IT-audits according to COBIT

Experiences of the Regional Audit Court of Upper Austria

Regional Audit Court of Upper Austria

- Regional Audit Court is responsible for the audit of
  - IT-organisations within the Administration of Upper Austria and of associated companies
  - Computer centres
- So far the Regional Audit Court has audited the IT of the Administration of Upper Austria including one big computer centre two times using the COBIT model (2001/2002 und 2008/2009)

IT - Department

- **Tasks**
  - development, IT-Strategy and IT-Standards
  - procurement, provision and operation of the IT-infrastructure
  - data security
  - software development and -servicing
  - IT-training and consulting

- **IT-expenses 2008: 24 Mio Euro**
  - 9.5 Mio Euro personnel expenses
  - 14.5 Mio Euro tangible expenses

- **App. 150 employees**

Control Objectives for Information and related Technology

(Version 4 respectively 4.1)

- **internationally acknowledged standard for the overall steering and control of the IT**
  - developed by the ***Information Systems Audit and Control Association (ISACA)***
- procedure for an overall **check and assessment of the IT** and its processes
- COBIT is a **process-oriented model** and therefore independent of the technology used or the branch

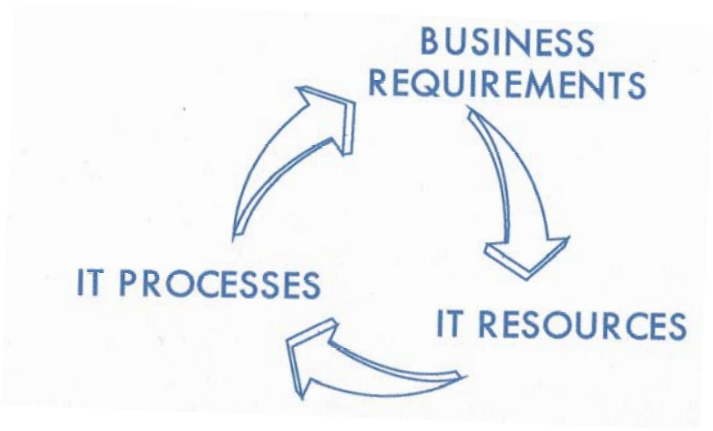
COBIT

- **COBIT guarantees**
  - **an overall assessment of the IT** according to the requirements of a professional IT-System
  - **reliable application of the Information Technology**
    - due to use of generally applicable IT-process-oriented control objectives and audit-tools
  - **fulfilment of IT-Governance Objectives**
    - constant alignment of the IT with business objectives and processes
    - supporting the fulfilment of business objectives
    - responsible and lasting use of IT-resources
    - increasing the satisfaction of customers and associates
    - minimizing IT-risks

COBIT

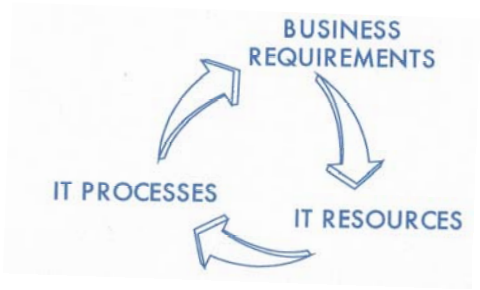
- **COBIT is an internationally acknowledged standard** for security, quality and compliance of Information Technology
- **auditing** is done by people who have acquired the competence within a special training by **ISACA**
- ISACA offers the following certifications:
  - **CISA** (Certified Information System Auditor)
  - **CISM** (Certified Information Security Manager)
  - **CGEIT** (Certified in the Governance of Enterprise IT)
  - **CRISC** (Certified in Risk and Information Systems Control)
- the **process model COBIT 4** contains 4 domains with 34 IT-processes; it can be broken down into 300 activities and controls

COBIT - Principles



COBIT - Principles

Confidentiality
Availability
Integrity
Compliance
Reliability
Effectiveness
Efficiency



Domains
- *Plan & Organise*
- *Acquire & Implement*
- *Deliver & Support*
- *Monitor & Evaluate*

Processes
Activities

Technology/Application
Information/Data
Infrastructure
Personnel

COBIT Framework

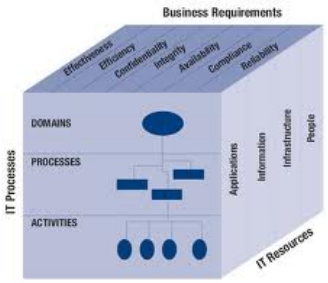
The structural design of COBIT is represented by the **COBIT Framework**. It contains **three central areas** which are essential for successful IT-Governance:

IT processes

Business Requirements concerning IT

IT resources

and shows the various divisions (types, categories)



COBIT Domains and Control Objectives

domain = cluster of main processes of a company

CONTROL OBJECTIVES

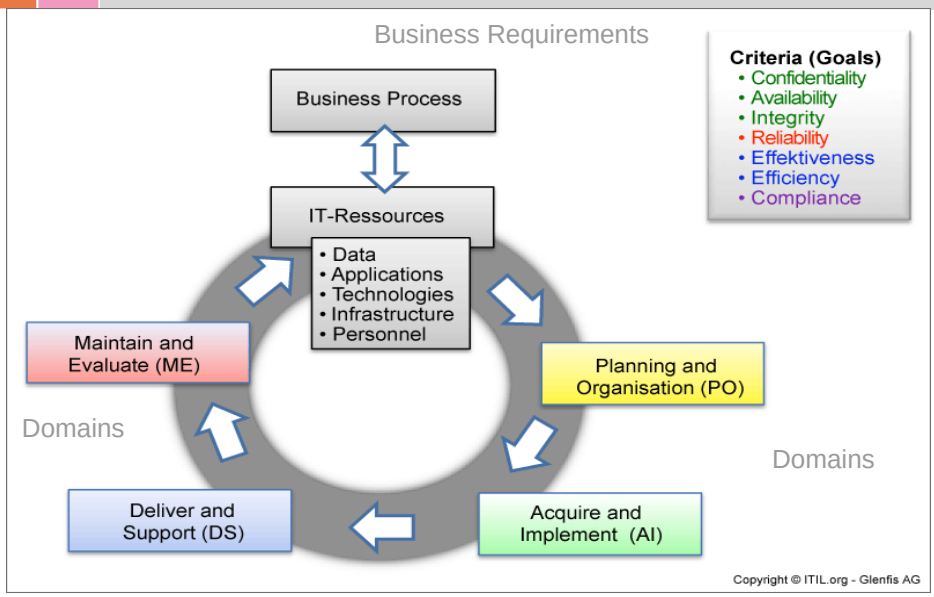
- **Plan and Organise** *(10 processes)*
  - compliance of company and IT-strategy
  - optimal use of IT-resources in the company
  - understanding within the organisation of the IT-objectives
  - provision of the proper resources and the IT-environment
  - assessment of the IT-risks
- **Acquire and Implement** *(7 processes)*
  - budget and time management regarding new projects
  - procurement and implementation
  - support of business objectives
  - functionality of Change Management
  - risks of adjustment to new systems

COBIT Domains and Control Objectives

CONTROL OBJECTIVES

- **Deliver and Support** *(13 processes)*
  - services delivered
  - optimization of IT-cost
  - productivity and security when using the system
    - *security standards*
    - *user trainings*
  - confidentiality, integrity and availability of data
- **Monitor and Evaluate** *(4 processes)*
  - control system in order to identify problems as soon as possible
  - effectiveness and efficiency of internal controls
  - link to business objectives
  - measuring and reporting of risks, controls and performance
  - auditing the compliance with legal requirements
    - *guaranteeing compliance*

COBIT-Process-Model



COBIT Results

- **IT-Strategy**
  - missing overall strategy
  - insufficient coordination with overall strategy of the Administration of Upper Austria
  - unclear basic position (innovator or promoter of the established ways)
  - unused synergies with other IT-organisations within the Administration of Upper Austria
  - further emphasis on outcome-orientation
  - no strategic controlling
- **Structures and Processes**
  - existence of double structures
  - suboptimal process design
  - incomplete process map
  - inefficient process steering
  - inadequate project management
  - specific problems with the implementation of the electronic file

COBIT Results

- **IT – Technology**
  - partly not up-to-date (specific recommendations for improvement)
- **Security**
  - concrete security problems and appropriate recommendations for improvement
- **Service Quality**
  - customer survey was done
  - better coordination of service quality and customer needs
  - concrete recommendations for improvement concerning servicing and service desk
  - response time partly too long
- **Personnel**
  - wages are not up to market value

COBIT Contact Data

- **COBIT versions**
  - 1996 COBIT 1
  - 1998 COBIT 2
  - 2000 COBIT 3
  - 2005 COBIT 4
  - 2007 COBIT 4.1
  - 2012 COBIT 5

- **ISACA** www.isaca.org
  - Certified COBIT auditors:
    - KPMG
    - Ernst&Young
    - IBM
    - PricewaterhouseCoopers
    - Swiss Life etc.

Thank you
for your Attention!

LRH, Promenade 31, 4020 Linz

www.lrh-ooe.at