GOVERNANCE OF INFORMATION TECHNOLOGY (IT)

Chapter 10

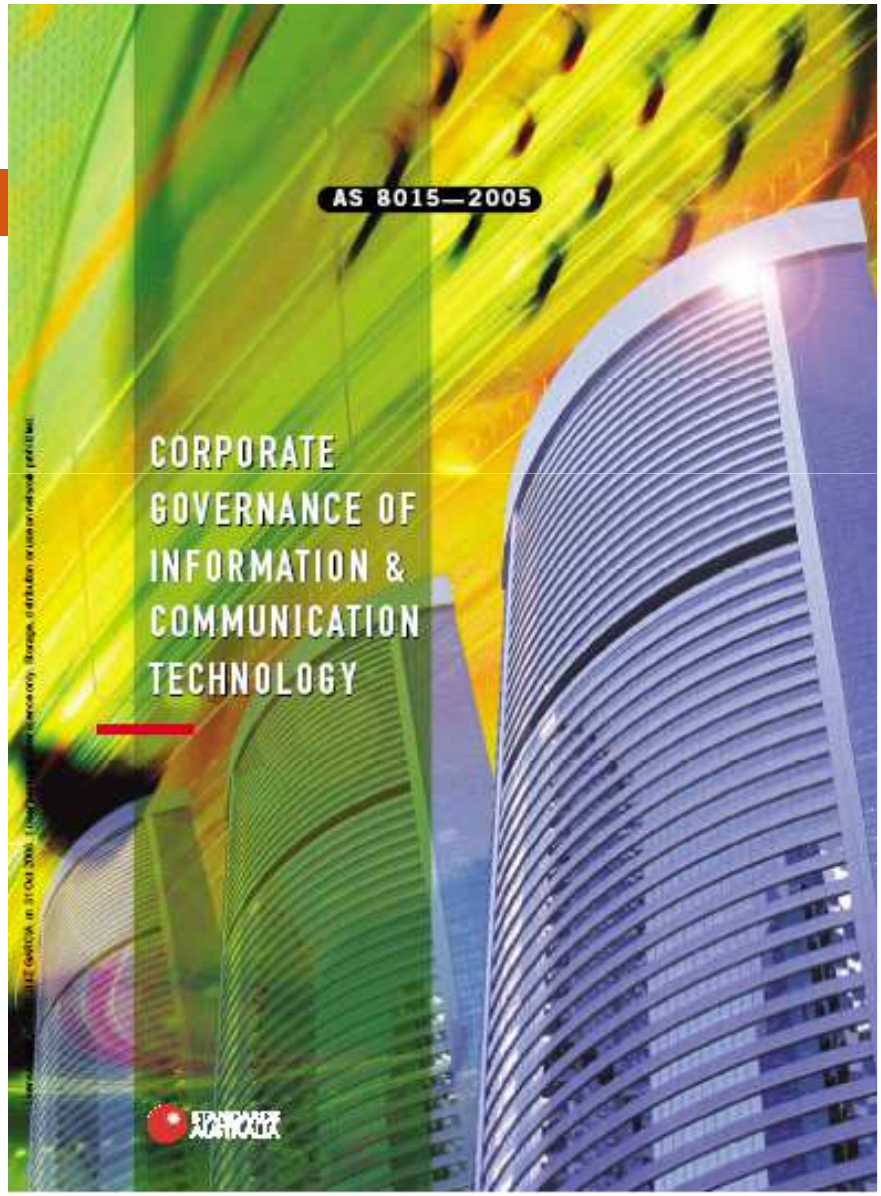
“*Standards are generally required when excessive diversity creates inefficiencies or impedes effectiveness*”. E.W. Hammond y J.J. Cimino

Summary

1. Introduction. Governing IT.
2. Management vs. Governance.
3. Decision-making and …
4. … structures of governance of IT.
5. Starting a framework for IT governance in their company without standards.
6. Business strategy, performance and governance of IT.
7. Align IT: indicators of progress.
8. The role of the CIO: IT leadership.
9. The value of IT.
10. ISO 38500, a conceptual model: the six principles of the standard.
11. Adapting the conceptual model of governance to the reality of the company.
12. Example Apps to aid decision-making for CIOs
13. Example Application Portfolio Management
14. To govern public enterprises, The 4 "E's"

Basic Reference

- Australian Standard Committee IT-030, IT Governance. Council of Standards Australia, 2005.
- ISO/IEC 38500:2008

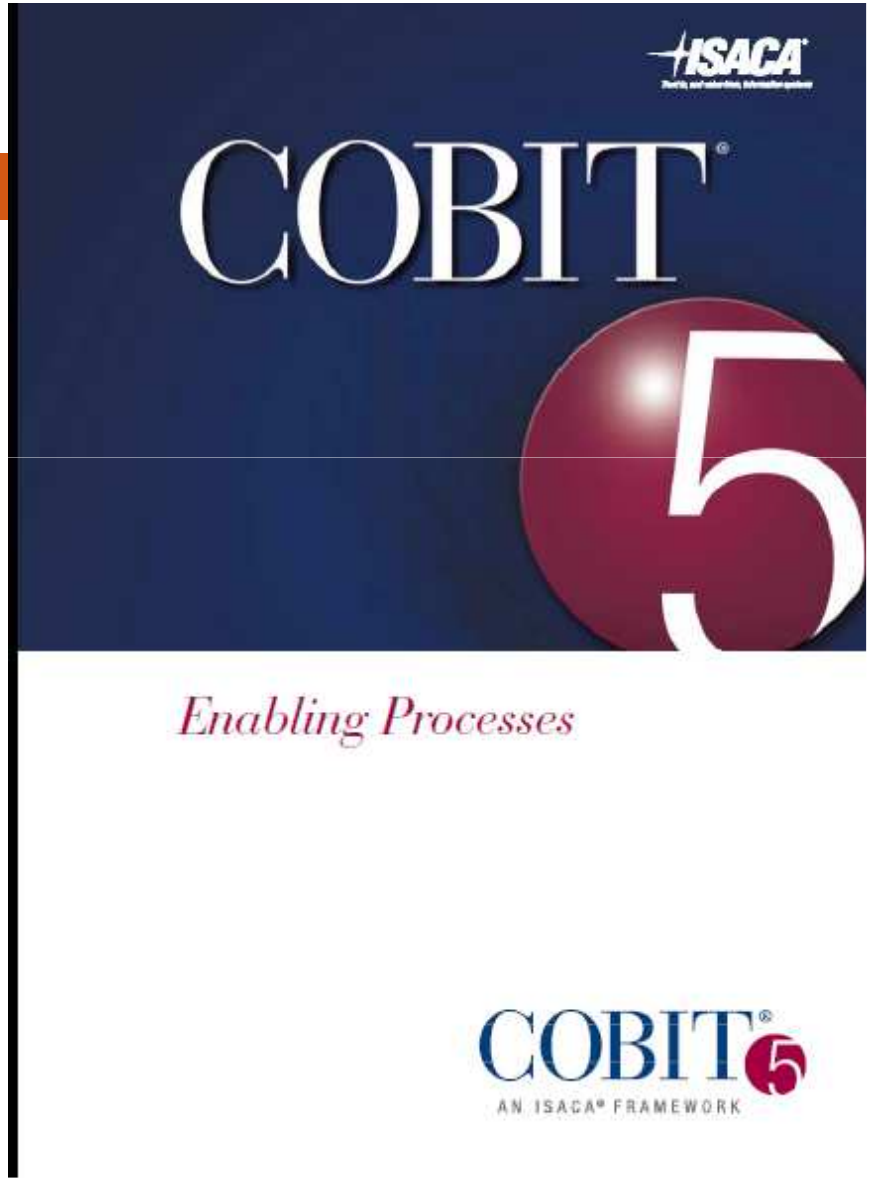


Basic Reference

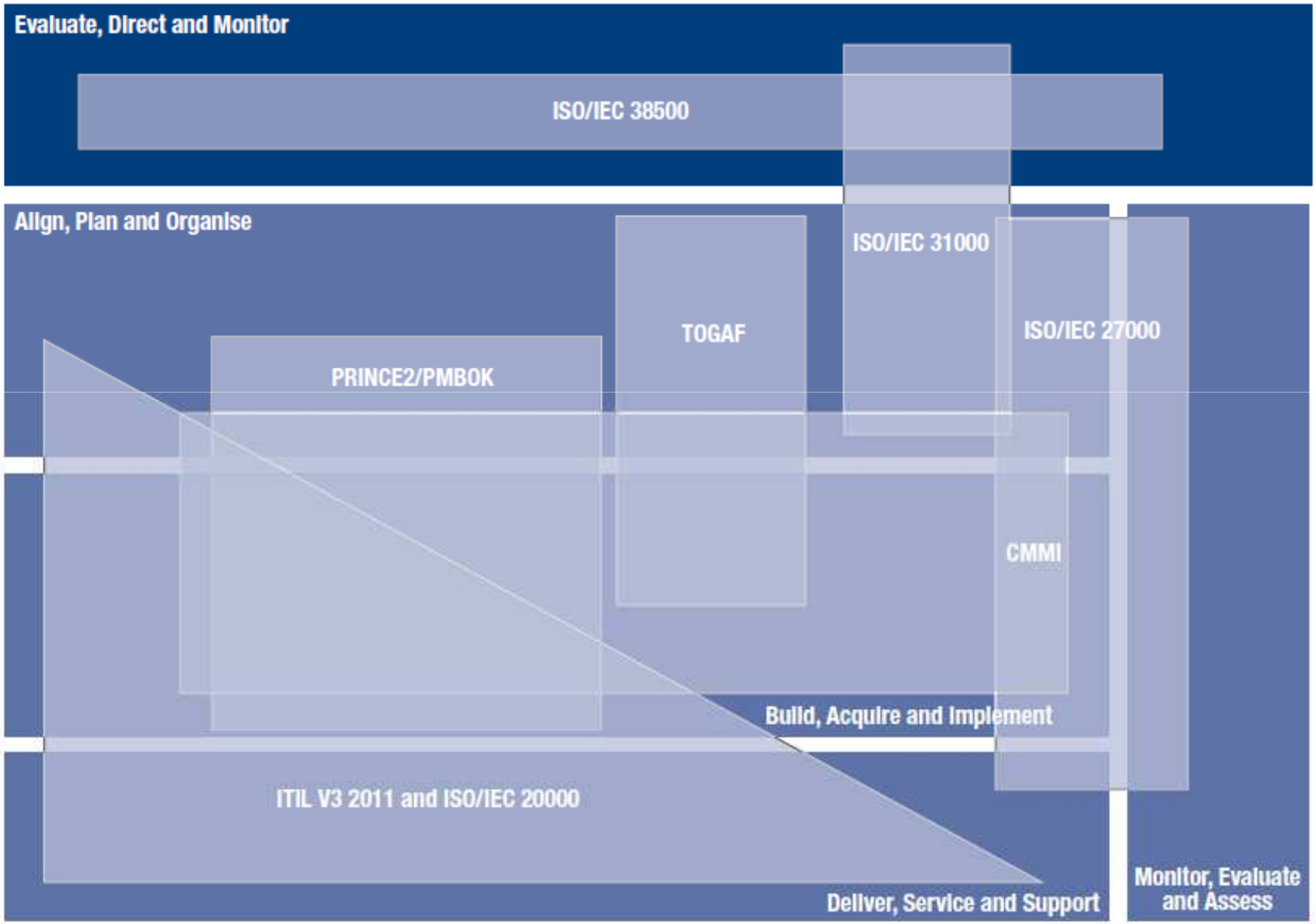
- *Waltzing with the Elephant* (2009). Mark Toomey, Infonomics Pty Ltd.

Basic Reference

- *ISACA*
  COBIT® 5: Enabling Processes, ISBN 978-1-60420-241-0
  United States of America



COBIT 5 vs. Rest of the world



Steps to Govern IT

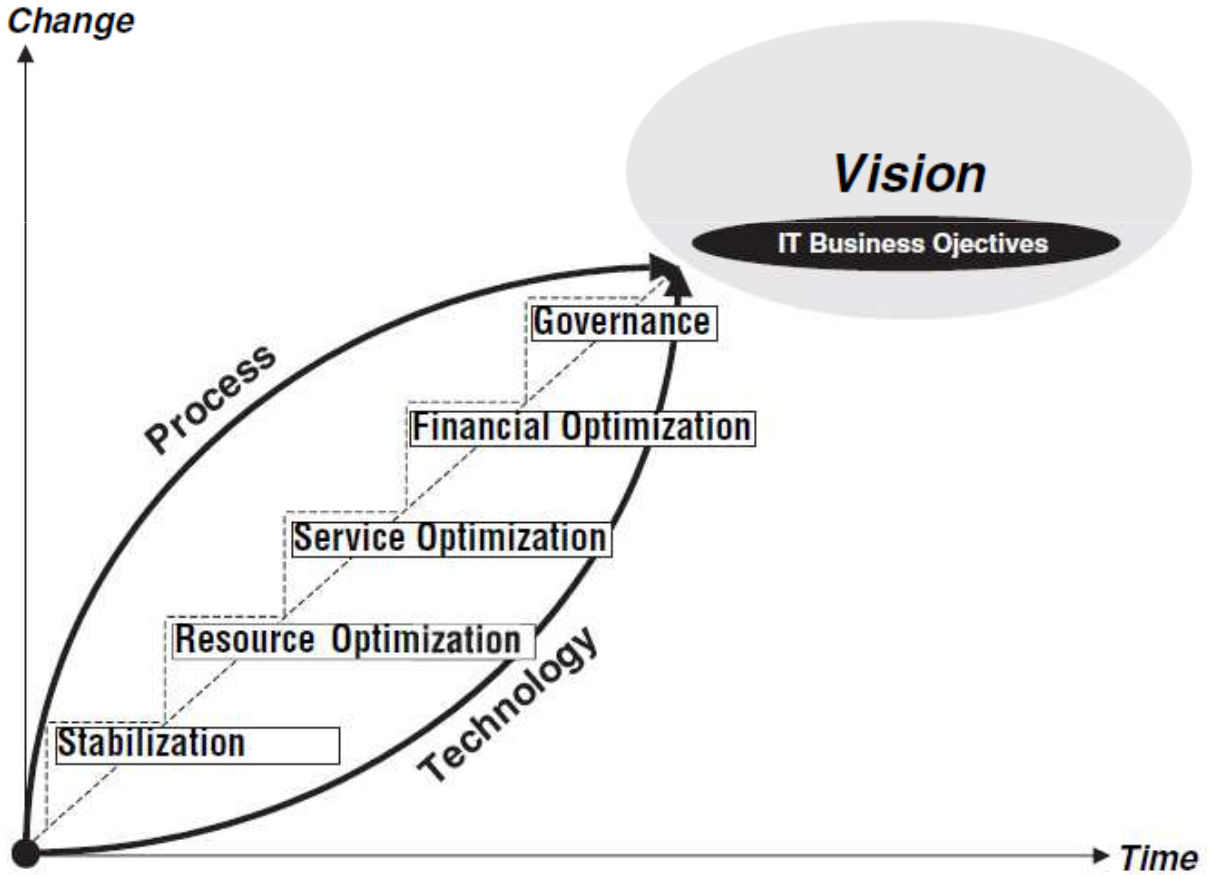
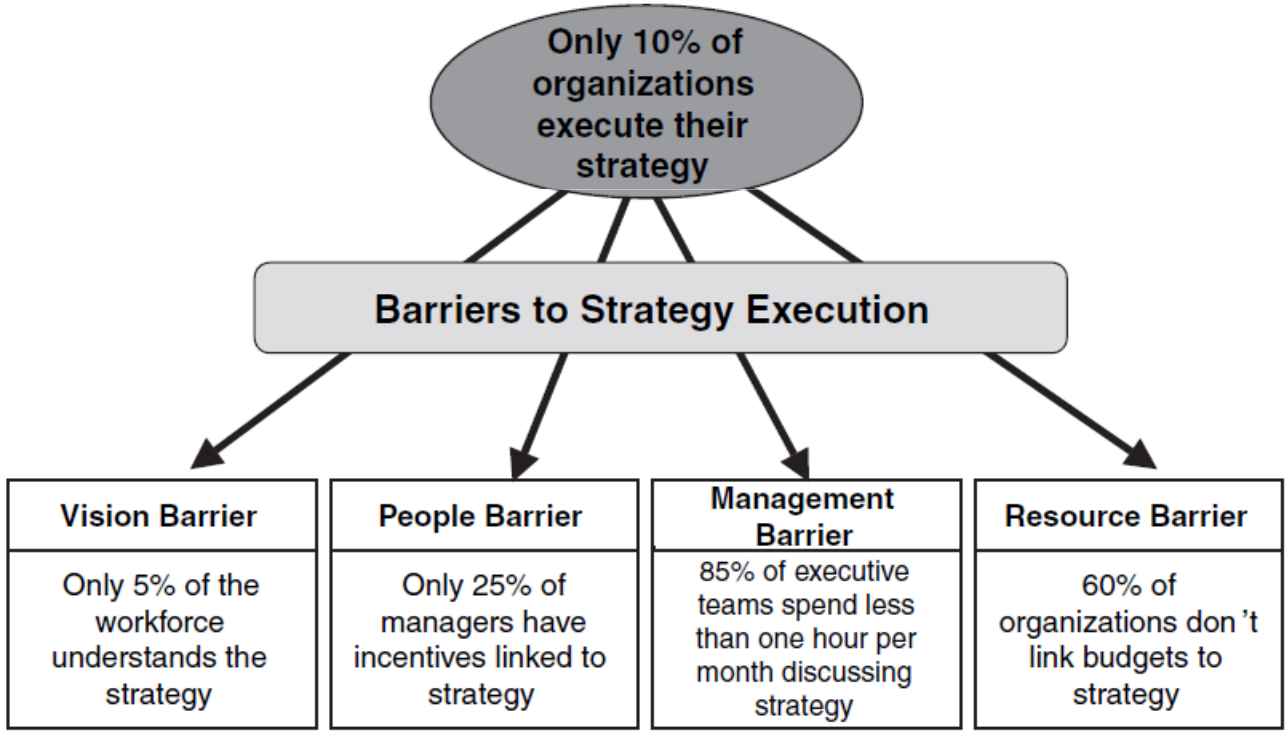


EXHIBIT 4.1 SAS's Steps to IT Governance

Strategy Barriers

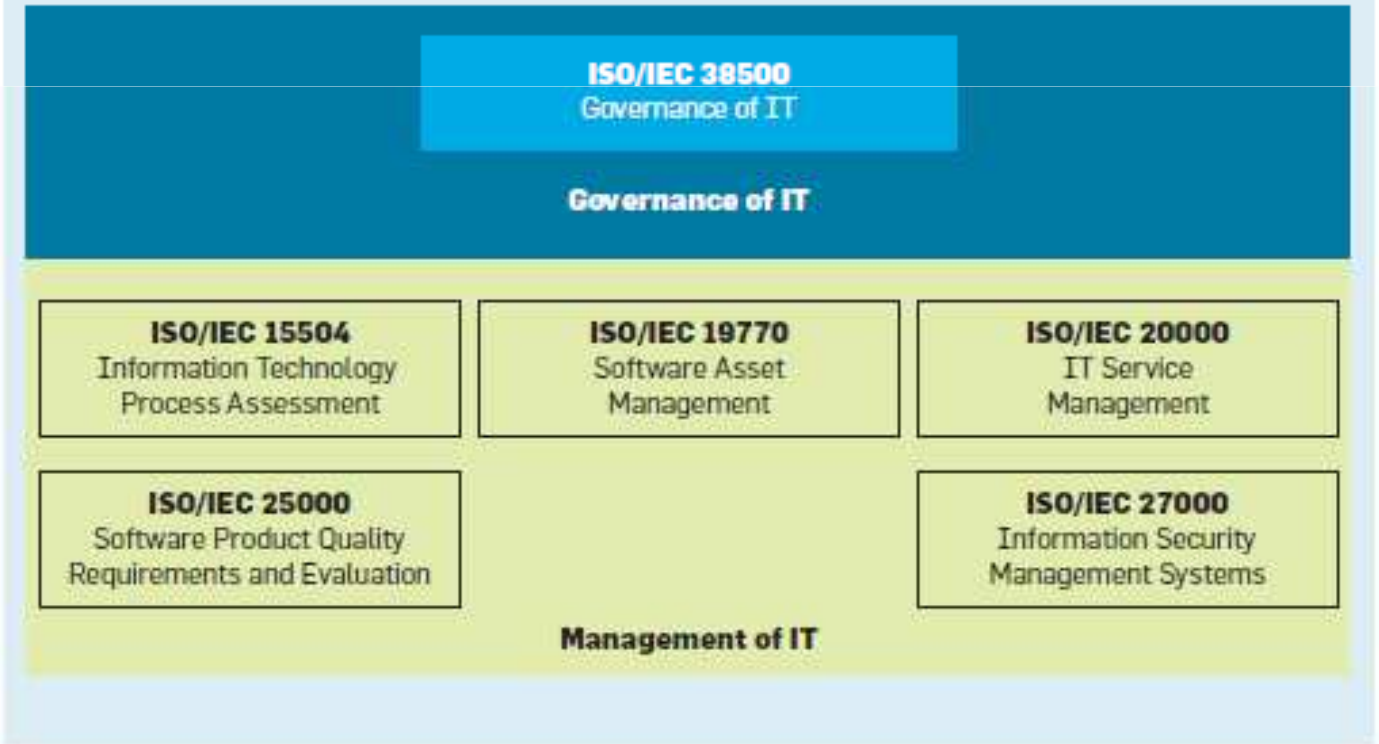


Adapted from material developed by Robert S. Kaplan and David P. Norton

EXHIBIT 5.2 The Barriers to Implementing Strategy

ISO/IEC Standards

Figure 1. Main ISO/IEC standards of IT management and governance of IT.



ISO/IEC 38500

- Information technology (IT) has become pervasive in supporting and enabling the strategy of organizations and this prevalence mandates the governance of IT as an organizational imperative.
- Organizations have made significant investments in IT to automate business processes and to communicate and transact electronically with their customers and suppliers.

ISO/IEC 38500

- The benefits from these investments have unfortunately not always materialised and in some instances organizations have incurred significant financial and reputational damage as a result of IT failures. This has further heightened governing body awareness of the need for the governance of IT and of their responsibilities in this regard.
- It may be, however, that some governing bodies are uncertain of what arrangements they need to have in place for the governance of IT.

ISO/IEC 38500

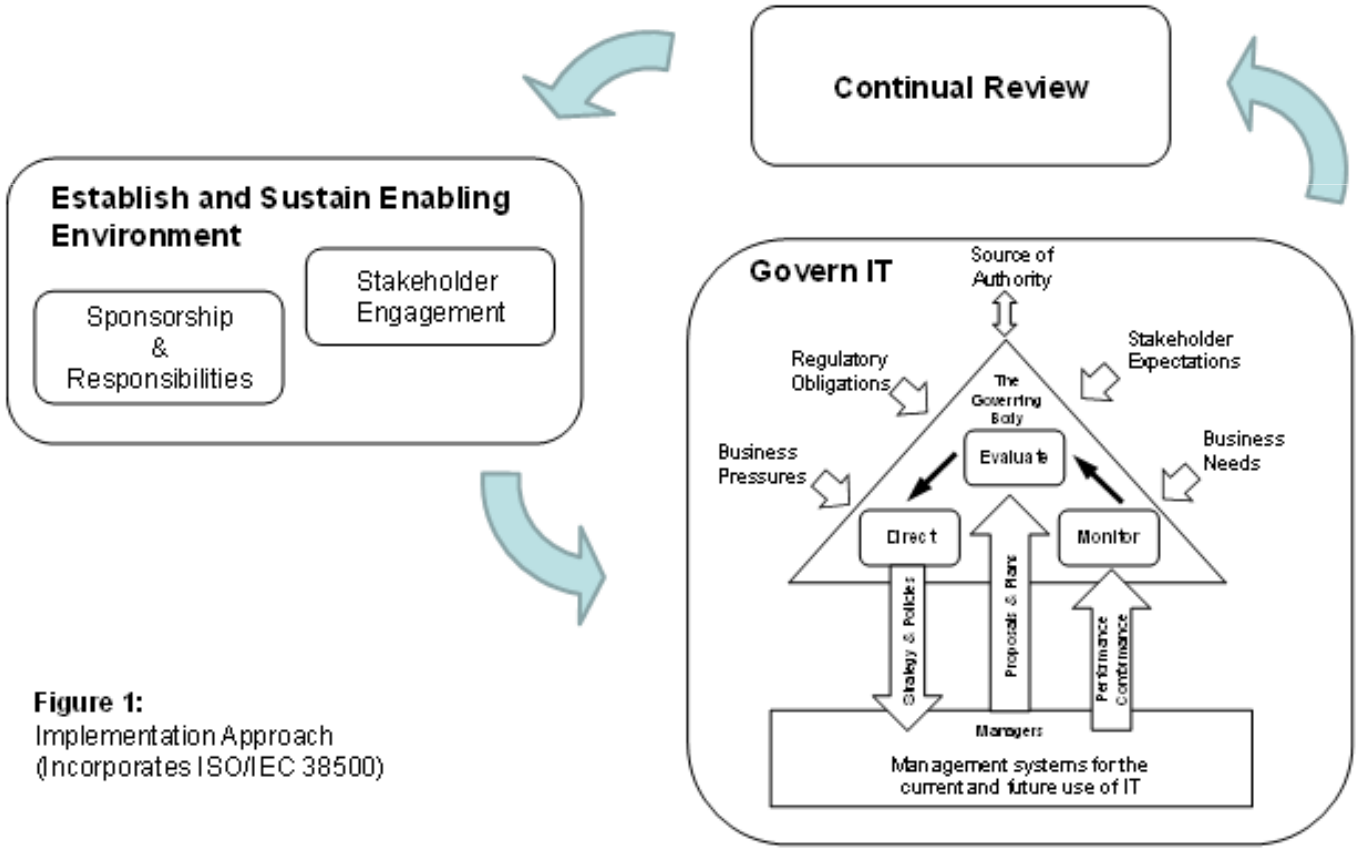
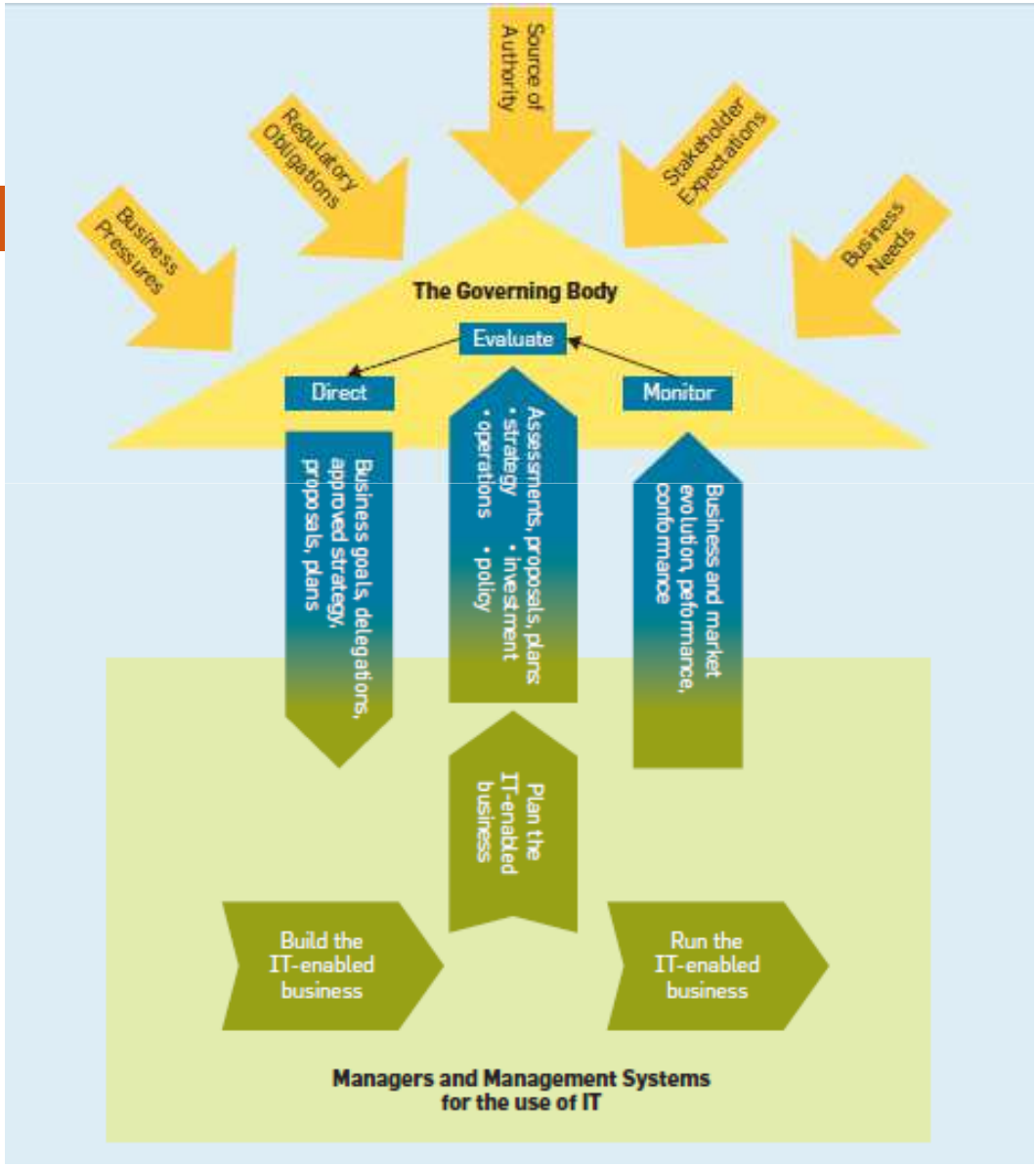


Figure 1:
Implementation Approach
(Incorporates ISO/IEC 38500)

ISO/IEC 38500

- The three activities of the governance model in ISO/IEC 38500, namely evaluate, direct and monitor, take place in the Govern IT phase. These are framed and guided by the six principles of the standard (responsibility, strategy, acquisition, performance, conformance, human behaviour) within the context of the internal and external environments, as well as organization’s culture for the governance of IT.

ISO/IEC 38500 Model



ISO/IEC 38500

- It is important to focus and describe what the result of the governance of IT should be when applying the ISO/IEC 38500 framework, rather than being process or control oriented. This will ensure that the governing body determines what needs to be achieved, rather than prescribing how it should be done, thereby appropriately guiding or steering the organization in its use of IT.
- In addition, an appropriate mechanism of assessment is required, which must take into account the principles-based nature of ISO/IEC 38500.

Principles ISO/IEC 38500

Responsibility

- Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions

Principles ISO/IEC 38500

Table B.1: Assessment criteria for the Responsibility principle

Beneficial Outcomes	Evidence of Success
The organization successfully implements IT enabled business change	Executive managers lead business process, organization structure and human change when implementing IT solutions
Organizational value is generated by IT	Executive managers treat IT as an investment for return, not solely as a cost to be reduced
The organization receives the quality of services it requires in the most effective and efficient manner possible	Executive managers determine the best IT delivery model considering : o Decision rights and control structures (central, de-central, federal, etc.) o Supply : Optimising the provision of IT (sourcing strategy)

Principles ISO/IEC 38500

Strategy

- The organization’s business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and on-going needs of the organization’s business strategy.

Principles ISO/IEC 38500

Table B.2: Assessment criteria for the Strategy principle

Beneficial Outcomes	Evidence of Success
The organization's operations are effectively supported by IT and strategic change is appropriately enabled by IT	IT clearly aligned to business strategy and architecture
The organization's decision support systems provide high quality and timely information	The business requirements regarding usability, confidentiality, integrity and availability of data used for decisions are identified and met.
The organization's objectives are enabled through IT innovation	IT used to: o Enable, disrupt and redefine business models o Engage and connect with customers

Principles ISO/IEC 38500

Acquisition

- IT acquisitions are made for valid reasons, on the basis of appropriate and on-going analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

Principles ISO/IEC 38500

Table B.3: Assessment criteria for the Acquisition principle

Beneficial Outcomes	Evidence of Success
Investments in IT prioritised on the extent to which their potential contribution to the business is both attractive and achievable	IT investments structured into portfolios, returns on investments required to meet hurdle rates
Business requirements are fully supported by selected IT solutions	IT solutions procurement process ensures that functionality, usability, architectural, security, performance, availability, etc. requirements are met
Implementation programs proceed according to plan and achieve business benefits	Change programs structured to deliver business capabilities with careful management of costs, risks, schedule and benefits

Principles ISO/IEC 38500

Performance

- IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements

Principles ISO/IEC 38500

Table B.4: Assessment criteria for the Performance principle

Beneficial Outcomes	Evidence of Success
All stakeholders able to interact and transact with IT systems that provide the services, levels of service and service quality to meet their requirements	IT appropriately responsive and available even in the event of high demand and or disaster. IT changes and upgrades effected only with planned disruption to the business.
Information is complete, accurate, secure and accessible	IT is protected against unauthorised access or changes to data. Controls in place to ensure the integrity of data
Stakeholders effectively assisted when requesting IT support	Effective service desk that resolves requests, incidents & problems and ensures that customers are assisted within defined service levels

Principles ISO/IEC 38500

Conformance

- IT complies with all mandatory legislation and regulations. Policies and practices clearly defined, implemented and enforced.

Principles ISO/IEC 38500

Table B.5: Assessment criteria for the Conformance principle

Beneficial Outcomes	Evidence of Success
The organization's policies, rules and mandates are accurately implemented by IT	Mature IT processes and controls in place, ensuring conformance to organizational policies, service requirements and risk appetite
The organization properly manages its information and transactions so that there are no breaches of legal and/or regulatory requirements	On-going monitoring of relevant legislation, implementation of necessary IT processes and controls and provision of independent assurance

Principles ISO/IEC 38500

Human Behaviour

- IT policies, practices and decisions demonstrates respect for Human Behaviour, including the current and evolving needs of all the ‘people in the process’.

Principles ISO/IEC 38500

Table B.6: Assessment criteria for the Human Behaviour principle

Beneficial Outcomes	Evidence of Success
Stakeholders use the organization's IT in an acceptable manner	Executive managers provide leadership, supported by appropriate policy education, training and conformance monitoring for users & service providers
Business efficiency and value generated from staff using IT in a productive and effective manner	On-going education, training & competence testing for all users on all aspects of the use of the organization's IT