

Information Security, Business Continuity & IT Governance

Dr. Nasser Saidi
Chief Economist DIFC
January 8, 2007

AGENDA

- **ISSUES**
- **CODES & STANDARDS**
- **SURVEY RESULTS**
- **RECOMMENDATIONS**

source will appear at the bottom



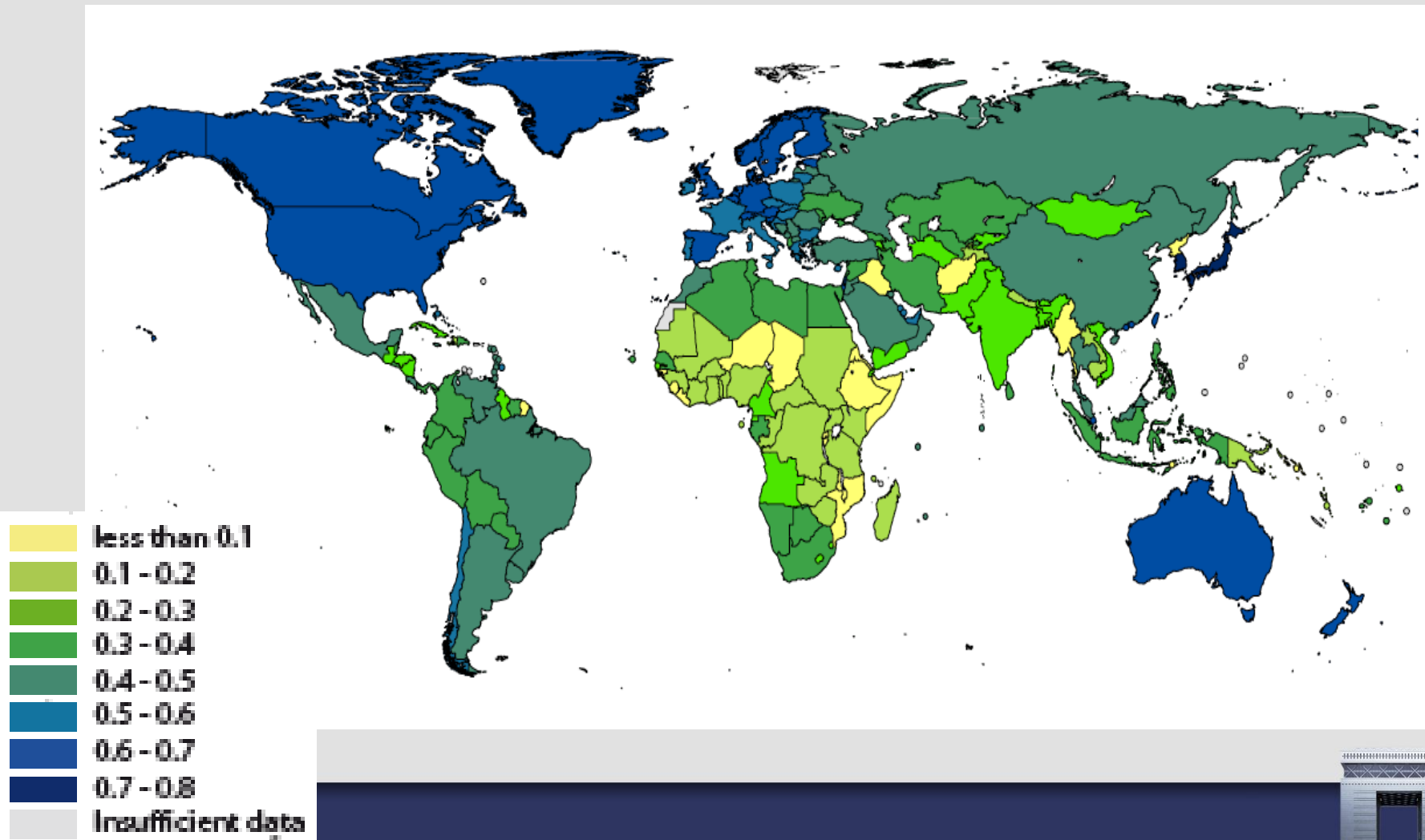
INFO SECURITY & BUSINESS CONTINUITY: SOME ISSUES

Digital technologies are transforming our economies and societies:

- Expansion in coverage
- Decline in ICT prices
- Growth in infrastructure
- New & advanced technologies, including broadband and mobile Internet
- New products and services: e-Services, e-Government, e-Banking
- Laws & Regulations
- Globalization: no islands!
- Logistics, Outsourcing and the Global Supply Chain
- Digital property protection
- E-Security & Trust

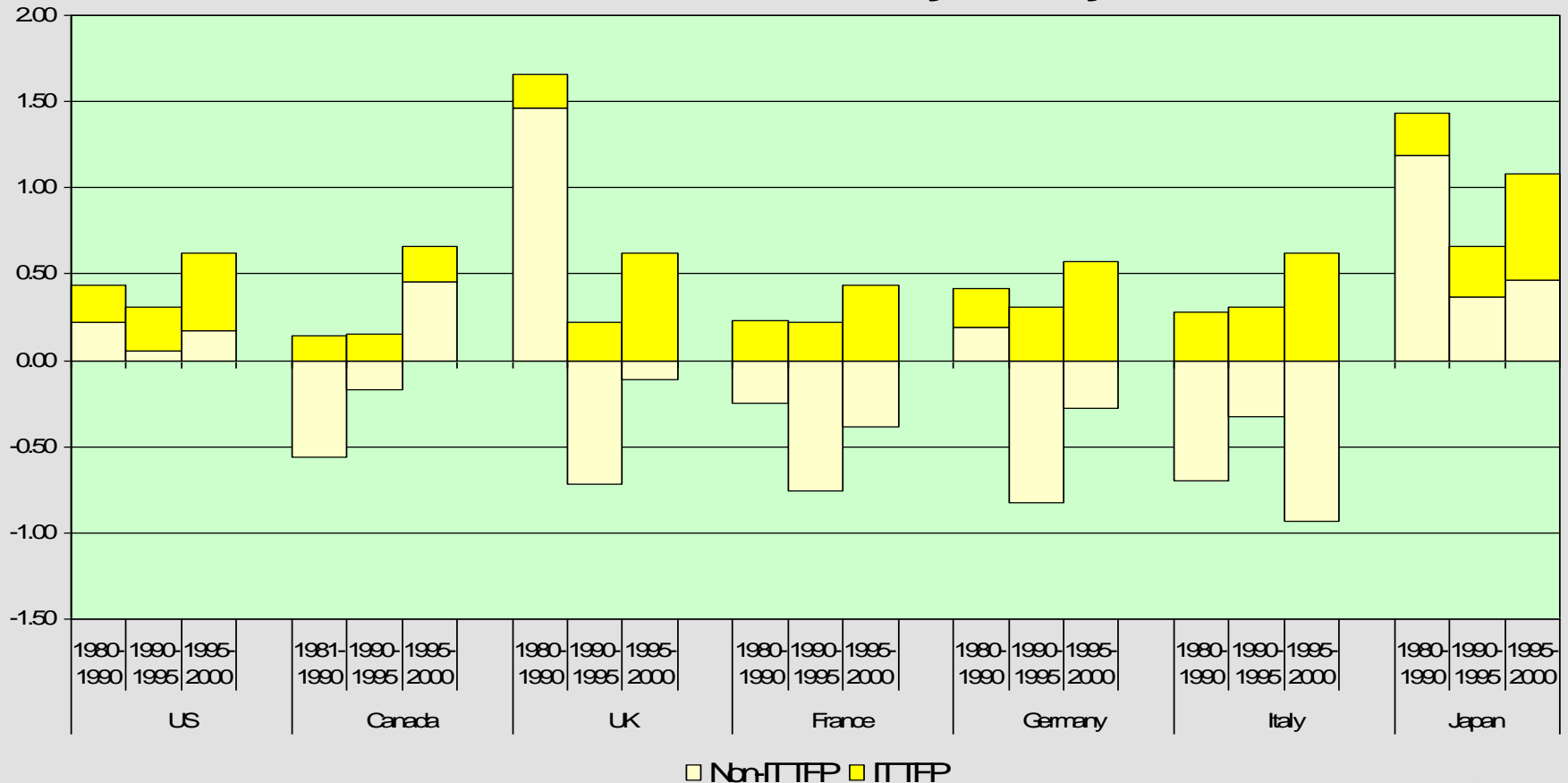


WISR, Digital Opportunity Index: Opportunity, Infrastructure, Utilization 2005; uneven digital development

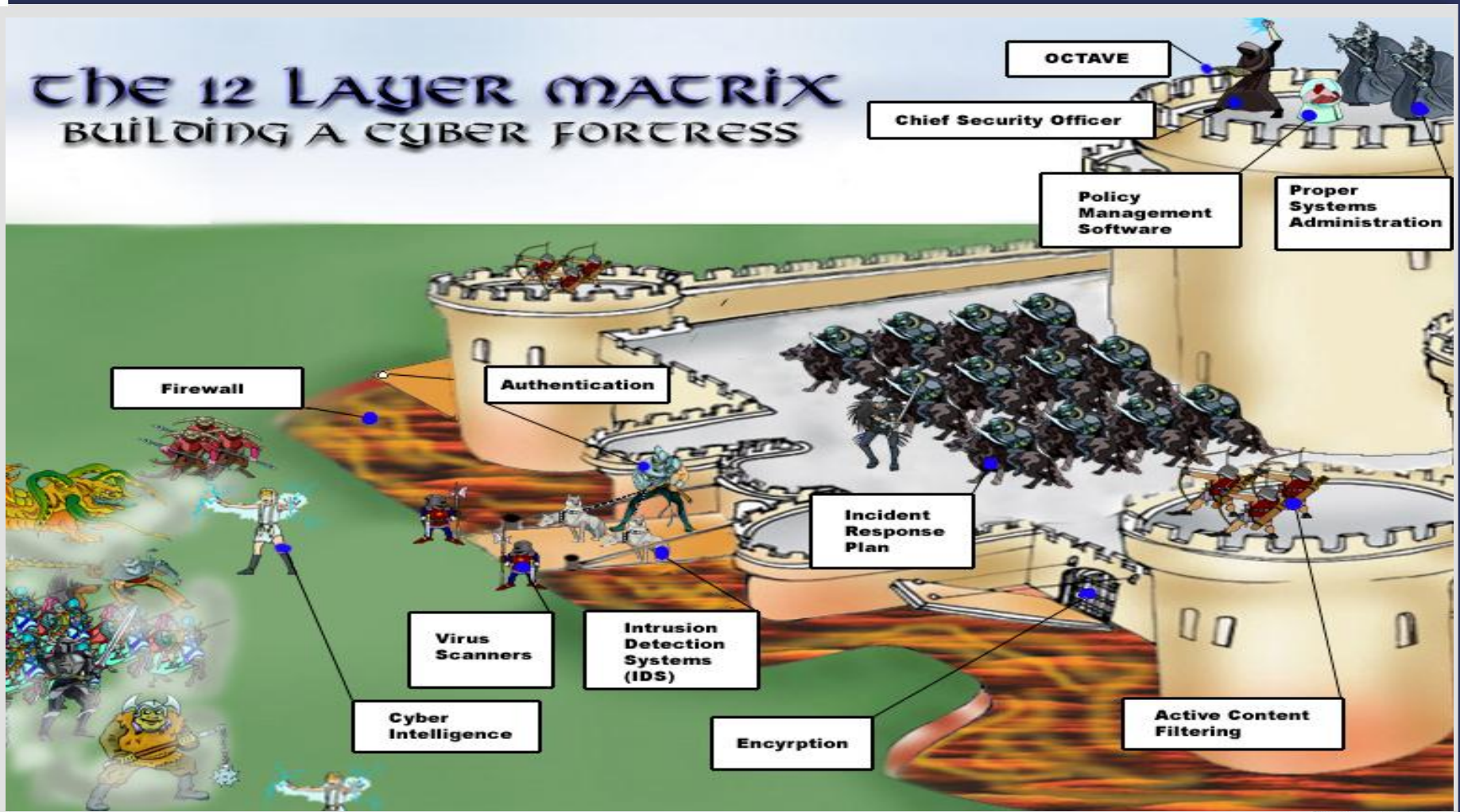


Economic Growth & IT (Source: Dale Jorgenson)

Sources of TFP Growth by Country



Cascading Risk: the Cyber Fortress (Source: Tom Kellerman)



IT Governance has both micro and macro dimensions, private and public aspects

IT Governance:

Public dimension: enabling framework for Digital economies & societies. E-Government imperative

Private dimension

“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 organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives.”

IT governance is concerned about two responsibilities:

IT must deliver value and enable the business

IT-related risks must be mitigated.



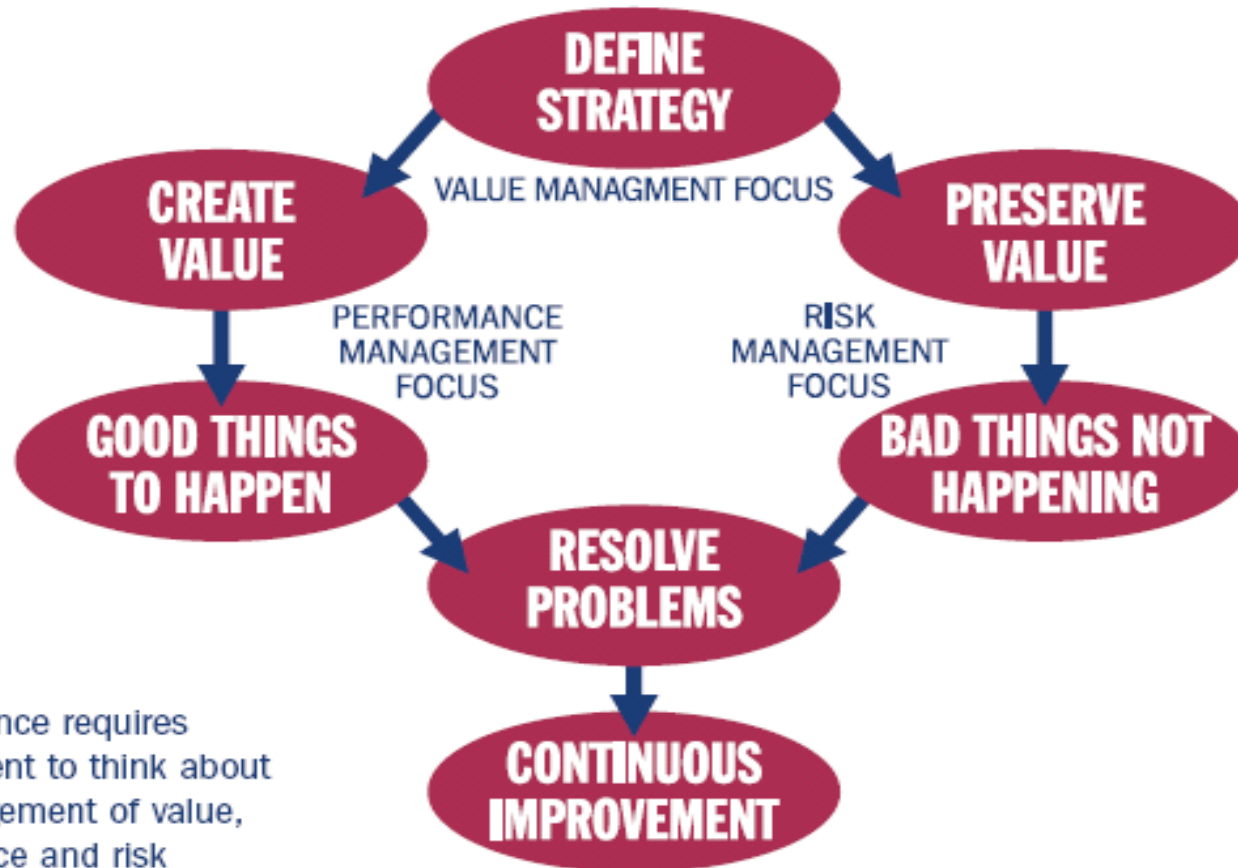
Standards: Control Objectives for Information and related Technology (COBIT)

COBIT covers four domains:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

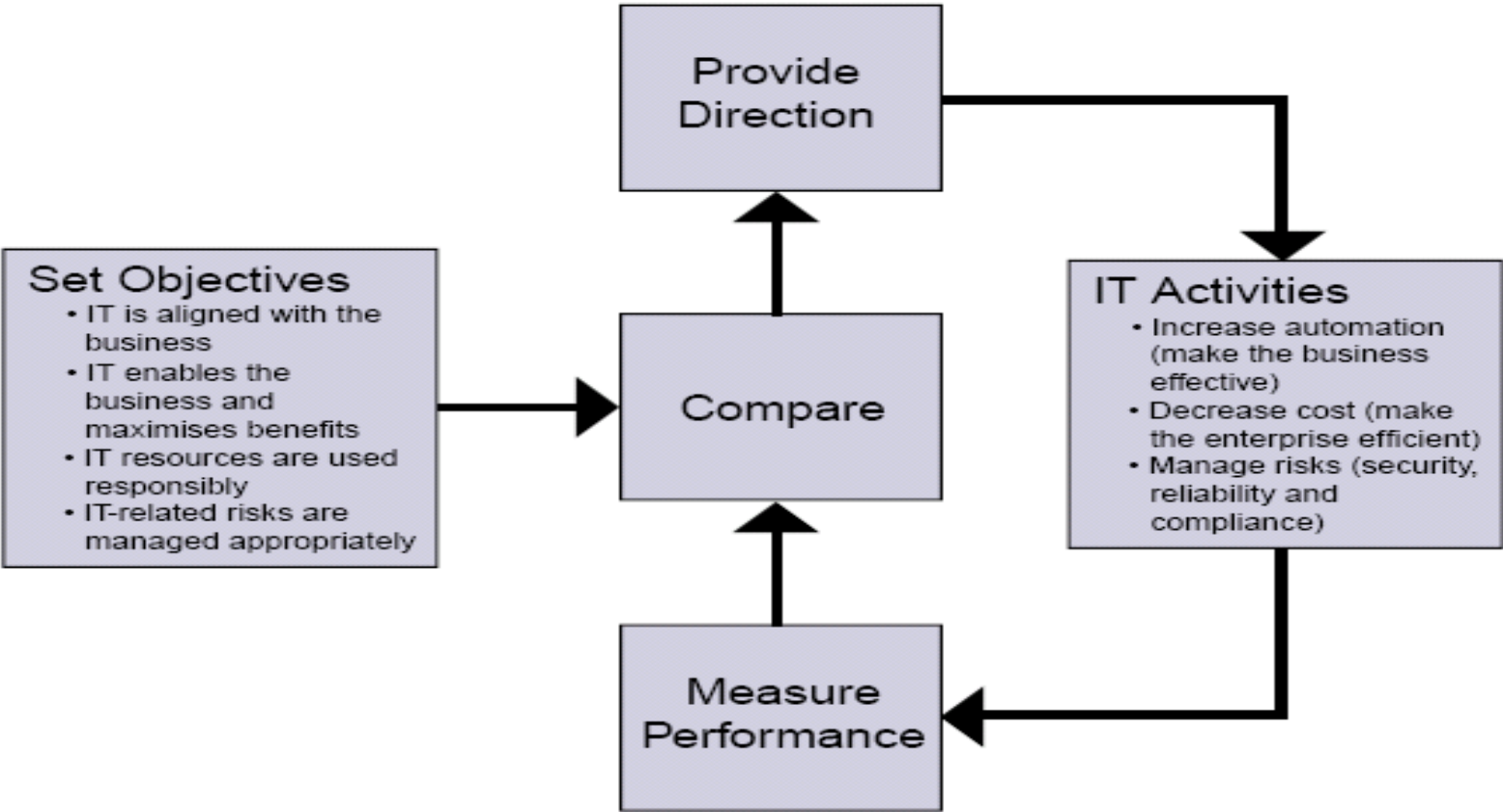


Figure 6

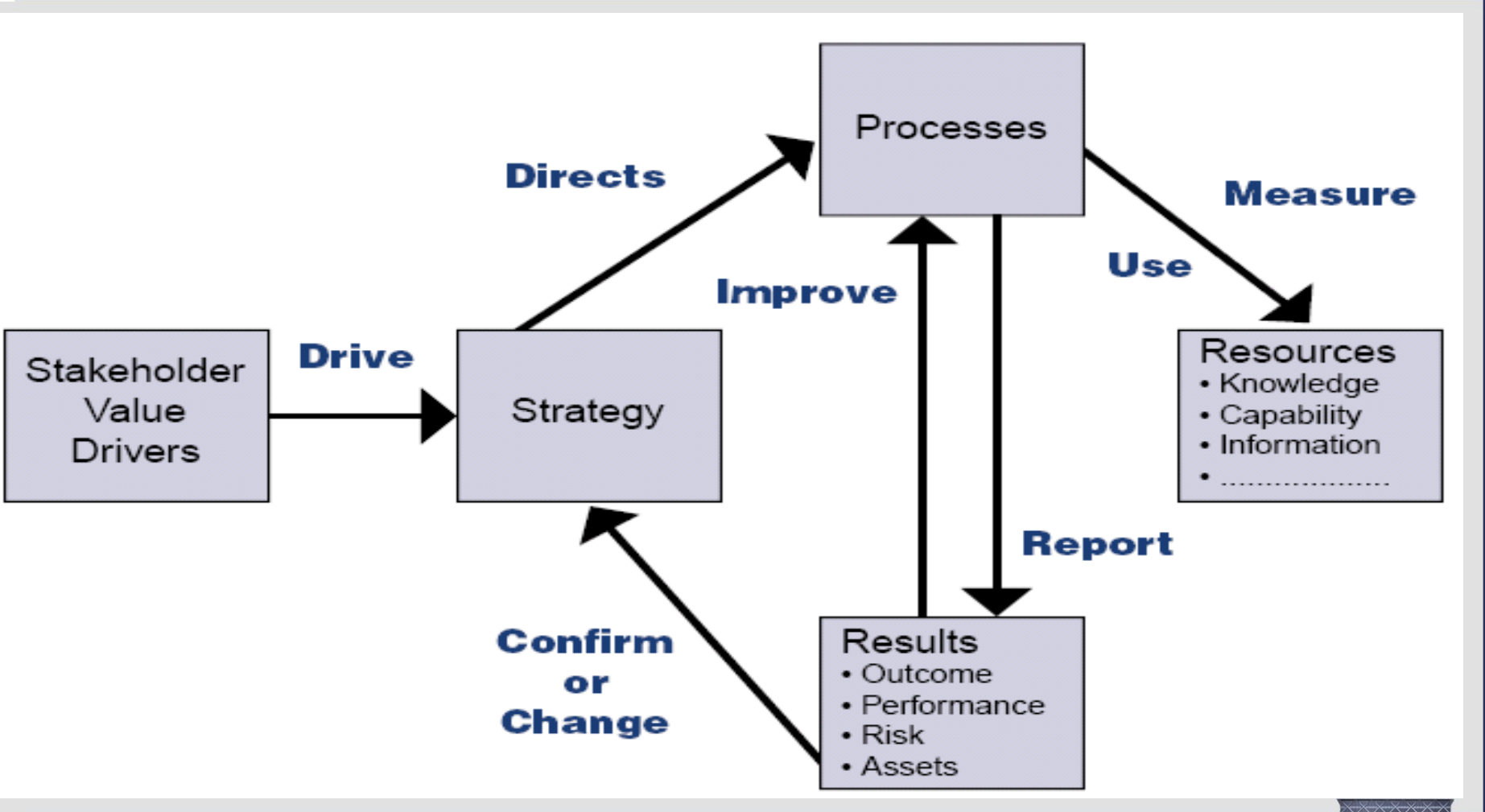


IT Governance requires management to think about the management of value, performance and risk

IT Governance Framework (Source: ITGI)



IT Governance Process (Source: ITGI)



AGENDA

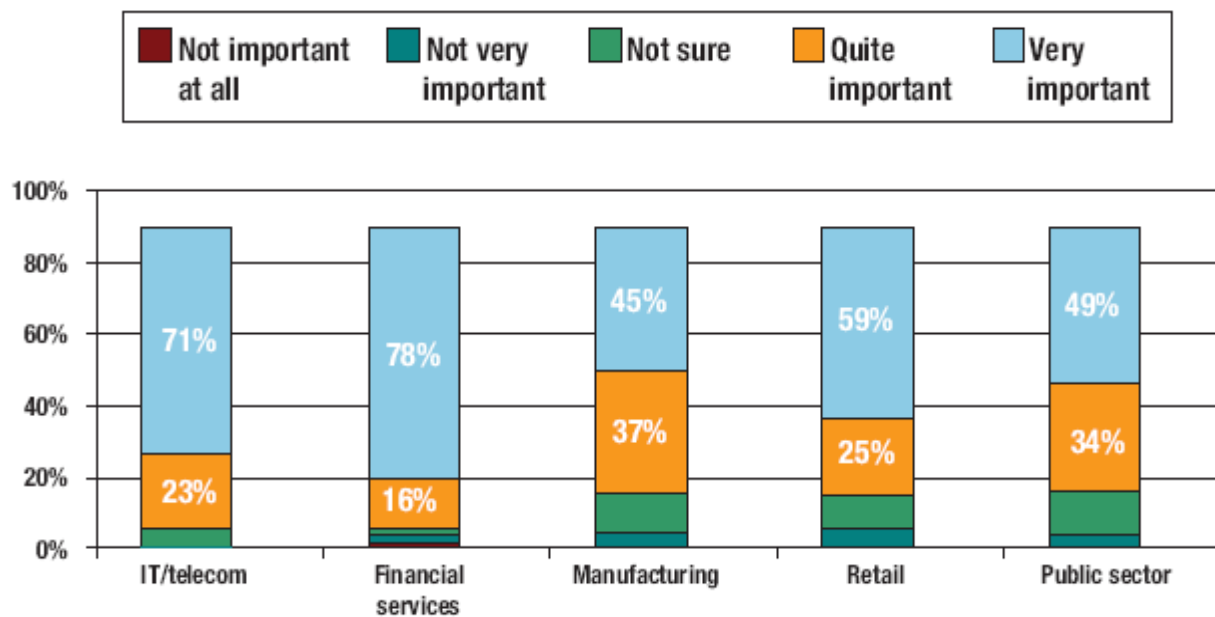
- ISSUES
- CODES & STANDARDS
- **SURVEY RESULTS**
- RECOMMENDATIONS

source will appear at the bottom



IT GOVERNANCE GLOBAL STATUS REPORT 2006 (ITGI)

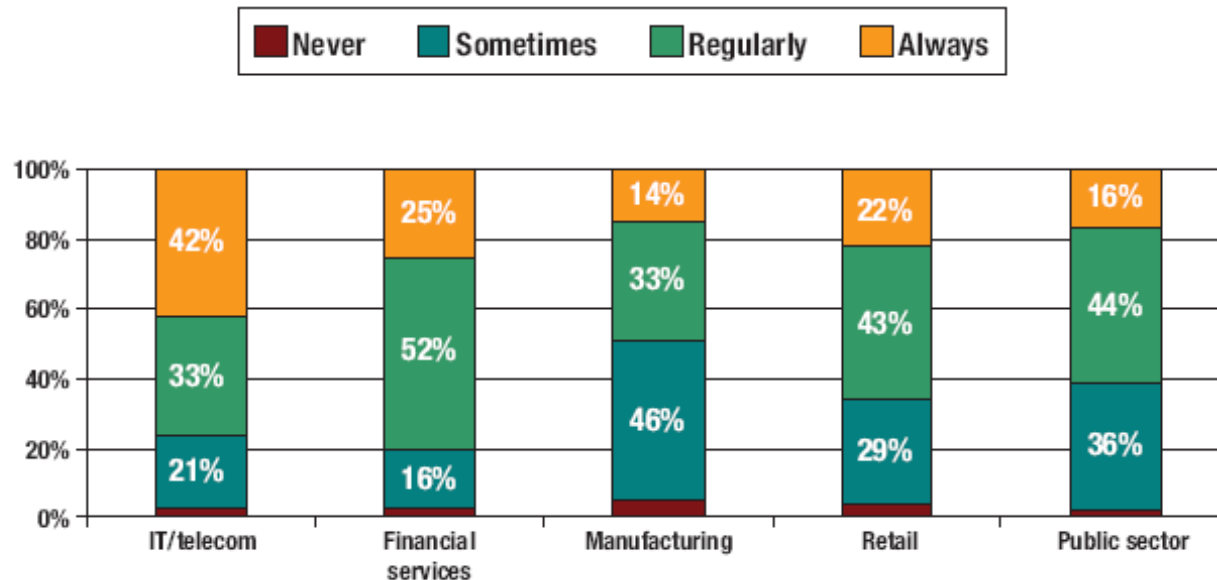
Figure 6—Importance of IT for Overall Strategy, by Industry Sector



Observation: IT's perceived importance is higher in the IT/telecom and financial services sectors, while it is seen as less important in manufacturing, retail and the public sector.

IT GOVERNANCE GLOBAL STATUS REPORT 2006 ([2])

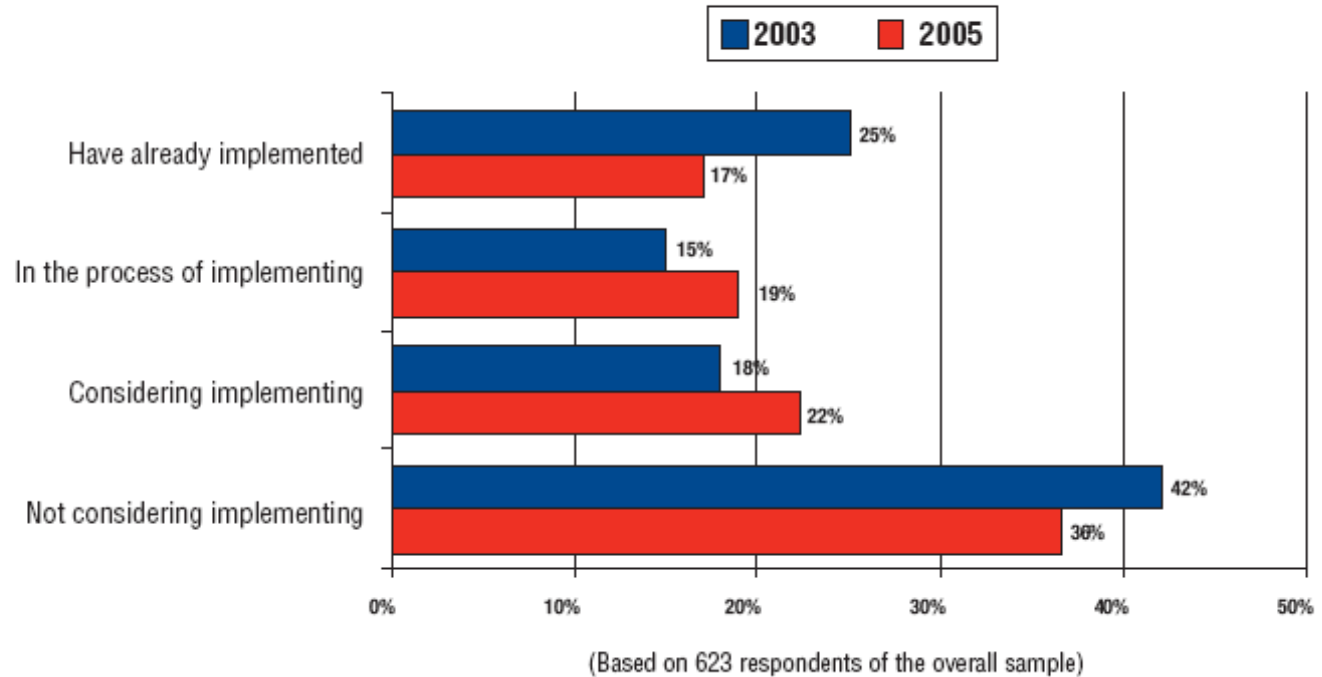
Figure 9—Frequency of IT on Board Agenda, by Industry Sector



Observation: IT is included on the board agenda most often in IT/telecom and financial services, and least often in manufacturing. This result is in line with the result of the previous question, which indicated that IT is more important to delivering on the organisation's strategy in the IT/telecom and financial services sectors than in the other sectors.

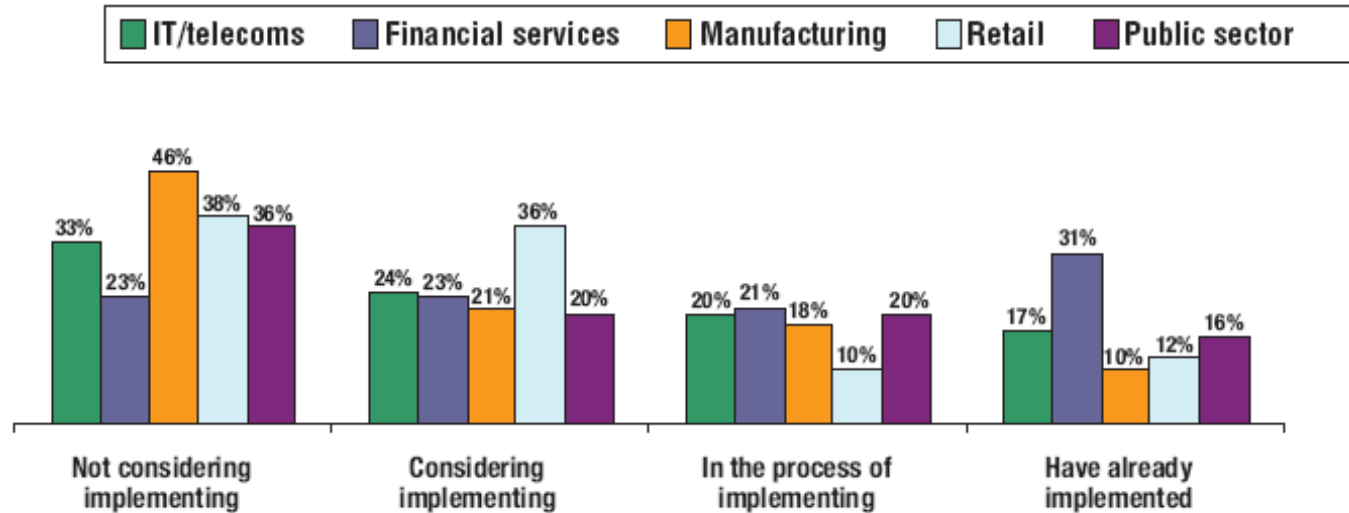
IT GOVERNANCE GLOBAL STATUS REPORT 2006 [3]

Figure 27—IT Governance Implementation Status



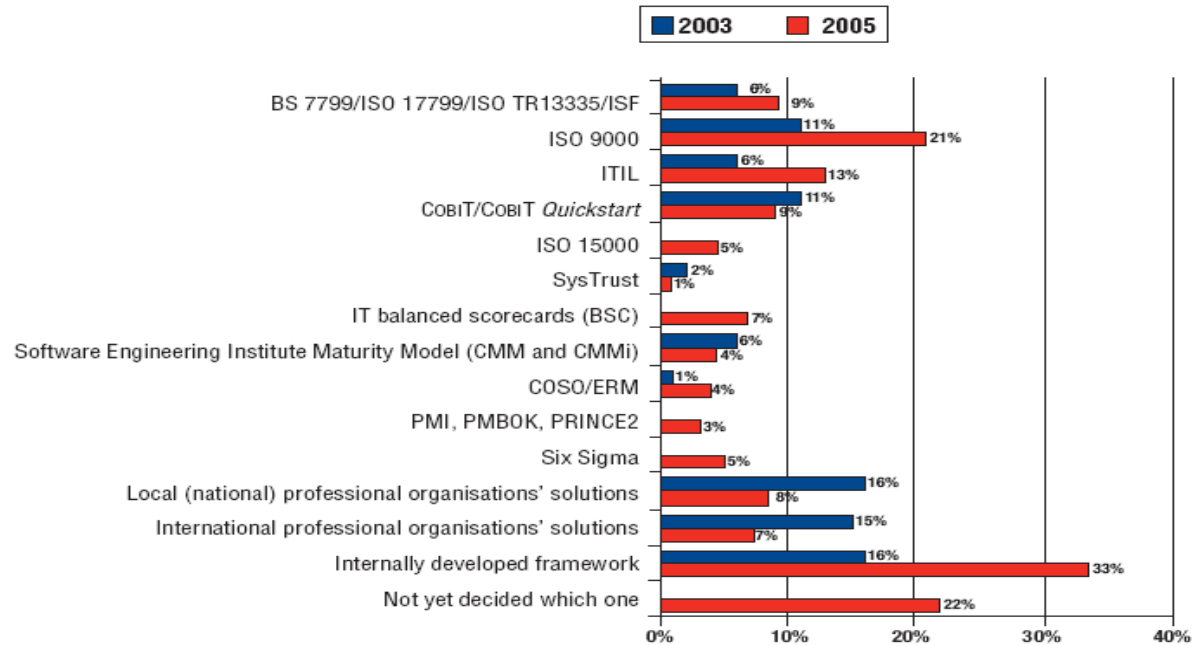
IT GOVERNANCE GLOBAL STATUS REPORT 2006 [4]

Figure 28—IT Governance Implementation Status, by Industry Sector



IT GOVERNANCE GLOBAL STATUS REPORT 2006 [5]

Figure 30—Selected IT Governance Frameworks



(Based on 440 respondents of the overall sample)

Observation: One-third of the participants use or are considering using an internally developed framework. Compared with 2003, the use of COBIT has decreased slightly. A possible explanation for this evolution could be that COBIT often acts as a baseline, in partial or complete form, to further elaborate an internally developed framework. Therefore, COBIT may be an integral (but not publicly acknowledged) part of the internally developed frameworks reflected in these responses.

Critical Elements of Information Security Program Success Survey by ISACA 2005

- Senior management commitment to information security initiatives
- Management understanding of information security issues
- Information security planning prior to implementation of new technologies
- Integration between business and information security
- Alignment of information security with the organization's objectives
- Executive and line management ownership and accountability for implementing, monitoring and reporting on information security



Comments on KPMG Survey 2007

- Business continuity is mainly viewed as IT whereas it is a comprehensive and strategic
- Business continuity drivers: respondents appear to neglecting outsourcing and supply chain issues
- Internal risks are the major issue: look inside the fortress!
- Non-adoption of International IS standards is a major weakness

Some Recommendations

- Information Security and IT Governance are strategic issues:
 - Put IT governance on the agenda of the Boards
 - Form Board IT Committees
- Businesses need to undertake threat and vulnerability analyses
- Businesses should adopt international standards: Control Objectives for Information and related Technology (COBIT)
- Digital economies and societies are vulnerable: protect critical infrastructure

