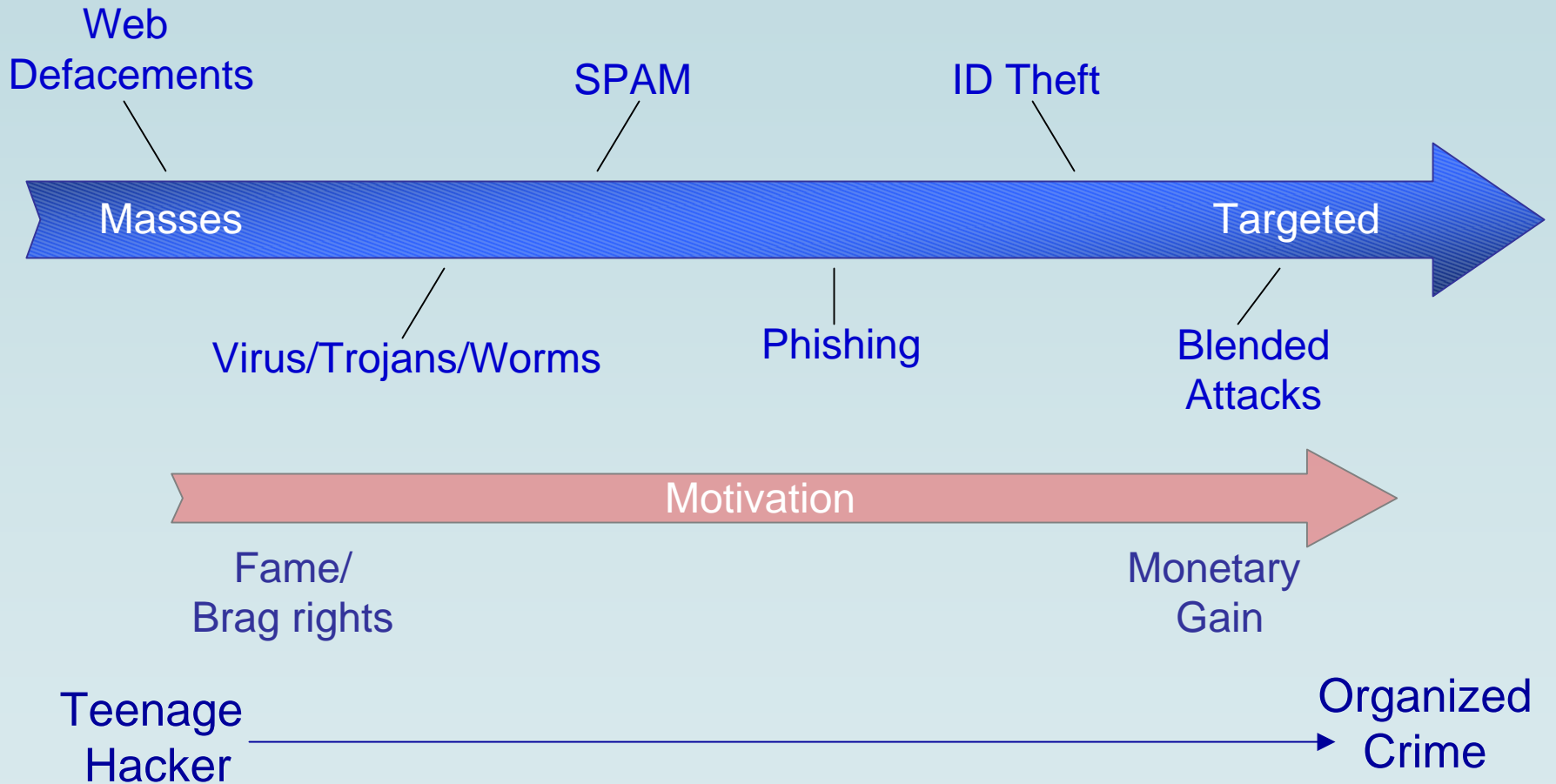


Governance Landscape

- Changes to landscape:
 - Increased regulatory, legislative and legal pressures
 - Privacy
 - Safeguarding Organization Records
 - Intellectual Property Rights
 - Increased market awareness & expectations to security, privacy and governance
 - Increased use/deployment of technology in business



IT Security Landscape



- **Regulations/Legislation:**
 - Drive need for strong governance processes
- **Management Expectation:**
 - IT to be positioned to comply with regulations in an efficient and cost effective manner
- **Additional audits:**
 - expected to validate compliance with regulations, in addition to SOX (e.g., PCI, Privacy Laws etc)
- **Controls frameworks:**
 - become as common as System Development frameworks 15-20 years ago. Organizations should consider developing these frameworks from existing models
- **IT Compliance/IT Risk Officers:**
 - become common place in large, heavily regulated industries
- **IT Changes:**
 - must simplify, standardize and then sustain their processes to manage risks and ensure compliance

Traditional IT Responsibilities(?)

- Risk Assessments
 - IT risk impacts business
- Business Continuity Plans
 - BCP \neq DRP
- Data Classifications
 - IT only custodians/guardians
 - Businesses are the owners

- IT to sustains and extends the enterprise's strategies and objectives
- IT governance is not an isolated discipline



Thank you

