Current approaches to *IT governance*

Models and frameworks

Lars Groth
Corporate negligence and regulatory failure was the root causes of the July Quebec train derailment and explosion, according to a study released by the Canadian Centre for Policy Alternatives (CCPA).
Risk Society

1984: Perrow:
Normal Accident Theory
Three Mile Island nuclear accident

“Dealing with hazards and insecurities induced and introduced by modern society itself”
Responses to ”Risk Society”

- **Societal level**
  - Increased readiness
  - Increased monitoring and surveillance

- **Business and finance level**
  - Laws and regulations, like
    - Sarbanes-Oxley
    - Basel II og III
  - Manuals for «Good governance», like
    - OECD Principles of Corporate Governance (comprehensive)
    - Statement on Auditing Standards 70 (SAS70) by the American Institute of Certified Public Accountants (financial)

- **The enterprise response**
  - Corporate governance
  - Focus on compliance with laws, regulations and important frameworks
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

"Miss Wilcox, send in someone to blame."
Some current trends for IT:

- From technology focus to business focus
- From IT management to IT Governance
- From IT-strategy to "Agility" and "Enterprise Architecture"
- Professionalization and standardization of the management of IT: From "rule of thumb" to a substantial number of "frameworks" at various levels of formalization
What is IT Governance?
Graph these case-sensitive comma-separated phrases: **IT governance**

between **1980** and **2008** from the corpus **English** with smoothing of **3**.
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.
First traces in 1962 og 63

- Ph. M. Thurston: "Who Should Control Information Systems?"

- J. T. Garrity: "Top Management and Computer Profits"
Garrity asks:

- Are applications selected on the basis of a careful feasibility study?
- Are project plans developed and progress reports prepared?
- Are plans and controls as effective as those applied to similar functions?
- Are completed projects appraised?
- Does top management devote time to the computer systems effort in proportion to its cost and potential?
- Does top management review plans and follow up on computer systems results?
- How many levels below the chief executive is the computer executive?
What he is after is:

- Who is responsible for IT-investments?
- Who obtains the information needed to decide on IT-investments?
- What kind of mechanisms are used to control the implementation of IT investment plans?

- and this actually comes quite close to the central questions in modern frameworks for IT governance.
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.
1992
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.

1993

"Thus, we propose that the position of the organization in the IT marketplace involves three sets of choices:

1. Information technology scope
2. Systemic competencies
3. **IT governance** – selection and use of mechanisms (for example, joint ventures with vendors, strategic alliances, joint research and development for new IT capabilities) for obtaining the required IT competencies. This is analogous to business governance, which involves make-versus-buy choices in business strategy."
Lars Groth
INF5890
IT governance
2014
Platform strategy
Strategic Alignment
Co-evolution
Competitive Advantage
Architecture
Experimentation and adaptivity
Co-evolution
Experimentation and adaptivity
Strategic Alignment
Competitive Advantage
Architecture
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
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

![Figure 7. Emerging IT Governance Paradigm](image-url)
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
ITIL
Information Technology Infrastructure Library

- 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 in 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
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
Six Sigma
Six Standard Deviations from Mean

- **DMAIC** (existing processes):
  - Define the problem
  - Measure key aspects of the current process
  - Analyze the data, seek out root cause of the defect under investigation.
  - Improve or optimize the current process based upon data analysis
  - Control the future state process to ensure that any deviations from target are corrected before they result in defects

- **DMADV** (new processes or products, also known as DFSS):
  - Define design goals that are consistent with customer demands and the enterprise strategy.
  - Measure and identify CTQs (characteristics that are Critical To Quality), product capabilities, production process capability, and risks
  - Analyze to develop and design alternatives
  - Design details, optimize the design, and plan for design verification
  - Verify the design, set up pilot runs, implement the production process and hand it over to the process owner(s)
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

- Mainly a method for assessing organizational maturity for software development

- Is nonetheless used also for evaluating maturity in IT/IS-related processes in general

- Has five levels of maturity
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

---

32
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 and 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.
PRINCE2
Projects IN Controlled Environments

PRINCE2 is a process-driven project management method, based on seven processes:

1. Starting up a project
2. Initiating a project
3. Directing a project
4. Controlling a stage
5. Managing stage boundaries
6. Managing product delivery
7. Closing a project
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)
Table 1: Classification of IT Governance Tools.

<table>
<thead>
<tr>
<th>Decision-Making Processes</th>
<th>Core Business Processes</th>
<th>Support Processes</th>
<th>Process Type / Organisational Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SAS70</td>
<td>• ITIL / BS15000</td>
<td>• ISO 17799 / BS7799</td>
<td>Procedure</td>
</tr>
<tr>
<td>• COBIT</td>
<td>• CMM / CMMI</td>
<td>• ASL</td>
<td>Activity</td>
</tr>
<tr>
<td></td>
<td>• IT Audut</td>
<td>• PRINCE2</td>
<td>Business Unit</td>
</tr>
<tr>
<td></td>
<td>• IT Due Diligence</td>
<td></td>
<td>Business System</td>
</tr>
</tbody>
</table>

- IT Governance Review
- IT Governance Assessment
- IT Governance Checklist
- IT Governance Assessment Process Model
- IT Service CMM
- SOX

Proceedings of the 39th Hawaii International Conference on System Sciences - 2006
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)
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
- PRINCE2/PMBOK
- TOGAF
- ISO/IEC 31000
- ISO/IEC 27000

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

Deliver, Service and Support

Monitor, Evaluate and Assess
- CMMI
“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

Cascade to Appendix D

Enterprise Goals

Cascade to Appendix B

IT-related Goals

Cascade to Appendix C

Enabler Goals

Cascade to Figure 5

Cascade to Figure 6
<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><strong>Financial</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01</td>
<td>Alignment of IT and business strategy</td>
<td></td>
</tr>
<tr>
<td>02</td>
<td>IT compliance and support for business compliance with external laws and regulations</td>
<td></td>
</tr>
<tr>
<td>03</td>
<td>Commitment of executive management for making IT-related decisions</td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>Managed IT-related business risk</td>
<td></td>
</tr>
<tr>
<td>05</td>
<td>Realised benefits from IT-enabled investments and services portfolio</td>
<td></td>
</tr>
<tr>
<td>06</td>
<td>Transparency of IT costs, benefits and risk</td>
<td></td>
</tr>
<tr>
<td><strong>Customer</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07</td>
<td>Delivery of IT services in line with business requirements</td>
<td></td>
</tr>
<tr>
<td>08</td>
<td>Adequate use of applications, information and technology solutions</td>
<td></td>
</tr>
<tr>
<td><strong>Internal</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09</td>
<td>IT agility</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Security of information, processing infrastructure and applications</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Optimisation of IT assets, resources and capabilities</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Enablement and support of business processes by integrating applications and technology into business processes</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Availability of reliable and useful information for decision making</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>IT compliance with internal policies</td>
<td></td>
</tr>
<tr>
<td><strong>Learning and Growth</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Competent and motivated business and IT personnel</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>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</td>
<td>S</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>EA02 Manage Requirements Definition</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EA03 Manage Solutions Identification and Build</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>EA04 Manage Availability and Capacity</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>EA05 Manage Organisational Change Enablement</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>EA06 Manage Changes</td>
<td>G</td>
<td>P</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>EA07 Manage Change Acceptance and Transitioning</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>EA08 Manage Knowledge</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EA09 Manage Assets</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>EA10 Manage Configuration</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>DSS01 Manage Operations</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>DSS02 Manage Service Requests and Incidents</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>DSS03 Manage Problems</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>DSS04 Manage Continuity</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>DSS05 Manage Security Services</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>DSS06 Manage Business Process Controls</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>MEA01 Monitor, Evaluate and Assess Performance and Conformance</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>MEA02 Monitor, Evaluate and Assess the System of Internal Control</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>MEA03 Monitor, Evaluate and Assess Compliance With External Requirements</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Internal Stakeholders</td>
<td>Internal Stakeholder Questions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief executive officer (CEO)</td>
<td>How do I manage performance of IT?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief financial officer (CFO)</td>
<td>How can I best exploit new technology for new strategic opportunities?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief information officer (CIO)</td>
<td>How do I build and structure my IT department?</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business executives</td>
<td>How do I obtain assurance over external providers?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business process owners</td>
<td>What are the (control) requirements for information?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business managers</td>
<td>Did I address all IT-related risk?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk managers</td>
<td>Am I running an efficient and resilient IT operation?</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service managers</td>
<td>What are the most effective and efficient sourcing options?</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal audit</td>
<td>How do I get assurance over IT?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy officers</td>
<td>Is the information I am processing well secured?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT users</td>
<td>How do I improve business agility through a more flexible IT environment?</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></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>
COBIT5: Enabling a Holistic Approach

Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.
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).
2. Covering the Enterprise End-to-end

- COBIT 5 addresses the governance and management of information and related technology from an enterprisewide, end-to-end perspective.

- This means that COBIT 5:
  - Integrates governance of enterprise IT into enterprise governance.
  - That is, the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system. COBIT 5 aligns with the latest views on governance.