IT-Prüfung nach dem COBIT- Ansatz

Erfahrungen des oö. Landesrechnungshofes

Oö. Landesrechnungshof

- Landesrechnungshof ist zuständig für die Prüfung von
  - IT-Organisationen des Landes und von Beteiligungsunternehmen
  - Rechenzentren

- LRH hat bisher bereits 2 mal die IT des Landes Oberösterreich incl. eines großen Rechenzentrums unter Anwendung des COBIT Modells geprüft (2001/2 und 2008/9)

IT - Abteilung

- **Aufgaben**
  - Entwicklung IT-Strategie und IT–Standards
  - Beschaffung, Bereitstellung und Betrieb der IT-Infrastruktur
  - Datensicherheit
  - Softwareentwicklung und –betreuung
  - IT–Schulung und Beratung

- **IT-Ausgaben 2008: 24 Mio Euro**
  - 9,5 Mio Euro Personalausgaben
  - 14,5 Mio Euro Sachausgaben

- **Ca. 150 Mitarbeiter**

Control Objectives for Information and related Technology
(Version 4 bzw 4.1)

- **International anerkannter Standard zur gesamthaften Steuerung und Kontrolle der IT**
  - Entwickelt von ***Information Systems Audit and Control Association (ISACA)***
- Verfahren zur umfassenden **Kontrolle und Bewertung der IT** und deren Prozesse
- Als **prozessorientiertes Modell** ist COBIT unabhängig von der eingesetzten Technologie oder der Branche

COBIT

- **COBIT gewährleistet**
  - **umfassende Beurteilung der IT** hinsichtlich der Anforderungen an professionelles IT-System
  - **verlässliche Anwendung der Informationstechnologie**
    - durch allgemein anwendbare IT-prozessbezogene Kontrollziele und Audit-Tools
  - **Erfüllung der IT – Governance Ziele**
    - fortwährende Ausrichtung der IT an den Unternehmenszielen und -prozessen
    - Unterstützung bei der Erreichung der Geschäftsziele
    - verantwortungsvoller u. nachhaltiger Einsatz der IT-Ressourcen
    - Erhöhung der Zufriedenheit von Kunden und Beteiligten
    - Minimierung von IT - Risken

COBIT

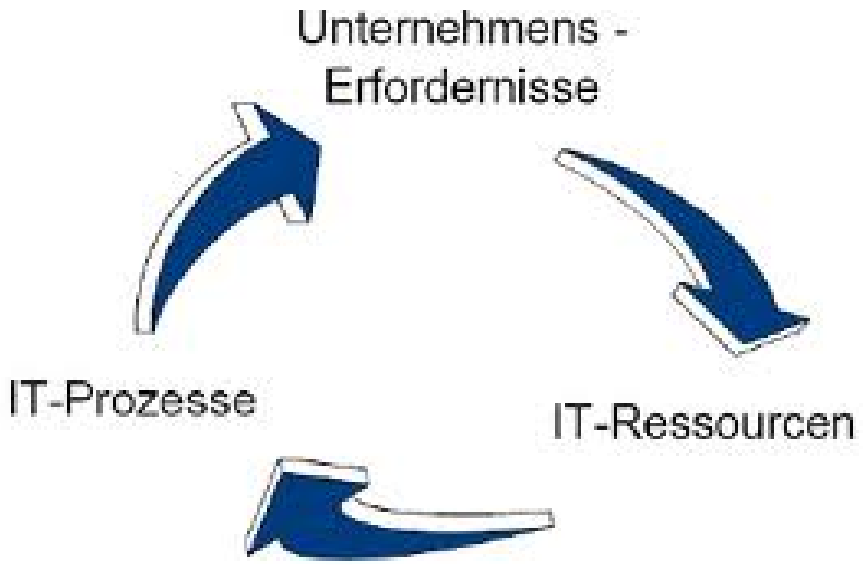
- **COBIT ist ein international anerkannter Standard** für Sicherheit, Qualität und Ordnungsmäßigkeit in der Informationstechnologie

- Die **Auditierung** erfolgt durch Personen, welche die Befähigung im Rahmen einer spezifischen Ausbildung durch die **ISACA** erlangt haben

- Die ISACA bietet hierfür Zertifizierungen an:
  - **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)

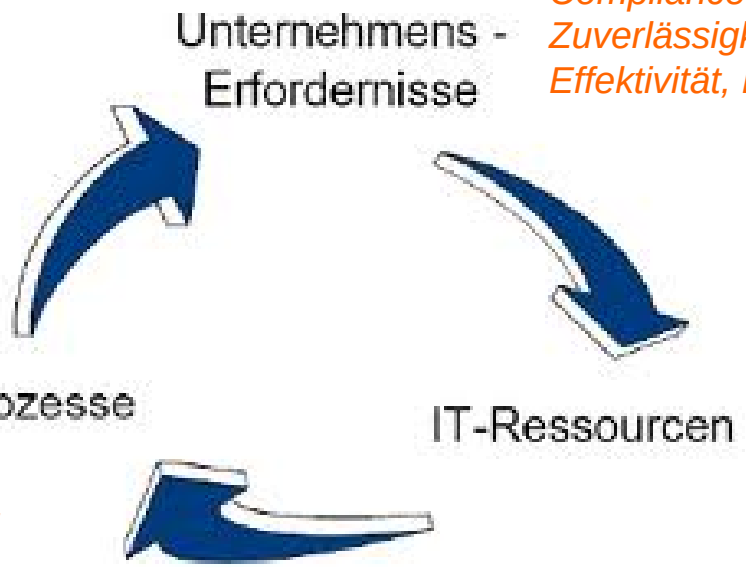
- Das **Prozessmodell COBIT 4** umfasst 4 Domains mit 34 IT-Prozessen. Dies kann bis auf über 300 Einzelaktivitäten bzw. Kontrollen heruntergebrochen werden

COBIT - Prinzip



COBIT - Prinzip

Vertraulichkeit
Verfügbarkeit
Integrität
Compliance
Zuverlässigkeit
Effektivität, Effizienz



Domänen
- *Planung & Organisation*
- *Beschaffung & Implementierung*
- *Betrieb & Support*
- *Überwachung*

Prozesse
Aktivitäten

Technologien/Anwendungen
Informationen/Daten
Geschäftsausstattung
Personal

COBIT Würfel

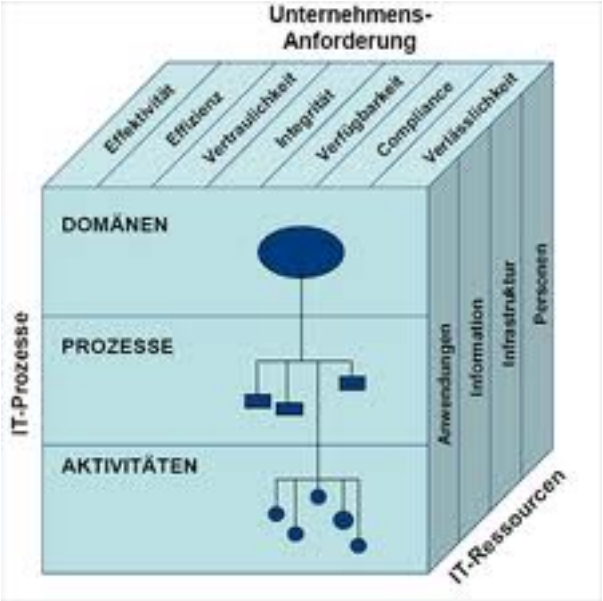
Der strukturelle Aufbau von COBIT wird durch den **COBIT-Würfel** repräsentiert. Er ist in die **drei zentralen Bereiche** unterteilt, die für eine erfolgreiche IT-Governance entscheidend sind:

IT-Prozesse

Unternehmensanforderungen an die IT

IT-Ressourcen

und zeigt die jeweiligen Untergliederungen (Typen, Kategorien)



COBIT Domänen u. Kontrollziele

Domäne = Bündel von (Haupt-)Prozessen eines Unternehmens

KONTROLLZIELE

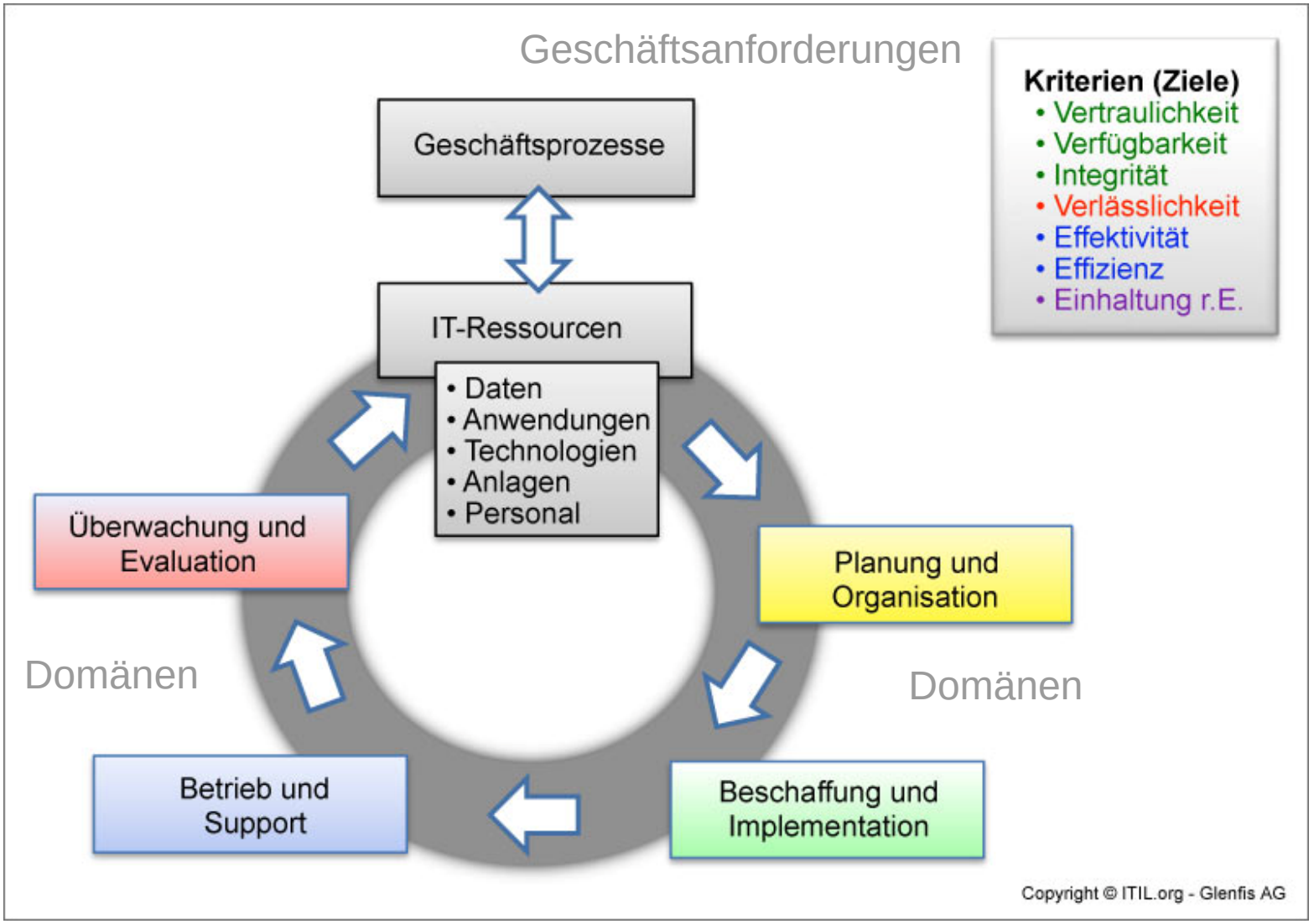
- **Planung und Organisation** *(10 Prozesse)*
  - Übereinstimmung der Unternehmens- mit der IT-Strategie
  - Optimale Nutzung der IT Ressourcen im Unternehmen
  - Verständnis in der Organisation für die IT–Ziele
  - Bereitstellung der richtigen Ressourcen und des IT–Umfeldes
  - Beurteilung der mit IT verbundenen Risken
- **Beschaffung und Implementierung** *(7 Prozesse)*
  - Budget und Zeitpläne bei neuen Projekten (und deren Einhaltung)
  - Beschaffungsvorgang u. Implementierung
  - Unterstützung der Unternehmensziele
  - Funktionalität des Change-Managements
  - Risken bei Umstellung auf neue Systeme

COBIT Domänen u. Kontrollziele

KONTROLLZIELE

- **Betrieb und Support** *(13 Prozesse)*
  - Dienstleistungserbringung
  - Optimierung der IT-Kosten
  - Produktivität u. Sicherheit beim Einsatz der Systeme durch Mitarbeiter
    - *Sicherheitsstandards*
    - *User-Schulung*
  - Vertraulichkeit, Integrität und Verfügbarkeit der Daten
- **Überwachung und Evaluation** *(4 Prozesse)*
  - Kontrollsystem zum frühzeitigen Erkennen von Problemen
  - Effektivität und Effizienz der internen Kontrollen
  - Verbindung zu den Unternehmenszielen
  - Messung und Reporting von Risken, Kontrollen, Performance
  - Prüfung der Einhaltung der rechtlichen Erfordernisse
    - *Sicherstellung der Compliance*

COBIT-Prozessmodell



COBIT Ergebnisse

- **IT-Strategie**
  - Gesamtstrategie fehlt
  - Keine ausreichende Abstimmung mit Gesamtstrategie des Landes
  - Grundlegende Positionierung unklar (Innovator oder Systemerhalter)
  - Ungenützte Synergien mit anderen IT-Dienstleistern im Bereich des Landes
  - Wirkungsorientierung muss verbessert werden
  - Strategisches Controlling fehlt
- **Strukturen und Prozesse**
  - Doppelstrukturen vorhanden
  - Suboptimale Prozessgestaltung
  - Unvollständige Prozesslandkarte
  - Keine effiziente Prozesssteuerung
  - Mangelhaftes Projektmanagement
  - Konkrete Mängel bei der Einführung des elektronischen Aktes

COBIT Ergebnisse

- **IT – Technologie**
  - teilweise nicht am Stand der Technik (konkrete Verbesserungsvorschläge)
- **Sicherheit**
  - Konkrete Sicherheitsmängel und entsprechende Verbesserungsvorschläge
- **Dienstleistungsqualität**
  - Kundenbefragung durchgeführt
  - Stärkere Anpassung der Dienstleistungsqualität an Kundenbedürfnisse
  - Konkrete Verbesserungsvorschläge zur Benutzerbetreuung und Service Desk
  - Reaktionszeiten teilweise zu lange
- **Personal**
  - Keine marktübliche Entlohnung

COBIT Kontaktdaten

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

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

Danke für die Aufmerksamkeit!

LRH, Promenade 31, 4020 Linz

www.lrh-ooe.at