Current approaches to **IT governance**

Models and frameworks

Lars Groth
Corporate Governance

- Based on "Principal-Agent Theory"
  - The relationship between shareholders and company management

- Govern responsibility in the relations between the various stakeholders:
  - Shareholders
  - Board of directors
  - Management
  - Auditors
  - Customers
  - Creditors
  - Regulatory bodies

- "Accountability"
  - Distribution of responsibility
  - Transparency
  - Documentation
Corporate negligence and regulatory failure was the root causes of the July 2013 Quebec train derailment and explosion, according to a study released by the Canadian Centre for Policy Alternatives (CCPA).
Graph these case-sensitive comma-separated phrases: IT governance

between 1980 and 2008 from the corpus English with smoothing of 3.
Most people point to Venkatraman:

- L. Loh og N. Venkatraman:
    The governance of an organizational information technology (IT) infrastructure is steadily shifting away from pure hierarchical and market mechanisms toward hybrid and partnership modes that involve external vendors. In particular, IT outsourcing has recently emerged as a significant administrative innovation in an organization’s IT strategy.

- J. C. Henderson og Venkatraman:
  - *Strategic alignment: Leveraging information technology for transforming organizations*, IBM Systems Journal, 1, 1993

Thus, we propose that the position of the organization in the I/T marketplace involves three sets of choices:

1. Information technology scope—those specific information technologies (for example, electronic imaging, local- and wide-area networks, expert systems, and robotics) that support current business strategy initiatives or could shape new business strategy initiatives for the firm. This is analogous to business scope, which deals with choices pertaining to product-market offerings in the output market.

2. Systemic competencies—those attributes of I/T strategy (for example, system reliability, cost-performance levels, interconnectivity, flexibility) that could contribute positively to the creation of new business strategies or better support of existing business strategy. This is analogous to the concept of business distinctive competencies, which deal with those attributes of strategy (pricing, quality, value-added service, superior distribution channels) that contribute to a distinctive, comparative advantage to a firm over its competitors.

3. I/T governance—selection and use of mechanisms (for example, joint ventures with vendors, strategic alliances, joint research and development for new I/T capabilities) for obtaining the required I/T competencies. This is analogous to business governance, which involves make-versus-buy choices in business strategy. Such choices cover a complex array of interfirm relationships such as strategic alliances, joint ventures, marketing exchange, and technology licensing.
Figure 4. Strategic Alignment Model

Organization and systems are interwoven
Complexity in the IT portfolio: DnB
Main systems of NAV (the Norwegian Labour and Welfare Administration) - and their dependencies
Figure 1-5. A combined overlay: the functioning of the organization
Organizations are woven together by system interconnections
Så hardt rammes din bransje av ny teknologi

Platform strategy

Competitive Advantage

Strategic Alignment

Experimentation and adaptivity

Co-evolution

IT governance

IT strategy
Some current trends for iT:

- From technology focus to business focus
- From IT-strategy to Co-evolution
- From IT management to IT Governance
- Professionalization and standardization of the management and governance of IT: From "rule of thumb" to a substantial number of "frameworks" at various levels of formalization
What is IT Governance?
Basically, IT governance is quite simple:

- It is about making sure that information technology provides the best possible support for the enterprise in delivering what it is there to deliver.

- Then it is about managing that technology in a prudent and professional way, just as any other asset class.

- “Good IT governance isn’t rocket science, but it requires discipline and commitment.”
  - Craig Symons, Forrester Research
Frameworks for governance

Partial or incidental
- ITIL
- Six Sigma
- CMM/CMMI
- IT Due Diligence
- IT Service CMM
- SOX (Sarbanes-Oxley)
- SAS70
- SysTrust
- IT Audit
- ISO / IEC 27002 (tidl. ISO 17799)
- PRINCE 2

Comprehensive
- COBIT
- ASL/BiSL
- IT Governance Review
- IT Governance Assessment
- IT Governance Checklist
- ITGAP (IT Governance Assessment Process) Model
- ISO 38500 IT Governance Standard
- Y-Model (Peculiar to Norwegian public administration)
Six Sigma
Six Standard Deviations from Mean

- General method for process improvement, developed by Motorola – widely used in industry
- Main focus on eliminating errors – a ”real” Six Sigma production process need to deliver 99,99966% error-free products. That translates into maximum 3,4 errors per million products.
- Has been extended over time to cover stability, predictability and customer focus (to deliver what the customer demands)
- Today often combined with Lean, a method (also originating from industry) for simplification and elimination of costs and planning time
- Comprises two project methods, one for improving existing processes and one for developing new ones
CMM / CMMI
Capability Maturity Model / Integration

- CMM: Originally developed as a tool for objectively assessing the ability of government contractors' processes to perform a contracted software project
  - Developed in the 1980s by Carnegie Mellon Software Engineering Institute for United States Department of Defense

- Around 2000 extended to the Capability Maturity Model Integration (CMMI) in order to handle the use of different models of software development in the same organization

Characteristics of the Maturity levels

- **Level 1: Initial**
  - Processes unpredictable, poorly controlled and reactive

- **Level 2: Managed**
  - Processes characterized for projects and is often reactive.

- **Level 3: Defined**
  - Processes characterized for the organization and is proactive.
    - Projects tailor their processes from organization’s standards

- **Level 4: Quantitatively Managed**
  - Processes measured and controlled

- **Level 5: Optimizing**
  - Focus on process improvement
IT Service CMM
IT Service Capability Maturity Model

- Developed through a research project partly supported by the Dutch government in the late 1990s
- A maturity model designed for IT service companies
- It has two objectives:
  1. To assess the maturity of suppliers of such services
  2. To provide guidelines for improvement of the suppliers’ processes for service delivery
- Is owned by Vrije Universiteit Amsterdam and CIBIT Academy
- Can be downloaded and freely used by anyone
SOX
Sarbanes-Oxley Act

- American law, also known as the “Public Company Accounting Reform and Investor Protection Act” (Senate) or "Corporate and Auditing Accountability and Responsibility Act“ (the House)

- Adopted in the wake of the scandals surrounding Enron, Worldcom og a number of other major American corporations

- Provides standards for governing and auditing for boards of directors, top management and auditors in corporations with many shareholders (typically large, publicly traded companies)

- Has consequences for IT through provisions for the storage of information:

  - All archives, including electronic documents and messages, must be kept for at least five years
SAS70
Statement on Auditing Standards No. 70, Service Organizations

- Standard for auditing developed by American Institute of Certified Public Accountants (AICPA), devised for service providers delivering services impacting the customers’ control obligations, such as:
  - Application service providers
  - Data centers
  - Financial transaction providers

- A tool for service auditors evaluating companies’ internal control procedures

- Companies must prove they have satisfactory control procedures and safety measures in order to take care of the customers’ data in an adequate way

- They are also required to organize their control activities in a way that allows their customers to identify which of their controls that cover the various part of their own financial reporting
SysTrust

- Developed in cooperation between American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA)
- A method for evaluating and testing reliability
- The test measures whether a system is reliable along three parameters:
  1. **Availability**: The system is available for operation and use at times set forth in service-level statements or agreements
  2. **Security**: The system is protected against unauthorized physical and logical access
  3. **Integrity**: System processing is complete, accurate, timely, and authorized
ISO/IEC 27002
(Previously ISO17799)

- “Information technology - Security techniques - Code of practice for information security management”
- Provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS)
- Information security is defined within the standard in the context of the C-I-A triad, namely the preservation of:
  - Confidentiality (ensuring that information is accessible only to those authorized to have access)
  - Integrity (safeguarding the accuracy and completeness of information and processing methods)
  - Availability (ensuring that authorized users have access to information and associated assets when required)
- Covers 12 main areas
PRINCE2
Projects IN Controlled Environments

- A project management methodology initially developed in 1989 by the Central Computer and Telecommunications Agency (CCTA) as a UK Government standard for IT project management (PRINCE).

- Revised in 1996 and released as a generic project management method (PRINCE2) and revised again in 2009 (PRINCE2:2009 Refresh) in order to integrate better with other Office of Government Commerce methodologies (like ITIL).

- Encompasses the high level management, control and organization of a project, but not lower level activities such as scheduling.

- In July 2013, ownership of the rights to PRINCE2 (as well as the other methodologies owned by the Office of Government Commerce) was transferred from HM Cabinet Office to AXELOS Ltd, a joint venture between the Cabinet Office and Capita plc.
Relevant Norwegian laws
- there are many!

- Generally, they fall into three classes:
  - Laws that apply to all enterprises, public and private
  - Laws applying to public enterprises and public administration only
  - Laws applying to specific sectors or industries

- The relevant provisions in these laws mainly regulate matters such as:
  - Information storage
  - Information safeguarding
  - Information access
  - Information use, incl. universal design
  - Public access to information
  - Copyright, intellectual property
Some examples:

- **Laws applying to all enterprises**
  - Act relating to the processing of personal data (Personopplysningsloven)
  - Act relating to copyright in literary, scientific and artistic works, etc. (Åndsverksloven)
  - Act relating to a prohibition against discrimination on the basis of disability (Diskriminerings- og tilgjengelighetsloven)

- **Laws applying to public enterprises and public administration**
  - Act relating to procedure in cases concerning the public administration (Forvaltningsloven), (especially §15)
  - Act relating to public access to documents in the public administration (Offentlighetsloven) (a new EU-directive is underway)
  - Act relating to Protective Security Services (Sikkerhetsloven)
  - Act relating to archives (Arkivloven) and Act relating to the legal deposit of generally available documents with regulations (Pliktavleveringsloven)
  - Act relating to public procurement (Lov om offentlige anskaffelser)
  - Regulations relating to ICT standards (Forskrift om IKT-standarder)
  - Local government act (Kommuneloven)

- **Sector laws**
  - Act relating to health personnel etc. (Helsepersonelloven)
  - Act relating to municipal health and care services etc. (Helse- og omsorgstjenesteloven)
  - Act on personal health data filing systems and the processing of personal health data (Helseregisterloven)
Y-modelen
(«The Y-model»)

Premise provider (governing role)

Purchaser
Supplier

NOT to be confused with:

Present: where are we now?
Wanted: where would we like to be?

What needs to change?

What are our options for change?

Plan: tasks and times to get us there?

As they have nothing whatsoever in common!
Michael Holm Larsen, Mogens Kühn Pedersen og Kim Viborg Andersen:

*IT Governance: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S*

Proceedings of the 39th Hawaii International Conference on System Sciences - 2006

---

<table>
<thead>
<tr>
<th><strong>Decision-Making Processes</strong></th>
<th><strong>Core Business Processes</strong></th>
<th><strong>Support Processes</strong></th>
<th><strong>Process Type / Organisational Entity</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• SAS70</td>
<td>• ITIL / BS15000</td>
<td>• ISO 17799 / BS7799</td>
<td>Procedure</td>
</tr>
<tr>
<td></td>
<td>• COBIT</td>
<td>• SysTrust</td>
<td>Activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASL</td>
<td>Business Unit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PRINCE2</td>
<td>Business System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Six Sigma</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT Service CMM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT Governance Review</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT Governance Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT Governance Assessment Checklist</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT Governance Assessment Process Model</td>
<td></td>
</tr>
</tbody>
</table>

---

**Table 1: Classification of IT Governance Tools.**
ASL/BiSL
Application Services Library/Business Information Services Library

- Open ("public domain") framework for the implementation of application management (ASL) and business information management (BiSL).
  - Developed in The Netherlands during the 1990s
  - Ties into ITIL for the management of infrastructure
  - Has much in common with ITIL (more at www.aslbislfoundation.org)
  - Three level models: Governance, Management and Operations

- ASL views the world from the IT function and divides it into two main parts:
  - Services
  - Applications

- BiSL views the world from the business side and focuses on:
  - Business strategy and business processes
  - Information needs and functional needs
  - Vendor management
  - Portfolio management
  - User support
ITGAP Model (IT Governance Assessment Process)

- Devised by Ryan Peterson in 2004 article in *Information Systems Management* (Fall 2004, pp. 7-22)
- More a method for assessing the effectiveness of a company’s IT governance architecture than for organizing it
- Devises a four-point roadmap for assessment:
  1. Describe and assess IT governance value drivers
  2. Describe and assess the differentiation of IT decision making authority for the portfolio of IT activities:
  3. Describe and assess the capabilities of IT governance:
  4. Describe and assess IT value realization
ISO 38500

- The purpose of the standard is to promote effective, efficient, and acceptable use of IT in all organizations by:
  - assuring stakeholders that, if the standard is followed, they can have confidence in the organization’s corporate governance of IT
  - informing and guiding directors in governing the use of IT in their organization, and
  - providing a basis for objective evaluation of the corporate governance of IT.

- The framework comprises definitions, principles and a model.

- It sets out six principles for good corporate governance of IT that express preferred behavior to guide decision making:
  1. responsibility
  2. strategy
  3. acquisition
  4. performance
  5. conformance
  6. human behavior
By far the leading tool for service management in IT

Defined as a separate standard within ISO / IEC, ISO 20 000

Initially developed in the 1980s by the British Government (Central Computer and Telecommunications Authority, CCTA), and specifically designed for systems delivery, operations, and support

CCTA was merged into the Office of Government Commerce i 2000

Version 2 launched in 2001

Revised extensively after consultations with a very large number of enterprises both in the private and public sector, v3 launched in 2011

Now shows ambitions (v3) to become a more general framework for managing the whole IT function
Main parts

- **ITIL Service Strategy:**
  - **understands organizational objectives and customer needs**

- **ITIL Service Design:**
  - **turns the service strategy into a plan for delivering the business objectives**

- **ITIL Service Transition:**
  - **develops and improves capabilities for introducing new services into supported environments**

- **ITIL Service Operation:**
  - **manages services in supported environments**

- **ITIL Continual Service Improvement:**
  - **achieves services incremental and large-scale improvements**
**COBIT**

Control Objectives for Information and Related Technology

- A framework developed by ISACA (Information Systems Audit and Control Association), which was founded in 1967
- First version launched in 1996, present version (5.0) published 2012
- In 1998, ISACA established *IT Governance Institute* to start research on governance
- ISACA offers certification in four areas, including governance:
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - **Certified in the Governance of Enterprise IT (CGEIT)**
  - Certified in Risk and Information Systems Control (CRISC)
COBIT 5: Now One Complete Business Framework

An business framework from ISACA, at www.isaca.org/cobit

© 2012 ISACA® All rights reserved.
Figure 25—COBIT 5 Coverage of Other Standards and Frameworks

Evaluate, Direct and Monitor
- ISO/IEC 38500

Align, Plan and Organise
- ISO/IEC 31000
- CMMI
- TOGAF
- PRINCE2/PMBOK

Build, Acquire and Implement
- ITIL V3 2011 and ISO/IEC 20000

Deliver, Service and Support

Monitor, Evaluate and Assess
COBIT®

A Business Framework for the Governance and Management of Enterprise IT
"Information is a key resource for all enterprises, and throughout the whole information life cycle there is a huge dependency on technology."

Information and related technologies are pervasive in enterprises and they need to be governed and managed in a holistic manner, taking in the full end-to-end business and IT functional areas of responsibility."

– CobiT5, Executive Summary
**Figure 4—COBIT 5 Goals Cascade Overview**

- **Stakeholder Drivers** (Environment, Technology Evolution, …)
  - Influence

- **Stakeholder Needs**
  - Benefits Realisation
  - Risk Optimisation
  - Resource Optimisation

- **Enterprise Goals**
  - Cascade to Appendix D
  - Figure 5

- **IT-related Goals**
  - Cascade to Appendix B
  - Figure 6

- **Enabler Goals**
  - Cascade to Appendix C
The difference between *governance* and *management*

- **Governance** ensures that stakeholders 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 (EDM).
- **Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).
<table>
<thead>
<tr>
<th>BSC Dimension</th>
<th>Enterprise Goal</th>
<th>Relation to Governance Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Benefits Realisation</td>
</tr>
<tr>
<td>Financial</td>
<td>1. Stakeholder value of business investments</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>2. Portfolio of competitive products and services</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>3. Managed business risk (safeguarding of assets)</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>4. Compliance with external laws and regulations</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>5. Financial transparency</td>
<td>P</td>
</tr>
<tr>
<td>Customer</td>
<td>6. Customer-oriented service culture</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>7. Business service continuity and availability</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>8. Agile responses to a changing business environment</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>9. Information-based strategic decision making</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>10. Optimisation of service delivery costs</td>
<td>P</td>
</tr>
<tr>
<td>Internal</td>
<td>11. Optimisation of business process functionality</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>12. Optimisation of business process costs</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>13. Managed business change programmes</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>14. Operational and staff productivity</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>15. Compliance with internal policies</td>
<td>P</td>
</tr>
<tr>
<td>Learning and Growth</td>
<td>16. Skilled and motivated people</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>17. Product and business innovation culture</td>
<td>P</td>
</tr>
<tr>
<td>IT BSC Dimension</td>
<td>Information and Related Technology Goal</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td>01 Alignment of IT and business strategy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 IT compliance and support for business compliance with external laws and regulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>03 Commitment of executive management for making IT-related decisions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>04 Managed IT-related business risk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>05 Realised benefits from IT-enabled investments and services portfolio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>06 Transparency of IT costs, benefits and risk</td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td>07 Delivery of IT services in line with business requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>08 Adequate use of applications, information and technology solutions</td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td>09 IT agility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 Security of information, processing infrastructure and applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11 Optimisation of IT assets, resources and capabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12 Enablement and support of business processes by integrating applications and technology into business processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14 Availability of reliable and useful information for decision making</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15 IT compliance with internal policies</td>
<td></td>
</tr>
<tr>
<td>Learning and Growth</td>
<td>16 Competent and motivated business and IT personnel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>17 Knowledge, expertise and initiatives for business innovation</td>
<td></td>
</tr>
</tbody>
</table>
Figure 23—Mapping COBIT 5 IT-related Goals to Processes (cont.)

<table>
<thead>
<tr>
<th>COBIT 5 Process</th>
<th>Financial</th>
<th>Customer</th>
<th>Internal</th>
<th>Learning and Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA01 Manage Programmes and Projects</td>
<td>P S S P</td>
<td></td>
<td></td>
<td>S S</td>
</tr>
<tr>
<td>EA02 Manage Requirements Definition</td>
<td>P S S S</td>
<td>P</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>EA03 Manage Solutions Identification and Build</td>
<td></td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EA04 Manage Availability and Capacity</td>
<td></td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EA05 Manage Organisational Change Enablers</td>
<td></td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EA06 Manage Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA07 Manage Change Acceptance and Transitioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA08 Manage Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA09 Manage Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA10 Manage Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS01 Manage Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS02 Manage Service Requests and Incidents</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS03 Manage Problems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS04 Manage Continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS05 Manage Security Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS06 Manage Business Process Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEA01 Monitor, Evaluate and Assess Performance and Conformance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEA02 Monitor, Evaluate and Assess the System of Internal Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEA03 Monitor, Evaluate and Assess Compliance With External Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IT governance

Lars Groth
<table>
<thead>
<tr>
<th>Internal Stakeholders</th>
<th>Internal Stakeholder Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board</td>
<td>How do I get value from the use of IT? Are end users satisfied with the quality of the IT service?</td>
</tr>
<tr>
<td>Chief executive officer (CEO)</td>
<td>How do I manage performance of IT?</td>
</tr>
<tr>
<td>Chief financial officer (CFO)</td>
<td>How can I best exploit new technology for new strategic opportunities?</td>
</tr>
<tr>
<td>Chief information officer (CIO)</td>
<td>How do I build and structure my IT department?</td>
</tr>
<tr>
<td>Chief risk officer (CRO)</td>
<td>How dependent am I on external providers? How well are IT outsourcing agreements being managed?</td>
</tr>
<tr>
<td>Business executives</td>
<td>How do I obtain assurance over external providers?</td>
</tr>
<tr>
<td>Business process owners</td>
<td>What are the (control) requirements for information?</td>
</tr>
<tr>
<td>Business managers</td>
<td>Did I address all IT-related risk?</td>
</tr>
<tr>
<td>Risk managers</td>
<td>Am I running an efficient and resilient IT operation?</td>
</tr>
<tr>
<td>Security managers</td>
<td>How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner?</td>
</tr>
<tr>
<td>Service managers</td>
<td>What are the most effective and efficient sourcing options?</td>
</tr>
<tr>
<td>Human resource (HR) managers</td>
<td>Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance?</td>
</tr>
<tr>
<td>Internal audit</td>
<td>How do I get assurance over IT?</td>
</tr>
<tr>
<td>Privacy officers</td>
<td>Is the information I am processing well secured?</td>
</tr>
<tr>
<td>IT users</td>
<td>How do I improve business agility through a more flexible IT environment?</td>
</tr>
<tr>
<td>IT managers</td>
<td>Do IT projects fail to deliver what they promised—and if so, why? Is IT standing in the way of executing the business strategy?</td>
</tr>
<tr>
<td>Etc.</td>
<td>How critical is IT to sustaining the enterprise? What do I do if IT is not available?</td>
</tr>
<tr>
<td></td>
<td>What critical business processes are dependent on IT, and what are the requirements of business processes?</td>
</tr>
<tr>
<td></td>
<td>What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget?</td>
</tr>
<tr>
<td></td>
<td>How much of the IT effort goes to fighting fires rather than to enabling business improvements?</td>
</tr>
<tr>
<td></td>
<td>Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?</td>
</tr>
<tr>
<td></td>
<td>How long does it take to make major IT decisions?</td>
</tr>
<tr>
<td></td>
<td>Are the total IT effort and investments transparent?</td>
</tr>
<tr>
<td></td>
<td>Does IT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External Stakeholders</th>
<th>External Stakeholder Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business partners</td>
<td>How do I know my business partner’s operations are secure and reliable?</td>
</tr>
<tr>
<td>Suppliers</td>
<td>How do I know the enterprise is compliant with applicable rules and regulations?</td>
</tr>
<tr>
<td>Shareholders</td>
<td>How do I know the enterprise is maintaining an effective system of internal control?</td>
</tr>
<tr>
<td>Regulators/government</td>
<td>Do business partners have the information chain between them under control?</td>
</tr>
<tr>
<td>External users</td>
<td></td>
</tr>
<tr>
<td>Customers</td>
<td></td>
</tr>
<tr>
<td>Standardisation organisations</td>
<td></td>
</tr>
<tr>
<td>External auditors</td>
<td></td>
</tr>
<tr>
<td>Consultants</td>
<td></td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
</tr>
</tbody>
</table>
Comprehensive

- COBIT
- ASL/BiSL
- IT Governance Review
- IT Governance Assessment
- IT Governance Checklist
- ITGAP (IT Governance Assessment Process) Model
- ISO 38500 IT Governance Standard
This book draws on a considerable number of studies at CISR

*(Center for Information Systems Research ved MIT Sloan School of Management)*

- A study from 2001-2003 of 256 enterprises from North and South America, Asia and Europe
- 40 case studies from USA and Europe from 1999 to 2003
- One study of 30 IT managers from 2001
- An exploratory study of IT governance from 1998-99
- An examination of IT governance arrangements in 24 Fortune 100 firms in 2000
"We conclude that effective IT governance is the single most important predictor of the value an organization generates from IT."

Weill and Ross 2004, p. 3-4

"The best predictor of IT governance performance is the percentage of managers in leadership positions who can accurately describe IT governance."

Weill and Ross 2004, p. 13

*IT Governance* – How Top Performers Manage IT Decision Rights for Superior Results
Governance of IT:

- "Specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT"

- To govern is to determine who decides what. Three questions must be addressed:

  1. **What** decisions must be made to ensure effective management and use of IT?
  2. **Who** should make these decisions?
  3. **How** will these decisions be made and monitored?

- The authors assert that the research presented in the book shows that the enterprises with the best technology utilization achieves up to 40% better return on their IT investments than their competitors
IT: One of the six key assets

Corporate and Key Asset Governance

Corporate governance
- Shareholders
- Other stakeholders
- Monitoring
- Disclosure

Senior executive team
- Strategy
- Desirable behavior

Key assets
- Human assets
- Financial assets
- Physical assets
- IP assets
- Information and IT assets
- Relationship assets

Financial governance mechanisms (committees, budgets, etc.)

IT governance mechanisms (committees, budgets, etc.)

Key asset governance

IT governance.
What decisions must be made?

1. IT principles
   - What is the enterprise’s desired operating model?
   - How will IT support it?
   - How will IT be funded?

2. IT architecture
   - What are the needs for integration and standardization – and can they be fulfilled?

3. IT infrastructure
   - What is going to be included in the shared platforms and services?
     - Hardware and system software
     - IT skills and knowledge
     - Shared services like network and shared databases
     - Shared applications

4. Business application needs
   - What is needed, what to buy and what to develop? Particularly important when:
     - Application needs challenge the established architecture
     - Parallel projects with overlapping specifications results in solutions that do not work together, or parallel storage of data

5. Investment and prioritization
   - How much to spend, what to spend it on, who pays, and how to reconcile the needs of the different IT constituencies
What decisions must be made?

**FIGURE 2-3**

IT Infrastructure as a Centrally Coordinated Set of Shared and Reliable Services

- Local applications
- Shared and standard IT applications
- Shared information technology services
- Human information technology infrastructure
- Information technology components

Fast-changing local business applications such as insurance claim processing, Web bank loan applications, customer complaints support system, phone order support systems

Shared and standard applications that change less regularly, such as accounting, budgeting, human resource management

Services that are stable over time, such as management of shared customer databases, PC/LAN access

Human infrastructure of knowledge, skills, policies, standards, and experience binds components

Commodities such as computers, printers, routers, database software, operating systems, credit card swipers

Who will make the decisions?

<table>
<thead>
<tr>
<th>Decisionmakers</th>
<th>Configuration name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top management</td>
<td>Business Monarchy</td>
</tr>
<tr>
<td>IT management</td>
<td>IT Monarchy</td>
</tr>
<tr>
<td>Any strong manager with an agenda</td>
<td>Feudal</td>
</tr>
<tr>
<td>Most or all department or division managers</td>
<td>Federal</td>
</tr>
<tr>
<td>Top management and IT management in concert</td>
<td>Duopoly</td>
</tr>
<tr>
<td>Any and all</td>
<td>Anarchy</td>
</tr>
<tr>
<td>?</td>
<td>Don’t Know</td>
</tr>
</tbody>
</table>
# The governance matrix

(Complete)

<table>
<thead>
<tr>
<th></th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure Strategies</th>
<th>Business Application Needs</th>
<th>IT Investments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Decision</td>
<td>Input</td>
<td>Decision</td>
<td>Input</td>
<td>Decision</td>
</tr>
<tr>
<td>Business Monarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Monarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feudal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duopoly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Most common arrangements

### Percent per decision type for 256 enterprises from 23 countries

<table>
<thead>
<tr>
<th></th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure Strategies</th>
<th>Business Application Needs</th>
<th>IT Investments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Input</td>
<td>Decision</td>
<td>Input</td>
<td>Decision</td>
<td>Input</td>
</tr>
<tr>
<td>Business Monarchy</td>
<td>0</td>
<td>27</td>
<td>0</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>IT Monarchy</td>
<td>1</td>
<td>18</td>
<td>20</td>
<td>73</td>
<td>10</td>
</tr>
<tr>
<td>Feudal</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Federal</td>
<td>83</td>
<td>14</td>
<td>46</td>
<td>4</td>
<td>59</td>
</tr>
<tr>
<td>Duopoly</td>
<td>15</td>
<td>36</td>
<td>34</td>
<td>15</td>
<td>30</td>
</tr>
<tr>
<td>Anarchy</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Fat red numbers:** Most common arrangements for information input

**Fat black numbers:** Most common arrangements for decisions
## Governance arrangements:
The best and worst performers

*Percent per decision type*

<table>
<thead>
<tr>
<th>Governance安排</th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure Strategies</th>
<th>Business Application Needs</th>
<th>IT Investments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Input</td>
<td>Decision</td>
<td>Input</td>
<td>Decision</td>
<td>Input</td>
</tr>
<tr>
<td>Business Monarchy</td>
<td>0</td>
<td>27</td>
<td>0</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>IT Monarchy</td>
<td>1</td>
<td>18</td>
<td>20</td>
<td>73</td>
<td>10</td>
</tr>
<tr>
<td>Feudal</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Federal</td>
<td>83</td>
<td>14</td>
<td>46</td>
<td>4</td>
<td>59</td>
</tr>
<tr>
<td>Duopoly</td>
<td>15</td>
<td>36</td>
<td>34</td>
<td>15</td>
<td>30</td>
</tr>
<tr>
<td>Anarchy</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
**FIGURE 5-5**

**Top Three Governance Performers**

<table>
<thead>
<tr>
<th>Archetype</th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure Strategies</th>
<th>Business Application Needs</th>
<th>IT Investment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Monarchy</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td></td>
<td>2, 3</td>
</tr>
<tr>
<td>IT Monarchy</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Feudal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duopoly</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Anarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1, 2, 3 = Top three governance performers (achieving four performance objectives, weighted by importance).

© 2003 MIT Sloan School Center for Information Systems Research (CISR). Used with permission.
Seven characteristics of top governance performers

1. More managers in leadership positions could describe IT governance
2. Greater engagement and knowledge on the part of senior management
3. More direct involvement of the senior leaders in IT governance
4. Clearer business objectives for IT investment
5. More differentiated business strategies
6. Fewer renegade and more formally approved exceptions
7. Fewer changes in governance
Symptoms of ineffective governance

- Senior management senses low value from IT investments
- IT is often a barrier to implementing new strategies
- The mechanisms to make IT decisions are slow or contradictory
- Senior management cannot explain IT governance
- Projects often run late and over budget
- Senior management sees outsourcing as a quick fix to IT problems
- Governance changes frequently
What will work best?

- The arrangements that suites YOU!
- IT should contribute as much as possible to the realization of enterprise goals....
- ....in a cost effective way.
Knowledge and cooperation