IT Governance from the standardization perspective - ISO 38500:2015

23 November 2018, Nicosia, Cyprus

Christos Tsiakaliaris | PMP, ISO27001 Lead Auditor

What is IT Governance? Definitions, Definitions, Definitions…

IT governance (ITG) is defined as the processes that ensure the effective and efficient ***use of IT in enabling an organization to achieve its goals****.*

Gartner.

CIO FROM IDG

IT governance is a formal framework that provides a structure for organizations to ***ensure that IT investments support business objectives****.*

IT governance is a formal framework that ensures the ***alignment of an organisation's IT and business strategy****.*

it governance™

techopedia

Information technology governance (IT governance) is the collective tools, processes and methodologies that enable an organization ***to align business strategy and goals with IT services, infrastructure or the environment****.*

What is IT Governance? More definitions…

ISO/IEC 38500:2015

A system *by which the current and future* ***use of IT is directed and controlled****.*

Governance ensures that stakeholder needs, conditions and options are evaluated to ***determine balanced, agreed-on enterprise objectives*** *to be achieved;* ***setting direction*** *through prioritisation and decision making; and* ***monitoring performance and compliance*** *against agreed-on direction and objectives.*

COBIT 5
AN ISACA® FRAMEWORK

IT Governance: How it will help my organisation?

- Improved business and IT alignment
- Clarity of responsibility and accountability for both the supply of and demand for IT in achieving the goals of the organization
- Ensures realisation of benefits from IT expenditure
- Ensures conformance with (regulatory, legislation, contractual) obligations
- Improved transparency of IT costs
- Improved performance
- Better responsiveness to market changes and opportunities
- Enhanced organisation image

ISO 38500:2015 – The standard for IT Governance

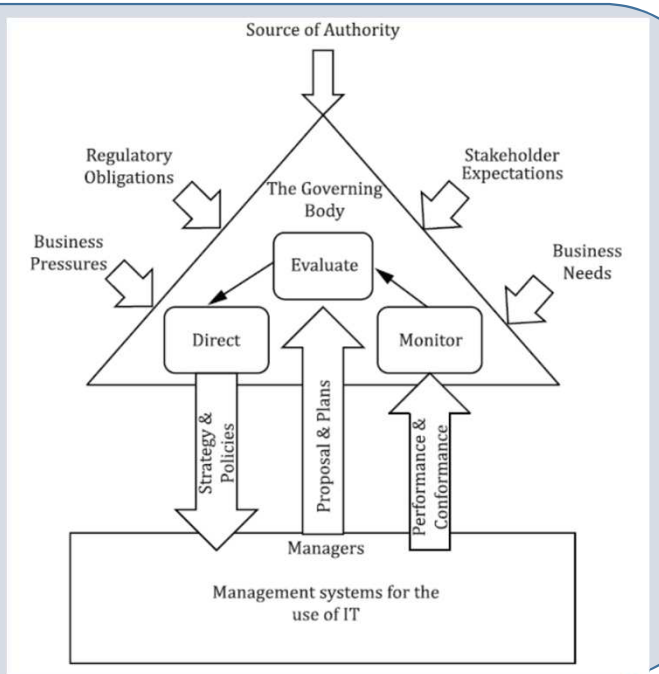
- Provides principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of information technology in their organizations
- Applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT
- Applies to all organizations regardless of their status (public, private, government, not-for-profit), size and extent of IT use

ISO 38500:2015 – The key elements

6 principles

1. Responsibility
2. Strategy
3. Acquisition
4. Performance
5. Conformance
6. Human behaviour

Model for the governance of IT



Supported by definitions, implementation guide, governance framework, …

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.

Source: ISO/IEC 38500:2015

- Investigation of options and assignment of responsibilities
  - Key considerations: Effectiveness, efficiency, acceptable use of IT
- Authorisation for decisions
- Adherence to strategies
- Reporting
- Monitoring of the performance of the people given responsibilities

Common issues with responsibility assignment

- Assignment of responsibilities only in theory -> “I want to control everything” type of assignment
- Assignment of responsibilities without any decision making authorisation -> “You are responsible but I will make the decisions”
- Lack of competences or status of the assignee

Strategy

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

Source: ISO/IEC 38500:2015

- Watch and be prepared for IT and business changes
- Employ appropriate risk management approach before making changes
- Adherence to strategies and policies
- Encourage the submission of proposals for making better use of IT
- Monitor the use of IT to ensure it is achieving its intended benefits

Common issues with business strategy

- The organisation plans without IT in mind:
  - Can the IT support the plans of the business?
  - Can the IT support be delivered on time and on expected levels?

- The IT makes development plans without thinking of the added value to be provided to the business:
  - New features?
  - Better response?
  - Enhanced continuity, security or availability?

Acquisition

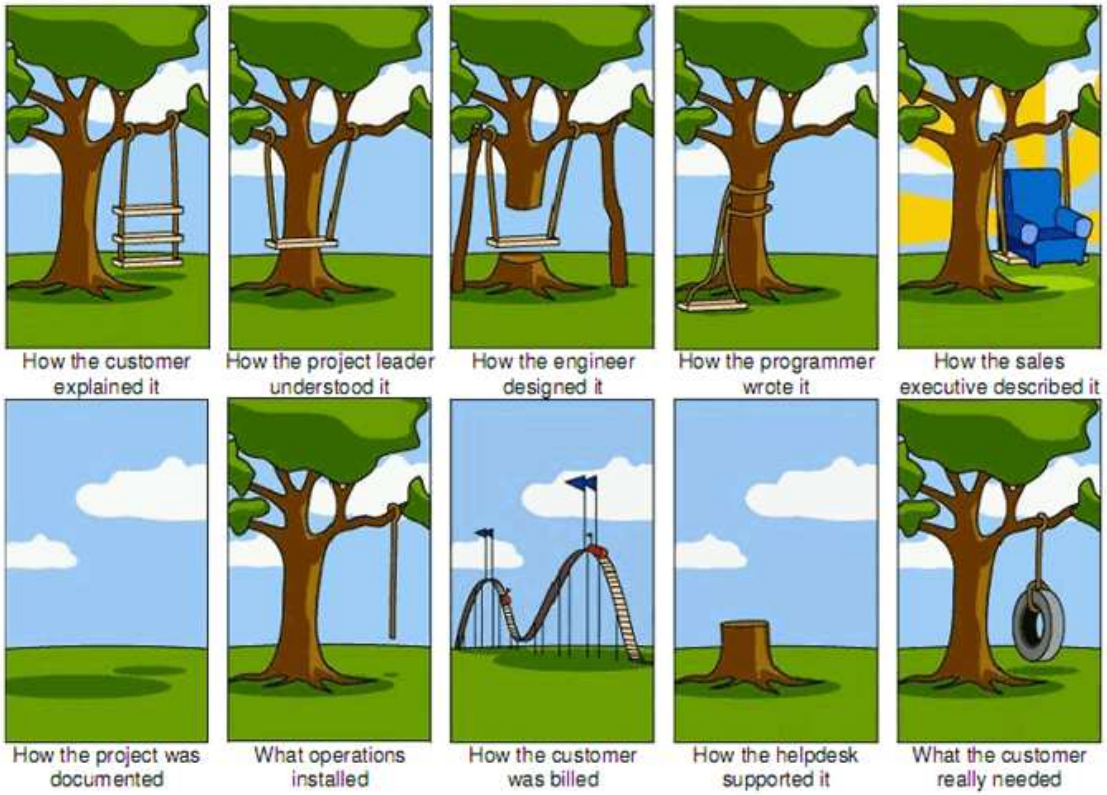
IT acquisitions are made for valid reasons, on the basis of appropriate and on-going analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

Source: ISO/IEC 38500:2015

- Investigation of options for the realization of approved proposals
  - Key considerations: Risks and value for money of proposed investments
- Ensure supply arrangements (internal and external) support the business needs of the organization
- Achieve common understanding between the organization that acquires IT and the supplier on the intended use of the IT
- Monitoring whether the IT investments deliver the expected features
- Monitoring of the suppliers' level of understanding of the organisation's needs as well as suppliers' performance

Common issues with acquisition

Common issues with acquisition



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.

Source: ISO/IEC 38500:2015

- Evaluation of proposals for IT developments
  - Key considerations: Level of support for business (capability, capacity), Risks
- Evaluation of risks deriving from the use of IT
- Evaluation of the effectiveness and performance of the organization's IT governance
- Adequate allocation of resources for the proper operation of IT
- Monitor the use of IT in support of the business
- Ensure policies are followed properly

According to business priorities and within budgetary constraints

Common performance issues

- Misalignment of levels of service with suppliers
- Security risks not identified, or addressed inefficiently
- Resources are never enough
- Unjustified budget increases, which are rarely recovered
- Lack of synchronisation between business and IT

Common performance issues

Over-performance

Under-performance

Conformance

The use of IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Source: ISO/IEC 38500:2015

- Conformance assessment against:
  - obligations, internal policies, standards, guidelines, etc.
  - the IT governance framework itself
- Establishment and issuance of policies and guidelines
- Code of ethics
- Regular audits

Common conformance issues

- Ineffective identification of conformance requirements
- Conformance requirements timely identified, but no budget available
- Complicated changes to IT systems needed to achieve compliance

Human Behaviour

IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving needs of all the 'people in the process'.

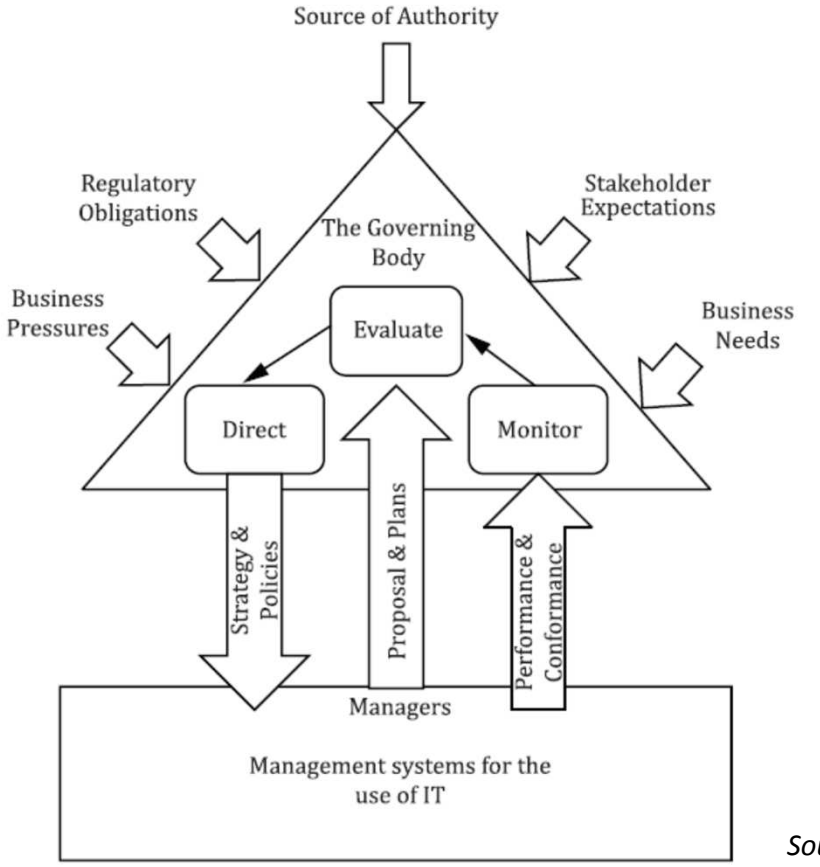
Source: ISO/IEC 38500:2015

- Respect for human behaviour in policies and work practices
- Encourage people to report risks, issues, problems, opportunities for improvement

Common issues with Human Behaviour

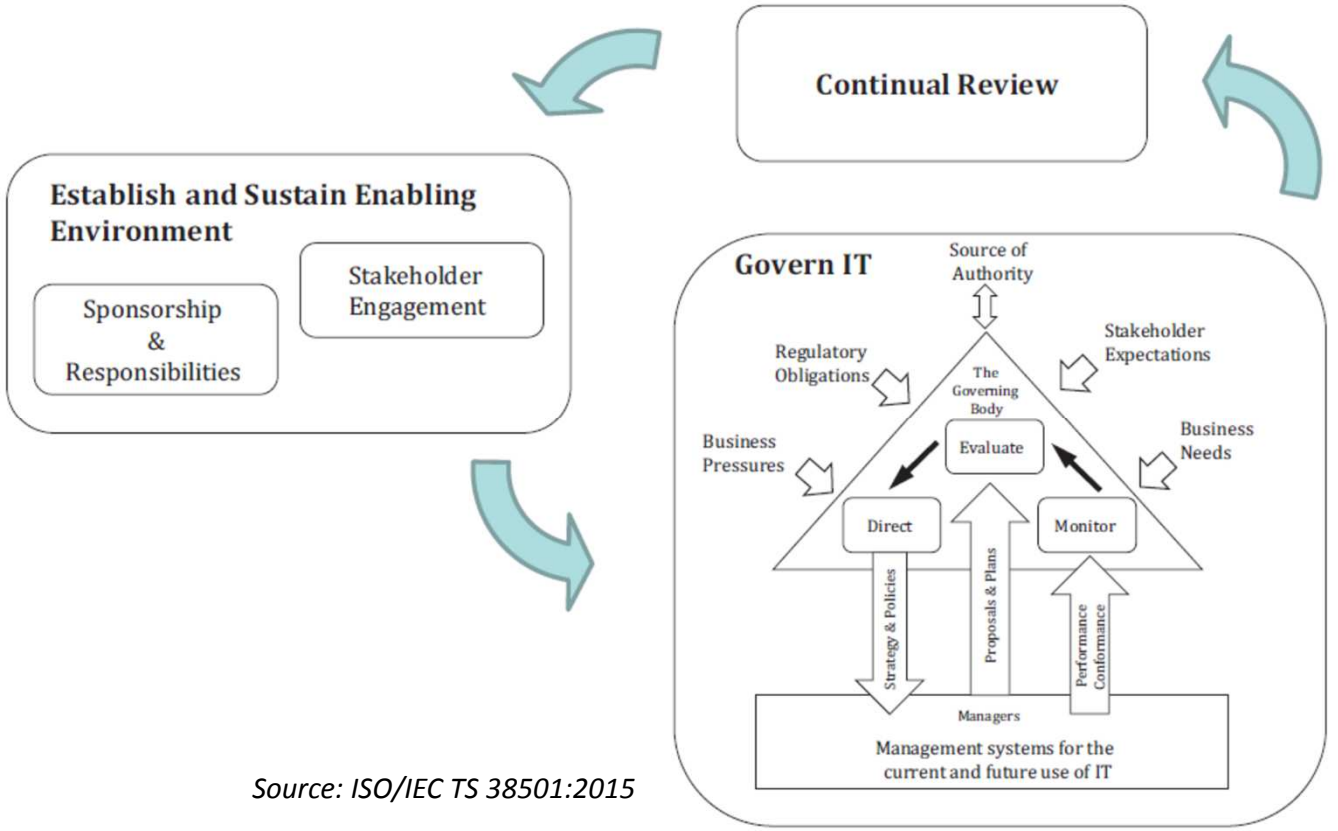
- Acceptable use of IT systems
- Use of IT for personal vs. professional purposes
- Interactions with interested parties: customers, suppliers, authorities, internal hierarchy

Model for governance of IT



Source: ISO/IEC 38500:2015

IT Governance implementation approach



Does it ring a bell?

Source: ISO/IEC TS 38501:2015

Establish and sustain enabling environment

- Ensure stakeholder engagement
  - Governing body
  - Executive managers
- Secure sponsorship and assign responsibilities:
  - awareness and education
  - coordination and administration activities

Govern IT

- Evaluate, direct and monitor
- Guided by the six principles
- Within the context of the internal and external environments, as well as organization's culture for the governance of IT

Govern IT in practice

Evaluate

- ❑ Understand internal environment
- ❑ Understand external environment
- ❑ Identify current state of the use of IT

Direct

- ❑ Define desired state for the use of IT
- ❑ Initiate change program
- ❑ Identify governance enabling mechanisms

Monitor

- ❑ Define evidence of success
- ❑ Establish monitoring system

What does it look like?

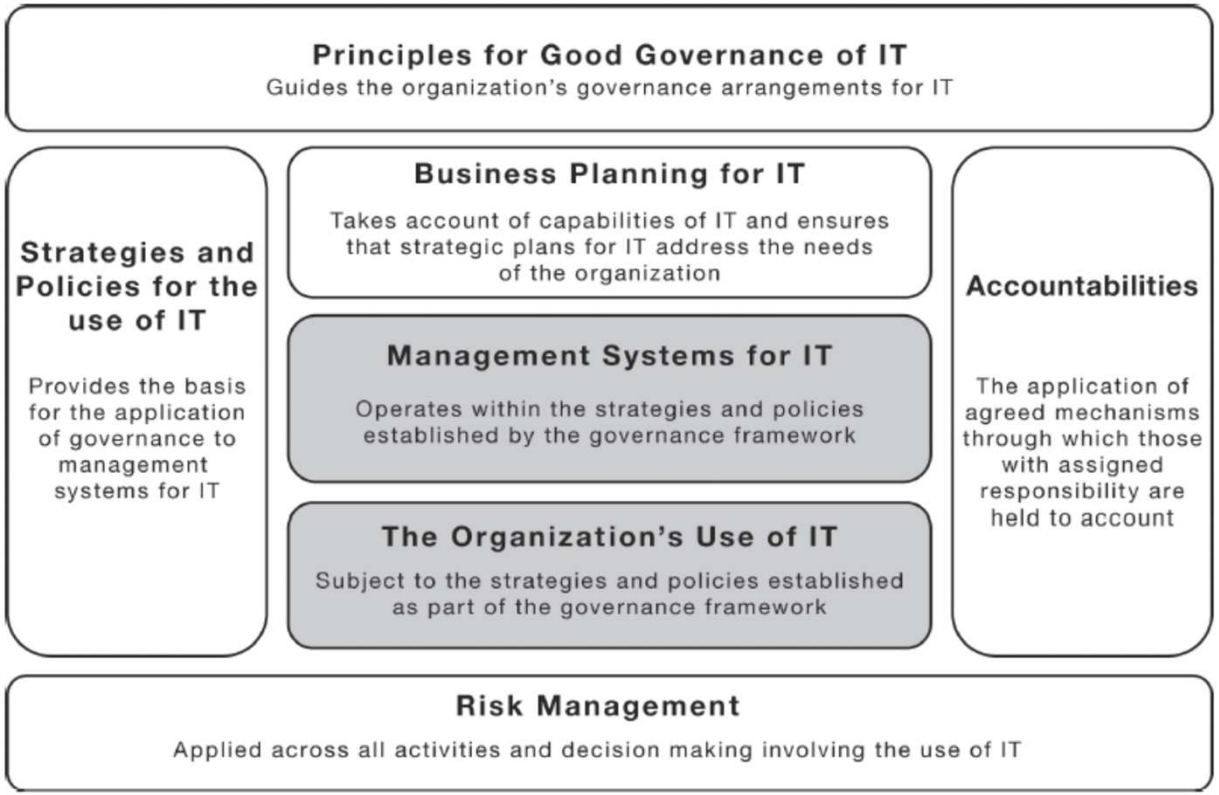
Continual review

- **Baseline for the governance of IT**
- Identify and assess opportunities for improvement
- Review the governance of IT implementation

A new iteration of the IT governance implementation cycle may be initiated

Governance vs. Management

***Management** is responsible for achieving organizational strategic objectives **within the strategies and policies for use of IT** set by the governing body*



Source: ISO/IEC TR 38502:2017


BREAK
TIME !!