6.CobIT

2005

CobIT – Control Objectives for Information and related Technology

- The IT Governance Institute was formed by the Information System Audit and Control Association (ISACA).
- CobIT Control Objectives for Information and related Technology was originally released as an IT process and control framework linking IT to business requirements.
- It was initially used mainly by the assurance community in conjunction with business and IT process owners.
- Beginning with the addition of Management Guidelines in 1998, CobIT is now being used more and more as a framework for IT governance, providing management tools such as metrics and maturity models to complement the control framework.

2

The CobIT Mission:

- To research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals.

3

Editions of CobIT

- CobIT represents a collection of documents which can be classified as generally accepted best practice for IT governance, control and assurance.
- The first edition of CobIT was issued by the Information Systems Audit and Control Foundation (ISACF) in 1996.
  - In 1998 the second edition was published with additional control objectives and the Implementation Tool Set.
  - The third edition currently available was issued by the IT Governance Institute in 2000, and added the Management Guidelines, as well as several other detailed control objectives.

4

CobIT - “parim praktika”

- CobIT-i kokkupanemisel on lähtutud väga laiast ringist erinevatest, IT valdkonna juhtimist mõjutada võivatest, standarditest, mistõttu väljend “parim praktika” (*“best practice”*) on CobIT-i iseloomustamiseks igati kohane.

5

CobIT-i tooteperekond

Kolmandas redaktsioonis koosneb CobIT kuuest väljaandest, mis üheskoos moodustavadki CobIT-i tooteperekonna:

- Annotatsioon (*Executive Summary*) annab standardist ülevaate, tutvustab kasutajale olulisi mõisteid ning CobIT-i ülesehitust;
- Raamstruktuur (*Framework*) kirjeldab ülevaatlikult CobIT-i struktuuri – neli valdkonda, mis jagunevad 34-ks IT põhiprotsessiks ehk – juhtkonna seisukohalt – juhtimisülesandeks (*control objective*). Iga juhtimisülesande aluseks on ärinõue, kõik nõuded seostatakse IT ressurssi vajadusega;

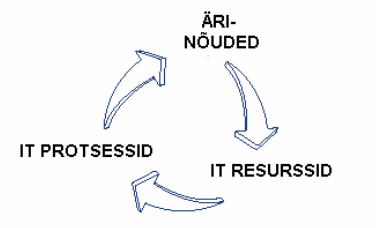
6

CobIT-i tooteperekond

- Juhtimiseesmärgid (*Control Objectives*) detailiseerivad veelgi 34 põhiprotsessi, defineerides ja sõnastades kasutajale 318 alamprotsessi, mis kohaselt juhituna peavad tagama soovitud eesmärgi – ärinõude tagamine – saavutamise.
- Auditi suunised (*Audit Guidelines*) kirjeldavad ülevaatlikult auditi läbiviimise protsessi ning esitavad põhjalikke praktilisi juhiseid IT protsessidega kaasnevate riskide avastamiseks, tõestamiseks ning hindamiseks.
- Rakendusjuhised (*Implementation Tool Set*) sisaldavad erinevaid teste juhtkonna teadlikkuse ning IT kontrollikeskkonna hindamiseks, üksikasjalikke suuniseid CobIT-i esmaseks tutvustamiseks ja rakendamiseks organisatsioonis, samuti lahendusi enimlevinud probleemidele standardi rakendamisel.
- Juhtimissuunised (*Management Guidelines*) on varustatud hindamismudeliga, kriitiliste edufaktoritega ning indikaatoritega eesmärgi saavutamise ja sooituse hindamiseks.

7

CobIT-i raamstruktuur



8

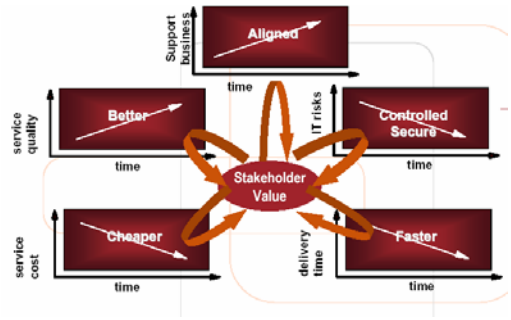
Finantsinspektsiooni soovituslik juhend – **Nõuded infotehnoloogia ala korraldamiseks**

- Soovituslik juhend on kehtestatud Finantsinspektsiooni juhatuse 22.09.2004 otsusega nr. 44-4
- Käesoleva juhendi koostamisel on võetud aluseks rahvusvaheliselt üldtunnustatud infotehnoloogia auditi ja juhtimise standardis CobIT (Control Objectives for information and Related Technology) ning selle lühivariandis CobIT Quickstart toodud juhtimiseesmärgid.
- CobIT-i juhtimiseesmärke on täiendatud ja täpsustatud infotehnoloogiat käsitlevates standardites (BS:7799, EVS- ISO/IEC 2382) sisalduvate nõuete ja definitsioonidega.

9

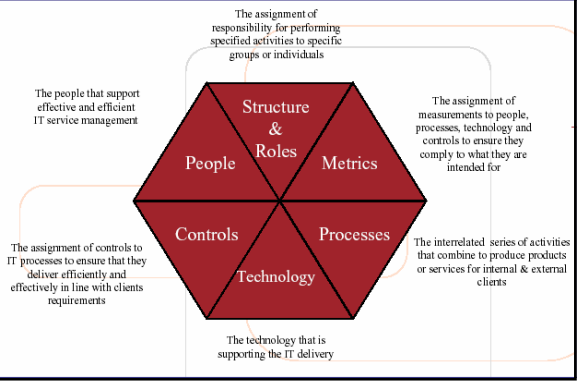
Achieving IT Goals

What do achieve with IT?

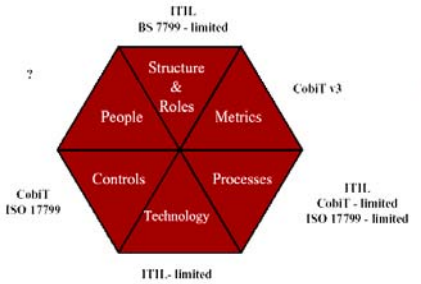


11

How to achieve IT goals?



How can we achieve IT goals?



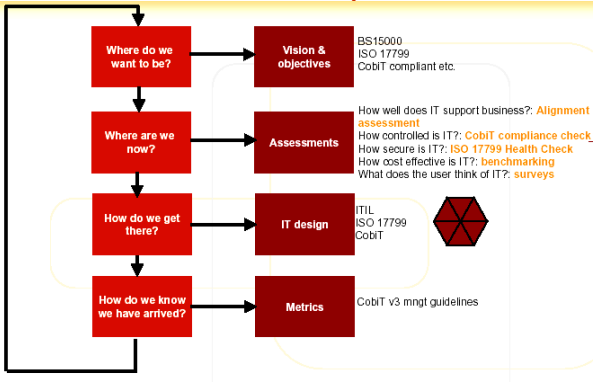
13

Where are the methods strong?

- ITIL strong in IT processes, but limited in security and system development
- CobiT strong in IT controls and IT metrics, but does not say how (i.e. process flows) and not that strong in security
- ISO 17799 strong in security controls, but does not say how (i.e. process flows)
- Conclusion:
  - No contradictions or real overlaps
  - None identify people requirements
  - Not strong on organisational side (structure & roles)
  - Not strong on technology side

14

Continious IT improvement



Ärieesmärkide saavutamine

Ärieesmärkide saavutamiseks peab informatsioon vastama järgmistele nõuetele:

- **turbenõuded**, mis jagunevad klassikaliselt nõueteks
  - konfidentsiaalsusele
  - terviklikkusele
  - käideldavusele
- **usaldusnõuded**, mille all mõistetakse
  - vastavust välisnõuetele (seadustele, lepingutele jmt)
  - usaldusväärsust ja piisavust juhtimisotsuste tegemiseks
- **kvaliteedinõuded**, mis jagunevad
  - toimivuseks – informatsioon on tõene/ kasutuskõlblik
  - tõhususeks – informatsiooni töötlemisel kasutatakse ressursse optimaalselt

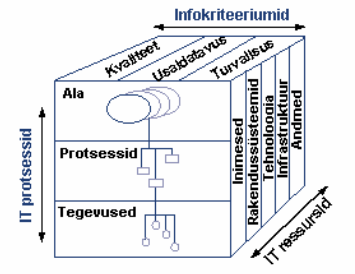
16

IT ressursid

- **andmed**
- **rakendussüsteemid**, mille all mõistetakse tarkvaralisi süsteeme
- **tehnoloogia**, mille all mõistetakse riistvara ja operatsioonisüsteeme
- **üldinfrastruktuur**, mis hõlmab endas ruume ja muid seadmeid, mis on vajalikud inforessursside majutamiseks ja toetamiseks
- **inimesed**, mille all mõistetakse personali oskusi, teadlikkust ja tööviljakust infoteenuse pakkumisel

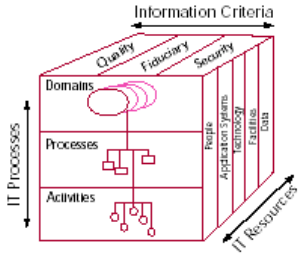
17

CobIT-i kuup



18

CobIT Cube



19

Informatsioonile esitatavate nõuete tagamine

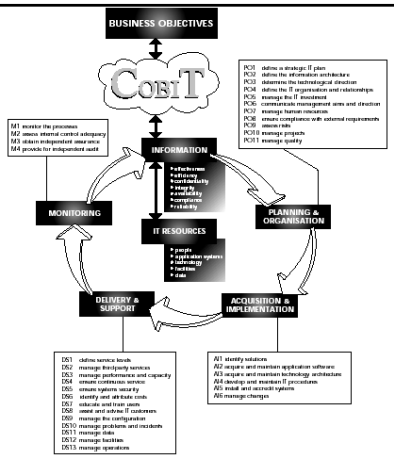
- Informatsioonile esitatavate nõuete tagamiseks tuleb kehtestada piisavad kontrollimeetmed, mis saavutatakse omavahel seotud IT protsesside kohase läbiviimise ning seirega.
- CobIT kehtestabki vastava struktuuri, koondades vajaliku tulemuse saavutamiseks teostatavad tegevustest protsessideks (tegevuste jadad, millel on määratletav algus ja lõpp) ning grupeerides protsessid aladeks.
- Organisatsioonides kujunevad aladest tihtipeale erinevate üksuste vastutusalad.

20

Mõju kolm taset

- Kõik protsessid ei avalda samasugust mõju informatsiooni kriteeriumitele. CobIT käsitlebki nimetatud mõju kolmel tasemel, tähistades need:
  - **primaarne**, mis tähendab, et protsessil on otsene mõju infokriteeriumile,
  - **sekundaarne**, mis näitab protsessi piiratud või kaudset mõju infokriteeriumile ja
  - **tühi**, mis näitab olulise mõju puudumist, kriteeriumile avaldavad mõju pigem teised protsessid.

21



CobIT IT Processes defined within the four domains

22

CobIT IT Processes

PLANNING AND ORGANISATION

PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Organisation and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage Human Resources
PO8	Ensure Compliance with External Requirements
PO9	Assess Risks
PO10	Manage Projects
PO11	Manage Quality

ACQUISITION AND IMPLEMENTATION

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Develop and Maintain Procedures
AI5	Install and Accredit Systems
AI6	Manage Changes

DELIVERY AND SUPPORT

DS1	Define and Manage Service Levels
DS2	Manage Third-Party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Assist and Advise Customers
DS9	Manage the Configuration
DS10	Manage Problems and Incidents
DS11	Manage Data
DS12	Manage Facilities
DS13	Manage Operations

MONITORING

M1	Monitor the Processes
M2	Assess Internal Control Adequacy
M3	Obtain Independent Assurance
M4	Provide for Independent Audit

23

Juhtimiseesmärkide jaotus ja käsitlemine

CobIT jagab IT protsessid neljaks laiemaks tegevusvaldkonnaks ehk alaks:

- plaanimine ja organisatsioon (*planning and organisation, PO*)
- hankimine ja evitamine (*acquisition and implementation, AI*)
- tarnimine ja tugi (*delivery and support, DS*)
- seire (*monitoring*)

24

Plaanimine ja organisatsioon

- Plaanimine ja organisatsioon keskendub strateegia ja taktika väljatöötamisele ning teavitamisele, riskide hindamisele ja projektijuhtimisele, otsides lahendusi, mis kõige paremini aitavad saavutada ärieesmärke.
- Pealegi on kohase organisatsiooni ülesehitamine sama oluline nagu korraliku infrastruktuuri loomine.

25

Hankimine ja evitamine

- Hankimine ja evitamine keskendub protsessidele, mille toel luuakse või ostetakse sisse uusi lahendusi, viiakse sisse muudatusi.
- Peamised kriteeriumid, mida ärinõuded informatsioonile nendes protsessides seavad, on toimivus ja tõhusus.

26

Tarnimine ja tugi

- Tarnimine ja tugi koondab endasse protsesse, mis on IT lahenduste rakendamise ning ekspluatatsiooniga.
- Oluline roll siinjuures on süsteemide talitluspidevuse ja turvalisuse tagamisel, aga ka kasutajate koolitamisel, probleemihaldusel jmt.

27

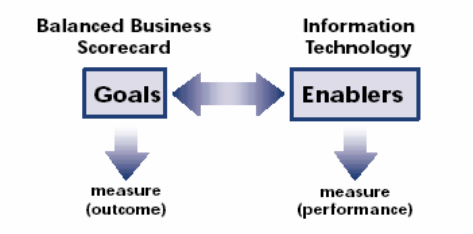
Seire

- Seire protsessid osutavad vajadusele kõiki IT protsesse regulaarselt hinnata, et olla järjepidevalt vastavuses äritegevusega seatud kvaliteedinõuetele.

28

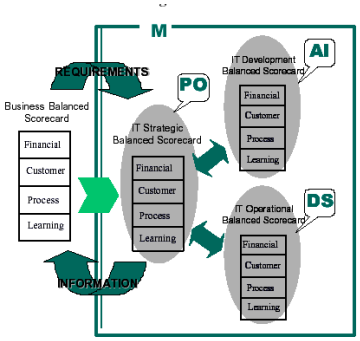
Juhtkonna suunised
Management guidelines

Goals & Enables



30

Balanced Scorecard



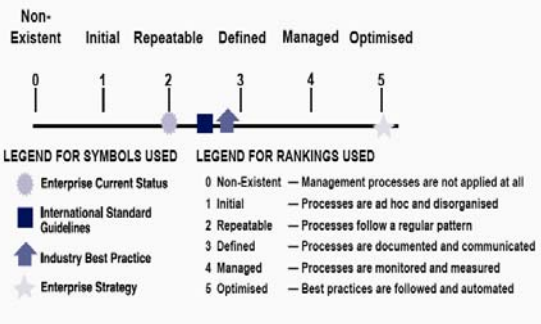
31

CSF, KGI, KPI

- **Critical Success Factors** - for getting processes under control
- **Key Goal Indicators** - for monitoring achievement of IT process goals
- **Key Performance Indicators** - for monitoring performance within each IT process

32

Maturity models



33

Generic Maturity Model

0 Non-Existent. Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.

1 Initial. There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is disorganised.

2 Repeatable. Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.

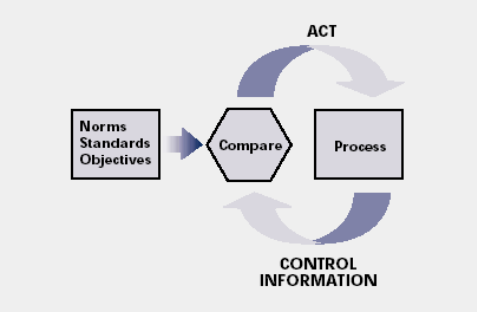
3 Defined. Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

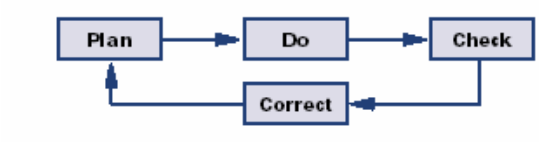
34

Critical Success Factors



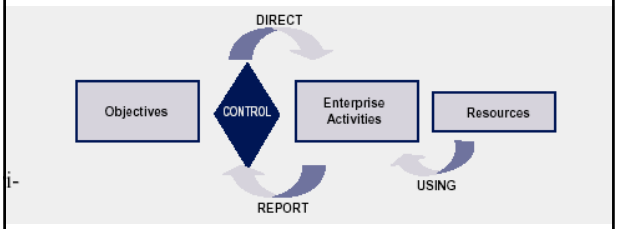
35

Four types of activities



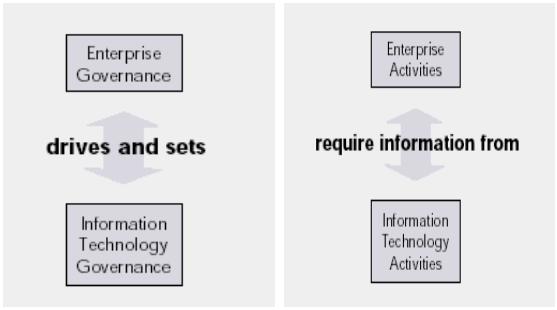
36

Enterprise Governance



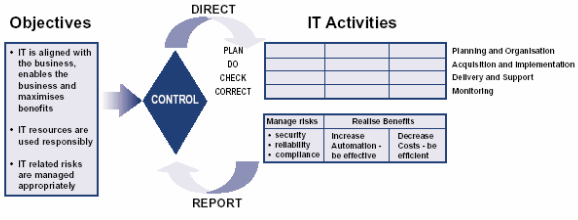
37

IT Governance



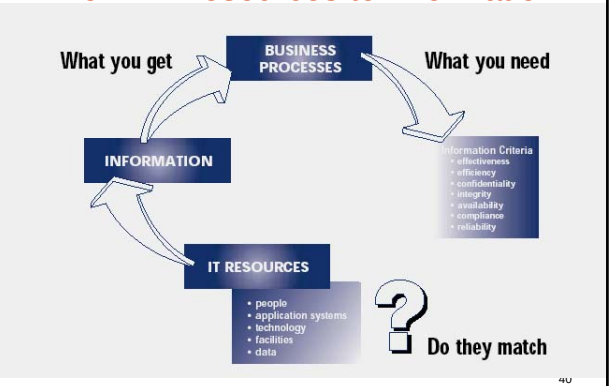
38

IT Governance



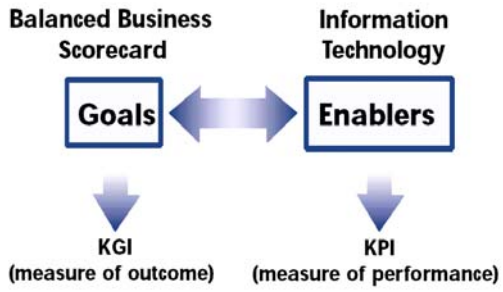
39

From IT Resources to Information



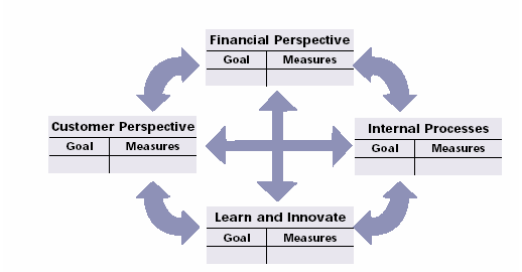
40

Key Goal Indicators



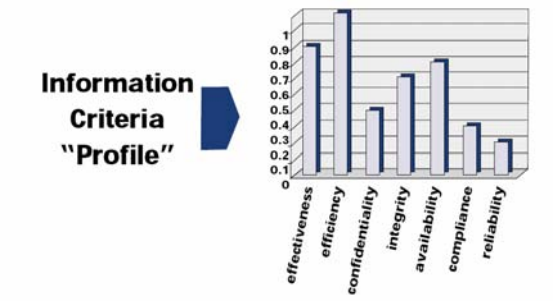
41

Four dimensions of the Balanced Business Scorecard



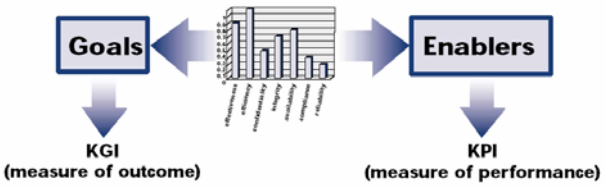
42

Information Criteria “Profile”



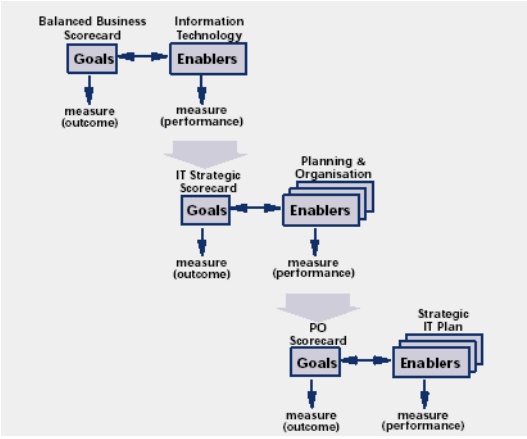
43

Key Performance Indicators

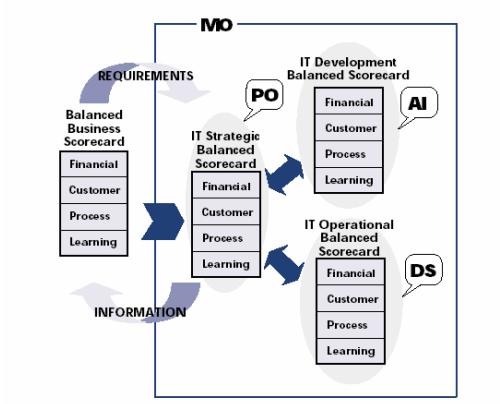


Information Criteria
• effectiveness
• efficiency
• confidentiality
• integrity
• availability
• compliance
• reliability

44



45



46

IT põhiprotsessid

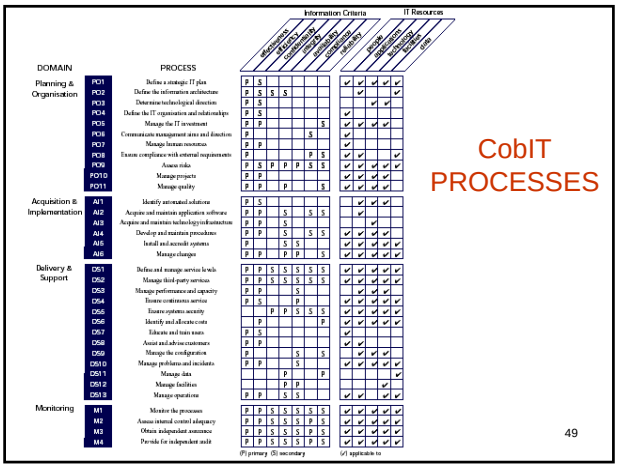
- Need neli ala jagunevad 34-ks IT põhiprotsessiks ehk – juhtkonna seisukohalt – kõrgema taseme juhtimiseesmärgiks.
- Iga juhtimiseesmärgi juures esitatakse selle aluseks olev ärinõue, mida võib ühtlasi käsitleda ka kui protsessi eesmärki.
- Ärinõude saavutamist võimaldav tegevus (juhtimisdeklaratsioon) ja protsessi kohase läbiviimise seisukohalt olulised pidepunktid (juhtimispraktikad) lihtsustavad eesmärgist arusaamist ja selle saavutamist.

47

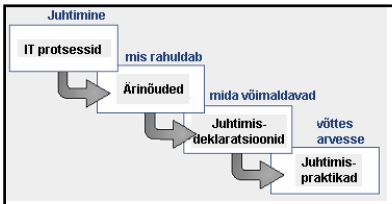
Juhtimiseesmärgid

- Iga protsessi jaoks defineerib CobIT veel täiendavalt detailsed juhtimiseesmärgid, mis aitavad leida õigeid kontrollikohti protsesside läbiviimisel ja hindamisel.
- Sõltuvalt protsessist võib neid olla kolmest kolmekümneni – ühtekokku 318 alamprotsessi/ tegevust.

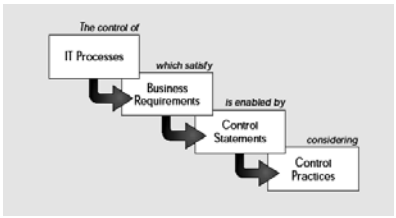
48



CobIT PROCESSES



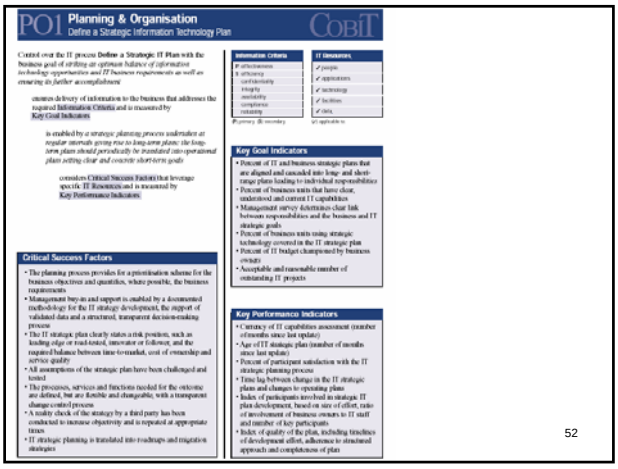
IT protsessid - struktuur



Example

P L A N N I N G & O R G A N I S A T I O N

MANAGEMENT GUIDELINES PO



PO1 Planning & Organisation
Define a Strategic Information Technology Plan
COBIT

Control over the IT process **Define a Strategic IT Plan** with the business goal of *striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment*

enables delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria

effectiveness	✓ people
efficiency	✓ applications
confidentiality	✓ technology
integrity	✓ facilities
availability	✓ data
compliance	
reliability	

(primary, secondary)

IT Resources

(applicable to)

Critical Success Factors

- The planning process provides for a prioritisation scheme for the business objectives and quantities, where possible, the business requirements
- Management buy-in and support is enabled by a documented methodology for the IT strategy development, the support of validated data and a structured, transparent decision-making process
- The IT strategic plan clearly states a risk position, such as leading edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality
- All assumptions of the strategic plan have been challenged and tested
- The processes, services and functions needed for the outcome are defined, but are flexible and changeable, with a transparent change control process
- A reality check of the strategy by a third party has been conducted to increase objectivity and is repeated at appropriate times
- IT strategic planning is translated into roadmaps and migration strategies

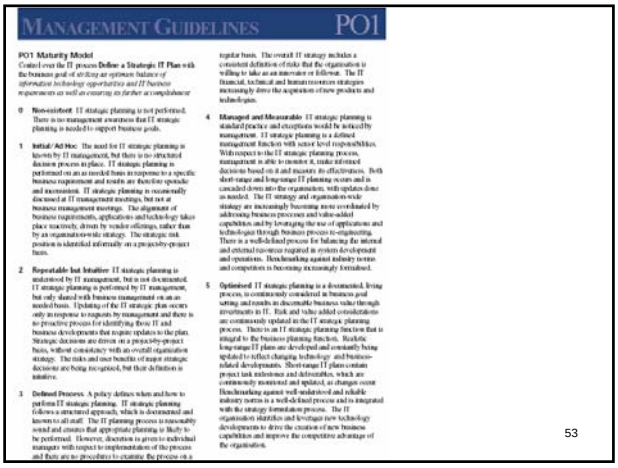
Key Goal Indicators

- Percent of IT and business strategic plans that are aligned and cascaded into long- and short-range plans leading to individual responsibilities
- Percent of business units that have clear, understood and current IT capabilities
- Management survey determines clear link between responsibilities and the business and IT strategic goals
- Percent of business units using strategic technology covered in the IT strategic plan
- Percent of IT budget championed by business owners
- Acceptable and reasonable number of outstanding IT projects

Key Performance Indicators

- Currency of IT capabilities assessment (number of months since last update)
- Age of IT strategic plan (number of months since last update)
- Percent of participant satisfaction with the IT strategic planning process
- Time lag between change in the IT strategic plans and changes to operating plans
- Index of participants involved in strategic IT plan development, based on size of effort, ratio of involvement of business owners to IT staff and number of key participants
- Index of quality of the plan, including timelines of development effort, adherence to structured approach and completeness of plan

52



MANAGEMENT GUIDELINES
PO1

PO1 Maturity Model

Control over the IT process **Define a Strategic IT Plan** with the business goal of *striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment*

0 **Non-existent** IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 **Initial/Ad Hoc** The need for IT strategic planning is known by IT management, but there is no structured decision process in place. IT strategic planning is performed on an as needed basis in response to a specific business requirement and results are therefore sporadic and inconsistent. IT strategic planning is occasionally discussed at IT management meetings, but not at business management meetings. The alignment of business requirements, applications and technology takes place reactively, driven by vendor offerings, rather than by an organisation-wide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 **Repeatable but Intuitive** IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but only shared with business management on an as needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan. Strategic decisions are driven on a project-by-project basis, without consistency with an overall organisation strategy. The risks and user benefits of major strategic decisions are being recognised, but their definition is intuitive.

3 **Defined Process** A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach, which is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process and there are no procedures to examine the process on a regular basis. The overall IT strategy includes a consistent definition of risks that the organisation is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly drive the acquisition of new products and technologies.

4 **Managed and Measurable** IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior level responsibilities. With respect to the IT strategic planning process, management is able to monitor it, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisation-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalised.

5 **Optimised** IT strategic planning is a documented, living process, is continuously considered in business goal setting and results in discernable business value through investments in IT. Risk and value added considerations are continuously updated in the IT strategic planning process. There is an IT strategic planning function that is integral to the business planning function. Realistic long-range IT plans are developed and constantly being updated to reflect changing technology and business-related developments. Short-range IT plans contain project task milestones and deliverables, which are continuously monitored and updated, as changes occur. Benchmarking against well-understood and reliable industry norms is a well-defined process and is integrated with the strategy formulation process. The IT organisation identifies and leverages new technology developments to drive the creation of new business capabilities and improve the competitive advantage of the organisation.

53

Additional Standards

Additional Standards

- **Technical standards** from ISO, EDIFACT, etc.
- **Codes of Conduct** issued by the Council of Europe, OECD, ISACA, etc.
- **Qualification criteria** for IT systems and processes: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc.
- **Professional standards** for internal control and auditing: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.
- **Industry practices and requirements** from industry forums (ESF, I4) and government-sponsored platforms (IBAG, NIST, DTI), etc., and
- **Emerging industry-specific requirements** from banking, electronic commerce, and IT manufacturing.

55

Additional Standards (short list)

- ITIL
- ISO/IEC 17799:2000
- ISO/IEC TR 13335
- ISO/IEC 15408
- TickIT
- NIST 800-14
- COSO

56

ITIL

- ITIL – The IT Infrastructure Library is a collection of best practices in IT service management. It is focused on the service processes of the IT and considers the central role of the user.

57

ISO/IEC 17799:2000

- ISO/IEC 17799:2000 – The Code of Practice for Information Security Management is an international standard, based on BS 7799-1. It is presented as best practice for implementing information security management.

58

ISO/IEC TR 13335

- ISO/IEC TR 13335 – The technical report Guidelines for the Management of IT Security contains information on IT security management not only from the planning perspective, but also from the implementation and maintenance perspectives.

59

ISO/IEC 15408

- ISO/IEC 15408 – Security Techniques—Evaluation Criteria for IT Security is used as a reference to evaluate and certify the security of IT products and services.

60

TickIT

- TickIT – TickIT provides a scheme for the certification of the software quality management system.It intends to improve the effectiveness of the quality management system and targets customers, suppliers and assurance professionals.

61

NIST 800-14

- NIST 800-14 – The special publication Generally Accepted Principles and Practices for Securing Information Technology Systems contains information for establishing a comprehensive IT security program.

62

COSO

- COSO Integrated Framework defines a framework that initiates an integrated process of internal control.

63