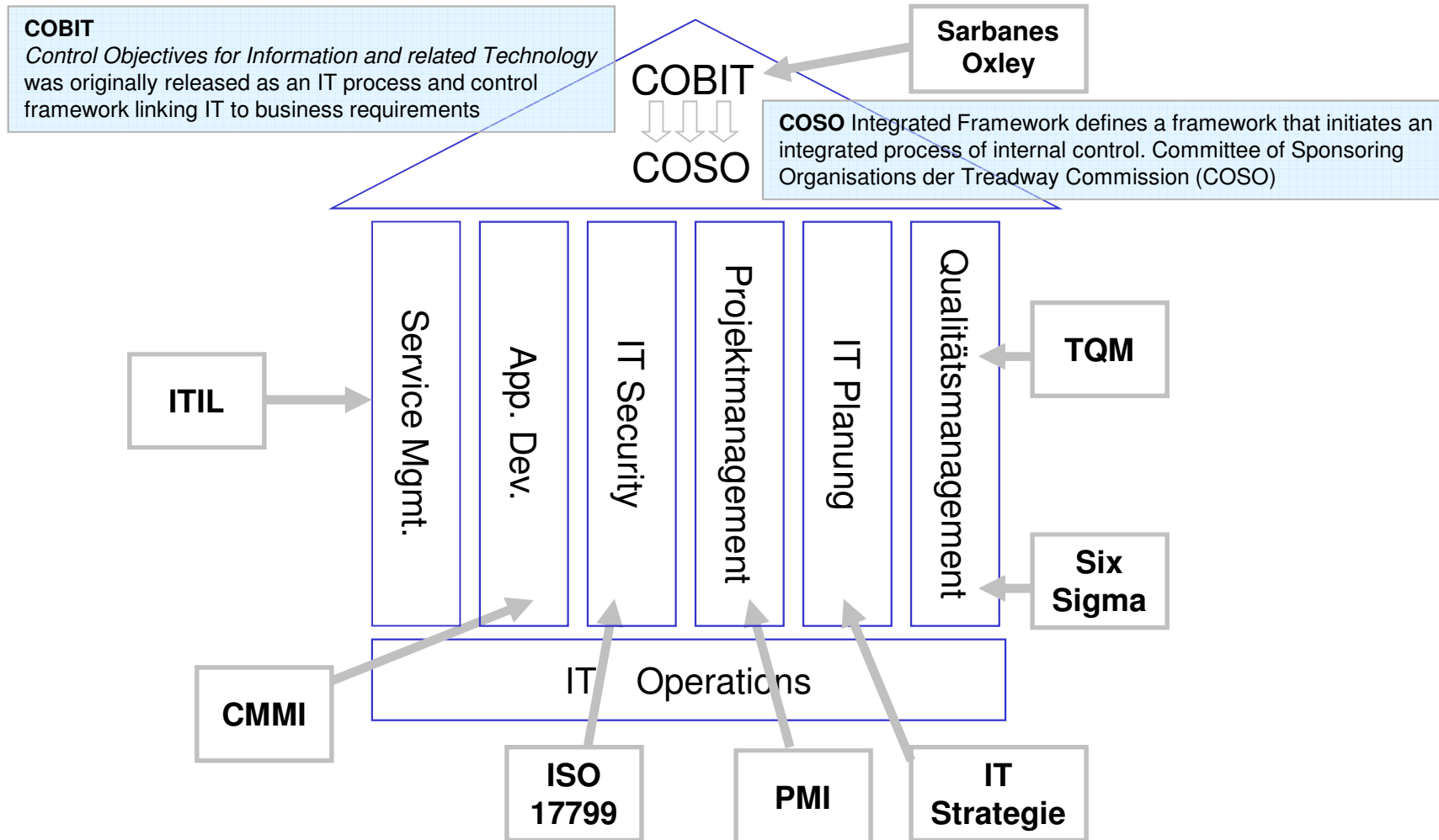


COBIT

Inhalt

- Grundlagen COBIT
- COBIT Domains
- COBIT Einführung
- COBIT und IT Governance

Kontroll- und IT Management Framework



Who needs a framework?

Board

- To ensure that the management follows and implements the strategic direction for IT

Management

- To make IT investment decisions
- To balance risk and control investment
- To benchmark existing and future IT environment

Users

- To obtain assurance on security and control of products and services they acquire internally or externally

Auditors

- To substantiate opinions to management on internal controls
- To advise on what minimum controls are necessary

Begriffsbestimmung

CobiT (*Control Objectives for Information and Related Technology*) ist das internationale anerkannte Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives.

Das **CobiT** Framework liefert Werkzeuge, die helfen, die Ausrichtung auf die Unternehmenserfordernisse sicherzustellen.

CobiT definiert hierbei nicht, WIE die Anforderungen umzusetzen sind, sondern nur WAS umzusetzen ist.

CobiT wurde ursprünglich (1993) vom internationalen Verband der EDV-Prüfer (Information Systems Audit and Control Association, ISACA) entwickelt, seit 2000 obliegt dem IT Governance Institute, einer Schwesterorganisation der [ISACA], CobiT zu entwickeln und fortzuschreiben.

Begriffsbestimmung

CobiT hat sich von einem Werkzeug für IT-Prüfer (Auditoren) zu einem Werkzeug für die Steuerung der IT aus Unternehmenssicht entwickelt.

CobiT ist in starker Anlehnung an COSO erstellt worden, um die Integration der IT-Governance in die Corporate Governance zu gewährleisten.

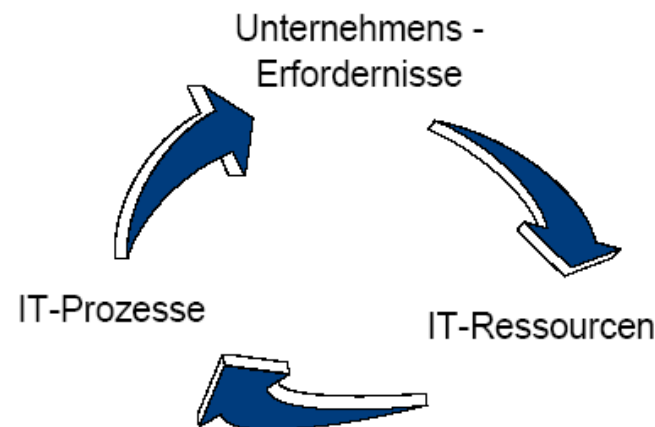
COSO (Committee of Sponsoring Organizations of the Treadway Commission) hat 1992 einen Standard für interne Kontrollen, das COSO-Modell, publiziert. Das Kontrollmodell dient der Dokumentation, Analyse und Gestaltung des internen Kontrollsystems, beschränkt sich allerdings stark auf die Finanzberichterstattung.

COBIT Charakteristiken

- fokussiert auf das Business
- orientiert an Prozessen
- basierend auf Controls
- getrieben von Messung

Fokussiert auf das Business

- Um die für die Erreichung der Ziele des Unternehmens erforderlichen Informationen bereitzustellen, muss das Unternehmen die IT-Ressourcen durch eine strukturierte Menge an Prozessen managen und steuern, die gewährleisten, dass die entsprechenden Services bereitgestellt werden.
- Das COBIT Framework liefert Werkzeuge, die helfen, die Ausrichtung auf die Unternehmenserfordernisse sicherzustellen.

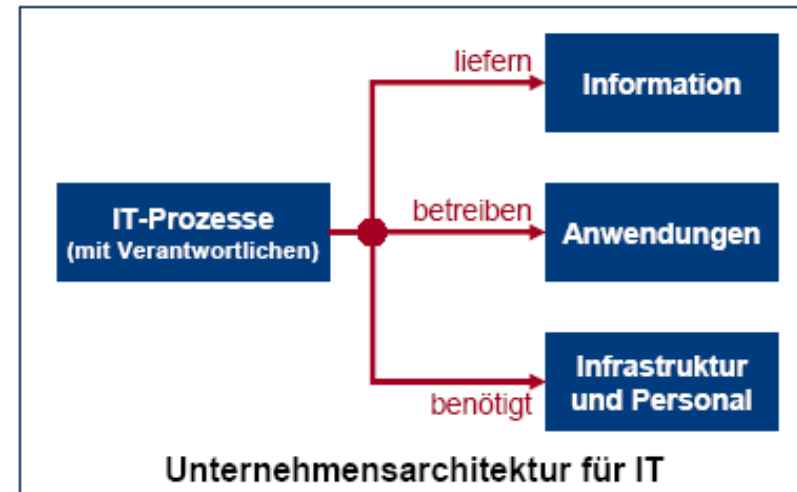
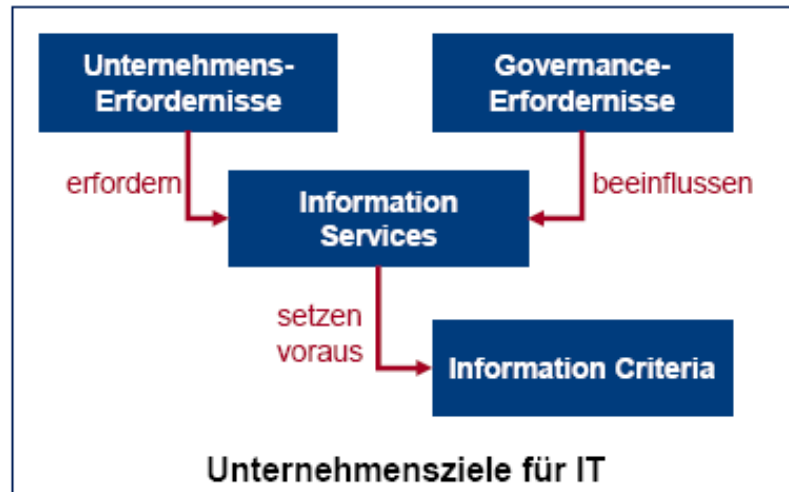
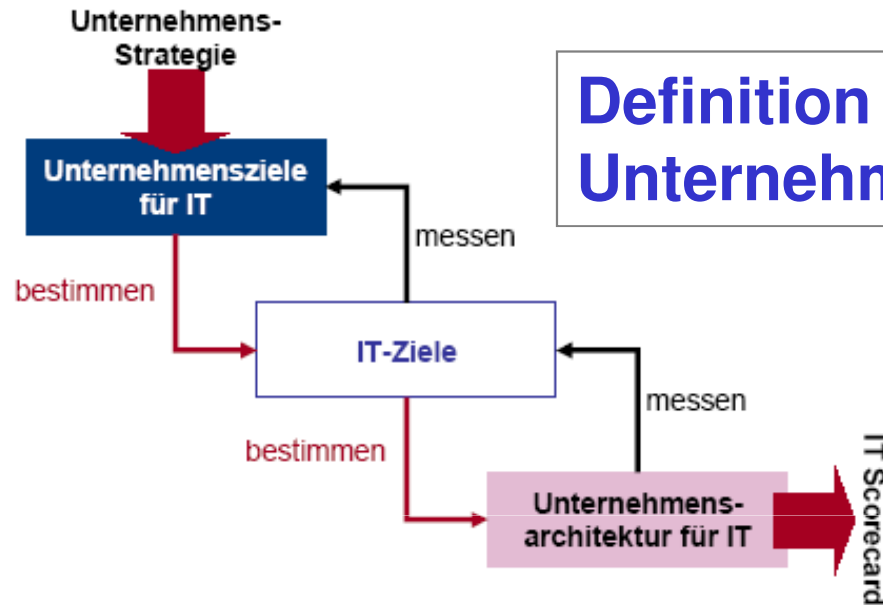


Informations Merkmale von COBIT

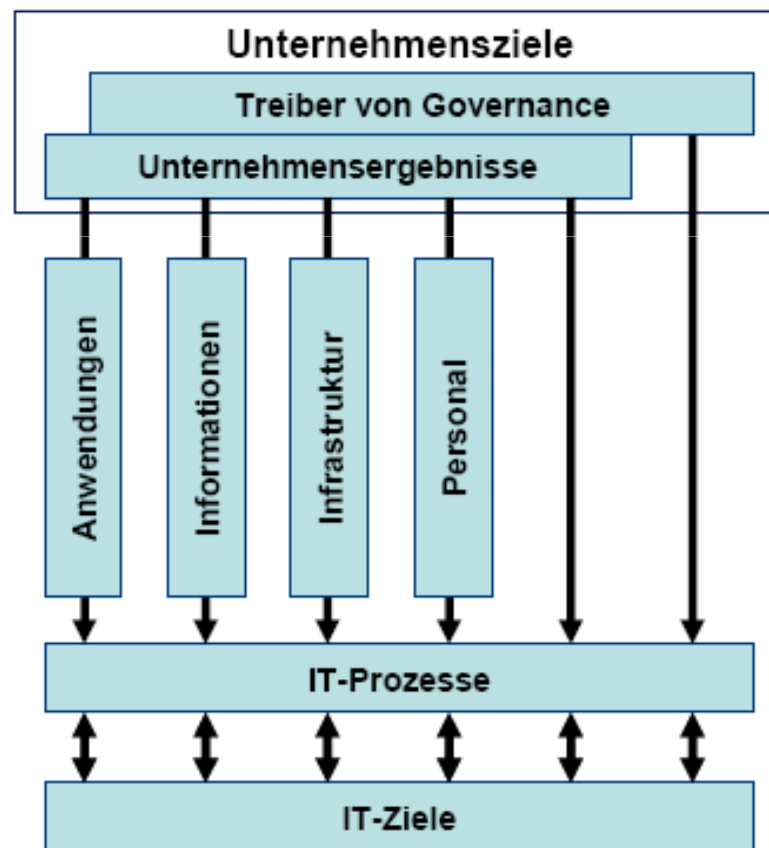
- **Effectiveness** (Wirksamkeit) behandelt die Relevanz und Angemessenheit von Informationen für den Geschäftsprozess sowie die angemessene Bereitstellung hinsichtlich Zeit, Richtigkeit, Konsistenz und Verwendbarkeit
- **Efficiency** (Wirtschaftlichkeit) behandelt die Bereitstellung von Information durch die optimale (produktivste und wirtschaftlichste) Verwendung von Ressourcen
- **Confidentiality** (Vertraulichkeit) behandelt den Schutz von sensiblen Informationen gegen unberechtigte Offenlegung
- **Integrity** (Integrität) bezieht sich auf die Richtigkeit und Vollständigkeit von Informationen sowie deren Gültigkeit in Übereinstimmung mit Unternehmenswerten und Erwartungen

Informations Merkmale von COBIT

- **Availability** (Verfügbarkeit) bezieht sich darauf, dass Informationen derzeit und in Zukunft für den Geschäftsprozess verfügbar sind. Sie betrifft auch den Schutz notwendiger Ressourcen und deren Leistungen
- **Compliance** (Compliance) behandelt die Einhaltung von Gesetzen, Regulativen und vertraglichen Vereinbarungen, welche der Geschäftsprozess berücksichtigen muss, zB extern auferlegte Kriterien sowie interne Richtlinien
- **Reliability** (Verlässlichkeit) bezieht sich auf die Angemessenheit bereitgestellter Informationen, die vom Management verwendet werden, um die Gesellschaft zu leiten und seine Treue- und Governance-Pflichten ausüben zu können



Management von IT-Ressourcen, um IT-Ziele zu erreichen



IT Ressourcen von COBIT

- **Applications** (Anwendungen) sind automatisierte Anwendungen und manuelle Verfahren, die Informationen verarbeiten
- **Information** (Informationen) sind die Daten in all ihren Formen
- **Infrastructure** (Infrastruktur) sind die Technologien und Anlagen (Hardware, Betriebssysteme, Netzwerke, Multimedia, etc und die Einrichtungen, die diese beherbergen und unterstützen)
- **People** (Personal) sind jene Personen, die für Planung, Organisation, Beschaffung, Implementierung, Betrieb, Unterstützung, Monitoring und Evaluierung der Informationssysteme und Services benötigt werden. Sie können – je nach Bedarf - intern, outgesourct oder vertraglich gebunden sein.

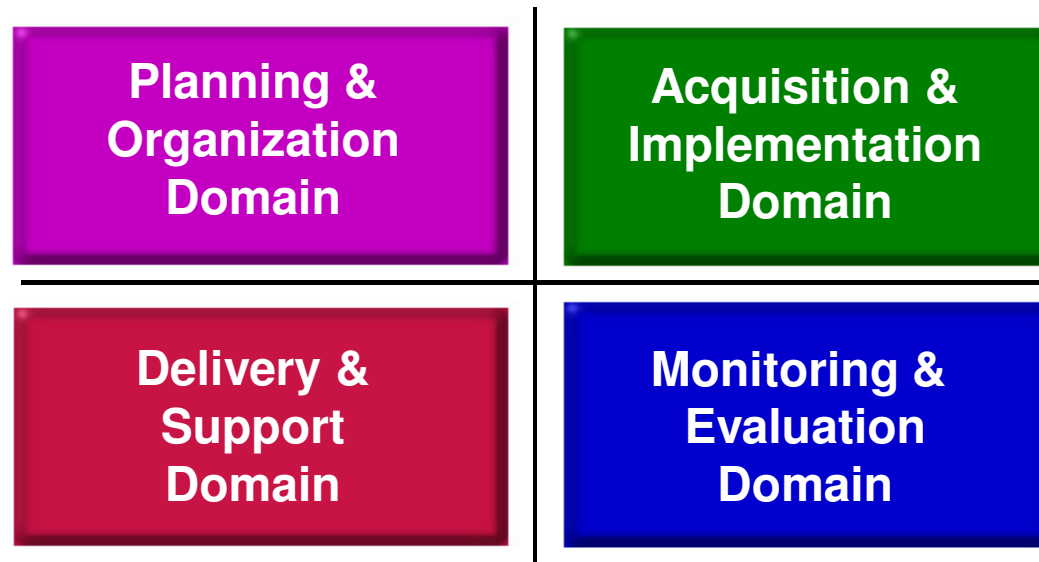
COBIT Charakteristiken

- fokussiert auf das Business
- orientiert an Prozessen
- basierend auf Controls
- getrieben von Messung

Orientiert an Prozessen

COBIT gliedert IT-Aktivitäten in einem generischen Prozessmodell in vier Domänen (engl.: Domain).

- **Planning and Organization** (plane und organisiere)
- **Acquisition and Implementation** (beschaffe und implementiere)
- **Delivery and Support** (erbringe und unterstütze)
- **Monitoring and Evaluation** (überwache und beurteile)



Plan and Organise - PO

- deckt Strategie und Taktik ab
- Identifikation, wie die IT am besten zur Erreichung der Unternehmensziele beitragen kann
- Die Umsetzung der strategischen Vision wird nach unterschiedlichen Gesichtspunkten geplant, kommuniziert und gemanagt
- Es soll eine geeignete Organisation und technologische Infrastruktur vorhanden sein.

Plan and Organise - PO

Fragen, welche beantwortet werden:

- Sind IT und Unternehmen aufeinander ausgerichtet?
- Nutzt das Unternehmen die IT-Ressourcen optimal?
- Versteht jeder in der Organisation die IT-Ziele?
- Sind IT-Risiken verstanden und werden sie gemanagt?
- Ist die Qualität der IT-Systeme ausreichend für die Anforderungen des Geschäfts?

Acquire and Implement - AI

- Identifikation, Entwicklung, Beschaffung und Umsetzung von IT-Lösungen
- Integration in die Geschäftsprozesse
- Änderungen und Wartung von bestehenden Systemen

Fragen, welche beantwortet werden:

- Entsprechen die Ergebnisse neuer Projekte mit hoher Wahrscheinlichkeit den Unternehmensanforderungen?
- Werden neue Projekte wahrscheinlich rechtzeitig und innerhalb des Budgets fertig gestellt?
- Werden die neuen Systeme nach ihrer Fertigstellung korrekt funktionieren?
- Werden Changes ohne unnötige Beeinträchtigung der gegenwärtigen Geschäftsprozesse durchgeführt?

Deliver and Support - DS

- Leistungserbringung (engl.: Service Delivery), Management der Sicherheit und Kontinuität, Service Support für BenutzerInnen und Management von Daten und Einrichtungen

Fragen, welche beantwortet werden:

- Werden IT-Services entsprechend den Prioritäten des Unternehmens erbracht?
- Sind die IT-Kosten optimiert?
- Können Anwender die IT-Systeme produktiv und sicher nutzen?
- Ist eine angemessene Vertraulichkeit, Integrität und Verfügbarkeit gegeben?

Monitor and Evaluate - ME

- regelmäßige Beurteilung der IT-Prozesse hinsichtlich ihrer Qualität und Einhaltung von Kontrollanforderungen
- Management der Performance, Überwachung von Internal Controls, Einhaltung von Regulativen und die Gewährleistung von Governance.

Fragen, welche beantwortet werden:

- Wird die Performance der IT gemessen, um Probleme zu erkennen, bevor es zu spät ist?
- Stellt das Management sicher, dass Internal Controls effektiv und effizient sind?
- Kann die IT-Performance zurück zu den Unternehmenszielen verknüpft werden?
- Werden Risiko, Control, Compliance und Performance gemessen und wird darüber berichtet?

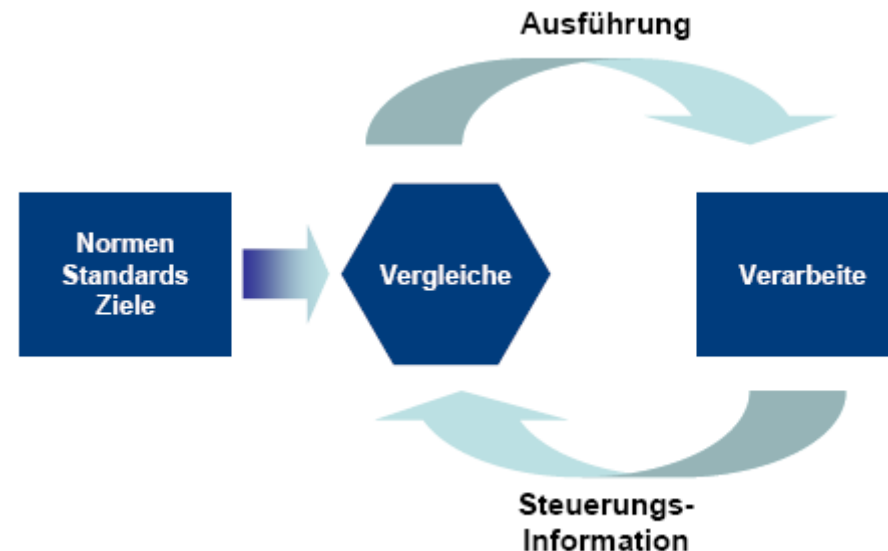
COBIT Charakteristiken

- fokussiert auf das Business
- orientiert an Prozessen
- basierend auf Controls
- getrieben von Messung

Prozesse erfordern Controls

- Controls sind Richtlinien, Verfahren, Praktiken und Organisationsstrukturen
- wurden entwickelt, um ausreichende Sicherheit zu geben, dass die Unternehmensziele erreicht werden
- unerwünschte Ereignisse sollen verhindert oder erkannt und korrigiert werden

Die Control Objectives von COBIT sind Minimalanforderungen für eine wirksame Steuerung jedes IT-Prozesses



COBIT Charakteristiken

- fokussiert auf das Business
- orientiert an Prozessen
- basierend auf Controls
- **getrieben von Messung**

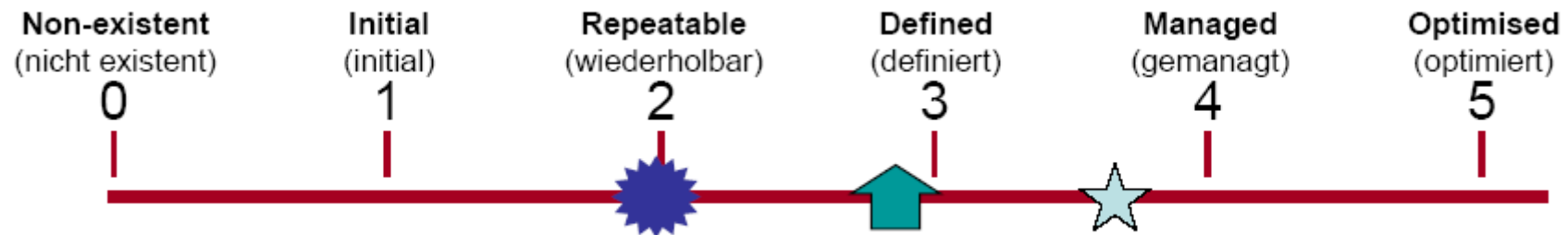
Maturity Modell - Reifegradmodell

- Methode der Organisationsbewertung
- beginnend beim Niveau nicht-existent (0) bis zu optimiert (5)
- Abgeleitet vom Maturity Model des Software Engineering Institutes (Reifegrad der Softwareentwicklung)
- für alle der 34 COBIT IT-Prozesse




Beurteilung durch das Management möglich

- Die derzeitige Performance - Wo sich das Unternehmen heute befindet.
- Den gegenwärtigen Status vergleichbarer Unternehmen - Der Vergleich.
- Das Unternehmensziel für die Verbesserung - Wo das Unternehmen sein will.

Maturity Modell – grafische Darstellung



SYMBOLE

-  Derzeitiger Status
-  Durchschnitt der Industrie
-  Unternehmensziel

NIVEAUS

- 0—Management Prozesse werden nicht angewandt
- 1—Prozesse sind ad-hoc und unorganisiert
- 2—Prozesse folgen einem regelmäßigen Muster
- 3—Prozesse sind dokumentiert und kommuniziert
- 4—Prozesse sind gemonitort und gemessen
- 5—Good Practices werden angewandt und automatisiert

Maturity Modell - Reifegradmodell

- **0 Non-existent** (nicht existent): Es ist kein Prozess erkennbar. Das Unternehmen nicht einmal den Bedarf erkannt, dass das Thema in Angriff genommen werden soll.
- **1 Initial** (initial): Es bestehen Anzeichen, dass das Unternehmen den Bedarf erkannt hat, das Thema zu behandeln. Es existieren jedoch keine standardisierten Prozesse, es ist vielmehr ein ad-hoc-Ansatz in Verwendung, der individuell und situationsbezogen angewandt wird. Der gesamthafte Managementansatz ist nicht organisiert.
- **2 Repeatable** (wiederholbar): Prozesse wurden soweit entwickelt, dass gleichartige Verfahren von unterschiedlichen Personen angewandt werden, die dieselbe Aufgabe übernehmen. Es besteht kein formales Training oder eine Kommunikation der Standardverfahren und die Verantwortung ist Einzelpersonen überlassen. Es wird stark auf das Wissen von Einzelpersonen vertraut, demzufolge sind Fehler wahrscheinlich.

Maturity Modell - Reifegradmodell

- **3 Defined** (definiert): Verfahren wurden standardisiert und dokumentiert und durch Trainings kommuniziert. Die Einhaltung der Prozesse ist jedoch der Einzelperson überlassen und die Erkennung von Abweichungen ist unwahrscheinlich. Die Verfahren sind nicht ausgereift und sind ein formalisiertes Abbild bestehender Praktiken.
- **4 Managed** (gemanagt): Es ist möglich, die Einhaltung von Verfahren zu überwachen und zu messen sowie Aktionen dort zu ergreifen, wo Prozesse nicht wirksam funktionieren. Prozesse werden laufend verbessert und folgen Good Practices. Automatisierung und Werkzeugunterstützung findet eingeschränkt und nicht integriert statt.
- **5 Optimised** (optimiert): Prozesse wurden, basierend auf laufender Verbesserung und Vergleichen mit anderen Unternehmen, auf ein Best-Practice-Niveau verbessert. IT wird integriert für die Workflow-Automatisierung verwendet, stellt Werkzeuge für die Verbesserung der Qualität und Wirksamkeit zur Verfügung und macht das Unternehmen flexibel, sich Änderungen anzupassen.

Maturity Modell - Reifegradmodell

Vorteil

- relativ einfach, sich in der Skala wiederzufinden
- erkennen, wo Handlungsbedarf für eine Performanceverbesserung notwendig ist
- Messung des Entwicklungsgrades von Management-Prozessen wird ermöglicht
- Unzulänglichkeiten im IT Prozessmanagement werden erkannt
- Definition von Ziele für den künftigen Status wird ermöglicht
- Bestimmung des richtige Niveaus durch die Art des Unternehmens, dessen Umwelt und Strategie

Ziele und Metriken

auf drei Ebenen festgelegt:

- **IT-Ziele** und Metriken, die definieren, was die Geschäftsbereiche von der IT erwarten
- **Prozessziele** und Metriken, die definieren, was der IT-Prozess liefern muss, um die Ziele der IT zu unterstützen
- Metriken der **Prozessperformance**

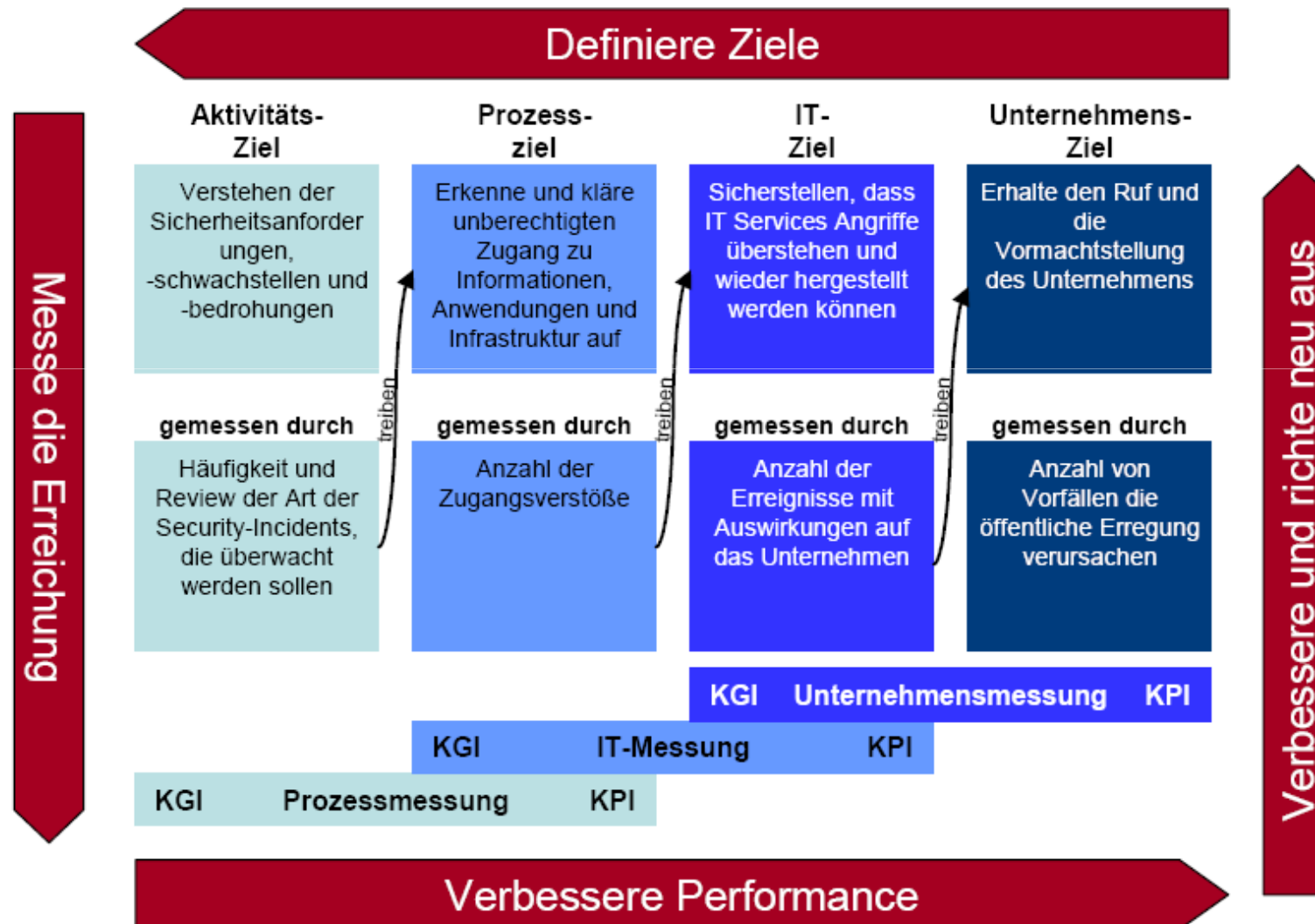
Key Goal Indicators (KGI) legen Messgrößen fest, die dem Management aufzeigen, ob ein **IT-Prozess** die *Unternehmenserfordernisse erfüllt* hat.

- Verfügbarkeit von Informationen, die von den Geschäftsprozessen benötigt werden.
- Mangel an Risiken bezüglich Integrität und Vertraulichkeit
- Kosteneffizienz von Prozessen und des Betriebs
- Bestätigung der Verlässlichkeit und Wirksamkeit

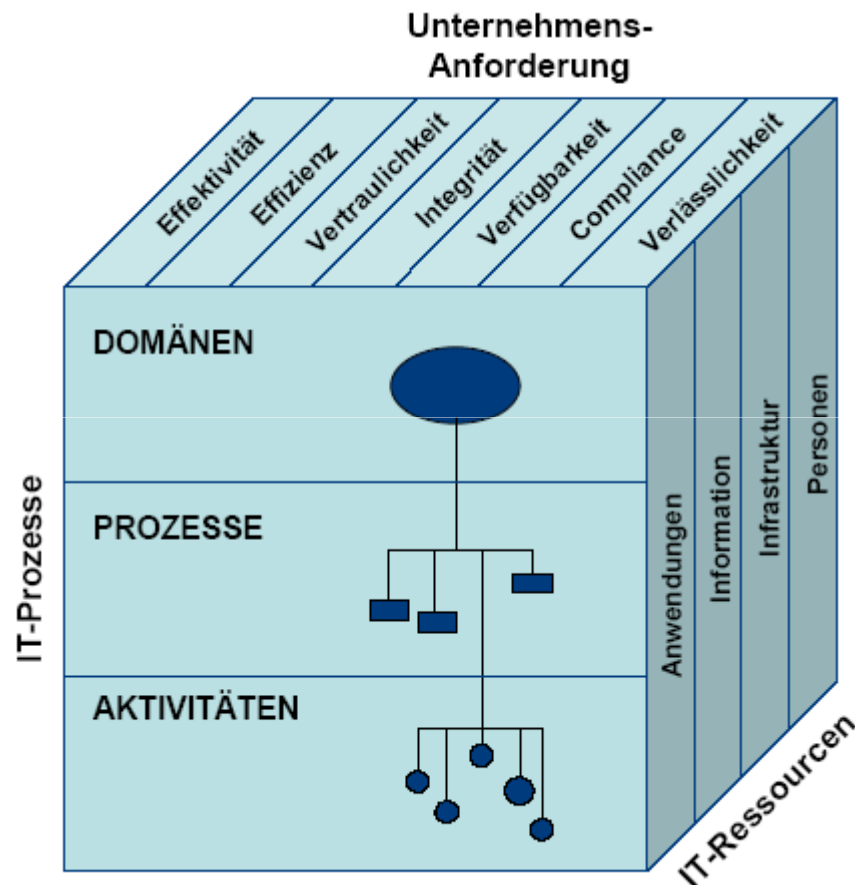
Key Performance Indicators (KPI) definieren Messgrößen, die bestimmen, *wie gut* die **Performance** von IT-Prozessen hinsichtlich der Unterstützung der Zielerreichung liegt.

- Früh-Indikatoren dafür, ob ein Ziel wahrscheinlich erreicht wird
- geben einen guten Einblick in Potential, Praktiken und Fähigkeiten
- messen die Ziele von Aktivitäten, um eine wirksame Prozessperformance zu erreichen

Beispiel: DS5 Ensure systems security



Der COBIT Würfel



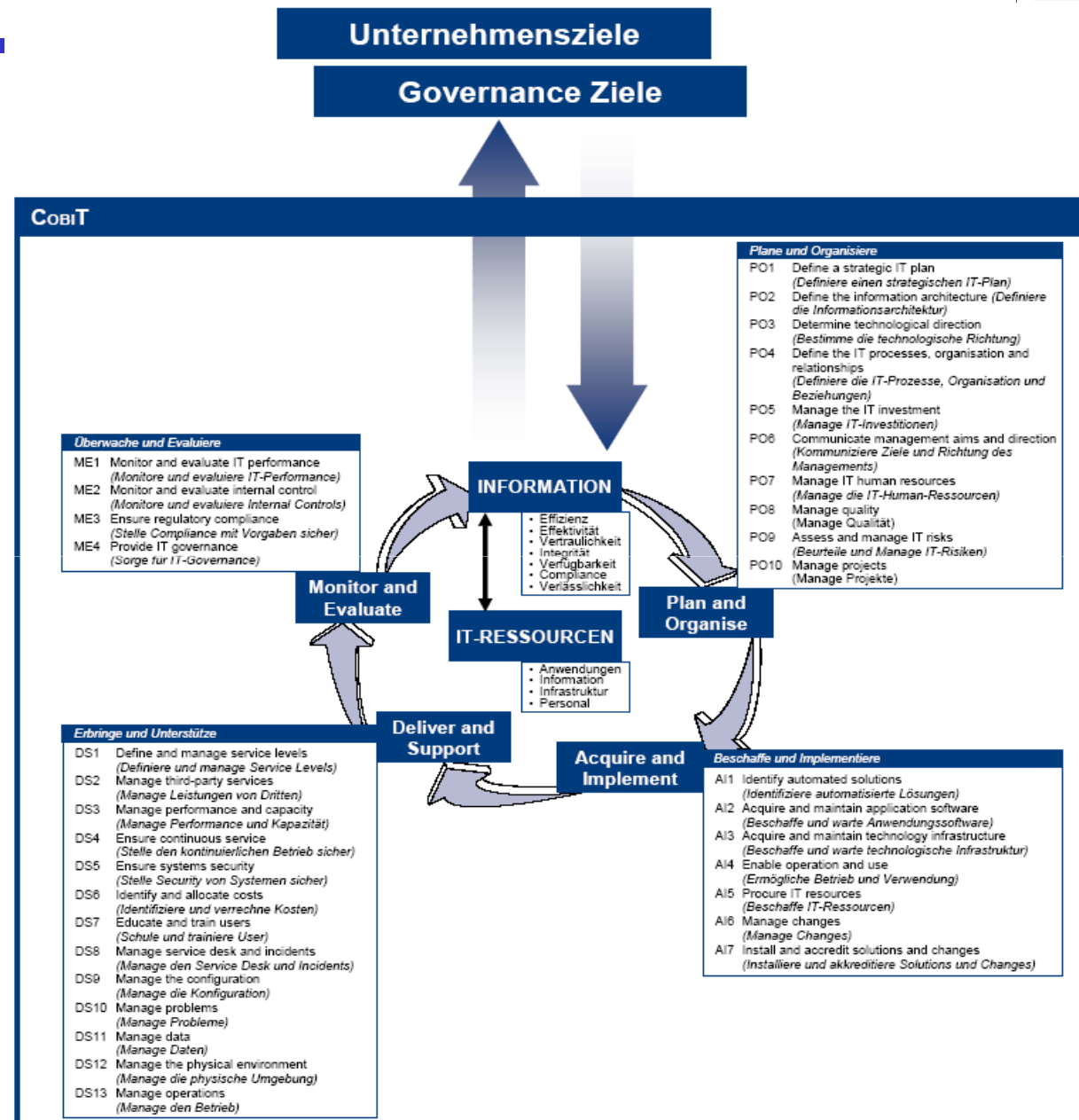
IT-Ressourcen werden durch IT-Prozesse gemanagt, um IT-Ziele zu erreichen, die auf Unternehmensanforderungen ausgerichtet sind.

Dies ist das Grundprinzip des COBIT Frameworks.

Inhalt

- Grundlagen COBIT
- COBIT Domains
- COBIT Einführung
- COBIT und IT Governance

COBIT Prozessmodell



Plan and Organise

- PO1 Define a Strategic IT Plan
(Definiere einen strategischen IT-Plan)
- PO2 Define the Information Architecture
(Definiere die Informationsarchitektur)
- PO3 Determine Technological Direction
(Bestimme die technologische Richtung)
- PO4 Define the IT Processes, Organisation and Relationships
(Definiere die IT-Prozesse, Organisation und Beziehungen der IT)
- PO5 Manage the IT Investment
(Manage IT-Investitionen)
- PO6 Communicate Management Aims and Direction
(Kommuniziere Ziele und Richtung des Managements)
- PO7 Manage IT Human Resources
(Manage die IT-Human-Ressourcen)
- PO8 Manage Quality
(Manage Qualität)
- PO9 Assess and Manage IT Risks
(Beurteile und Manage IT-Risiken)
- PO10 Manage Projects
(Manage Projekte)

Plan and Organise

BEISPIELE

PO1 „Define a Strategic IT Plan“

PO8 „Manage Quality“

Acquire and Implement

- AI1 Identify Automated Solutions
(Identifiziere automatisierte Lösungen)
- AI2 Acquire and Maintain Application Software
(Beschaffe und warte Anwendungssoftware)
- AI3 Acquire and Maintain Technology Infrastructure
(Beschaffe und warte technologische Infrastruktur)
- AI4 Enable Operation and Use
(Ermögliche Betrieb und Verwendung)
- AI5 Procure IT Resources
(Beschaffe IT-Ressourcen)
- AI6 Manage Changes
(Manage Changes)
- AI7 Install and Accredite Solutions and Changes
(Installiere und akkreditiere Lösungen und Changes)

Acquire and Implement

BEISPIEL AI2 „Acquire and Maintain Application Software“

Deliver and Support

- DS1 Define and Manage Service Levels
(Definiere und manage Service Levels)
- DS2 Manage Third-party Services
(Manage Leistungen von Dritten)
- DS3 Manage Performance and Capacity
(Manage Performance und Kapazität)
- DS4 Ensure Continuous Service
(Stelle den kontinuierlichen Betrieb sicher)
- DS5 Ensure Systems Security
(Stelle Security von Systemen sicher)
- DS6 Identify and Allocate Costs
(Identifiziere und verrechne Kosten)
- DS7 Educate and Train Users
(Schule und trainiere User)
- DS8 Manage Service Desk and Incidents
(Manage den Service Desk und Incidents)
- DS9 Manage the Configuration
(Manage die Konfiguration)
- DS10 Manage Problems
(Manage Probleme)
- DS11 Manage Data
(Manage Daten)
- DS12 Manage the Physical Environment
(Manage die physische Umgebung)
- DS13 Manage Operations
(Manage den Betrieb)

Deliver and Support

BEISPIEL DS4 „Ensure Continuous Service“

Monitor and Evaluate

- ME1 Monitor and Evaluate IT-Performance
(Monitore und evaluiere IT-Performance)
- ME2 Monitor and Evaluate Internal Control
(Monitore und evaluiere Internal Controls)
- ME3 Ensure Regulatory Compliance
(Stelle Compliance mit Vorgaben sicher)
- ME4 Provide IT-Governance
(Sorge für IT-Governance)

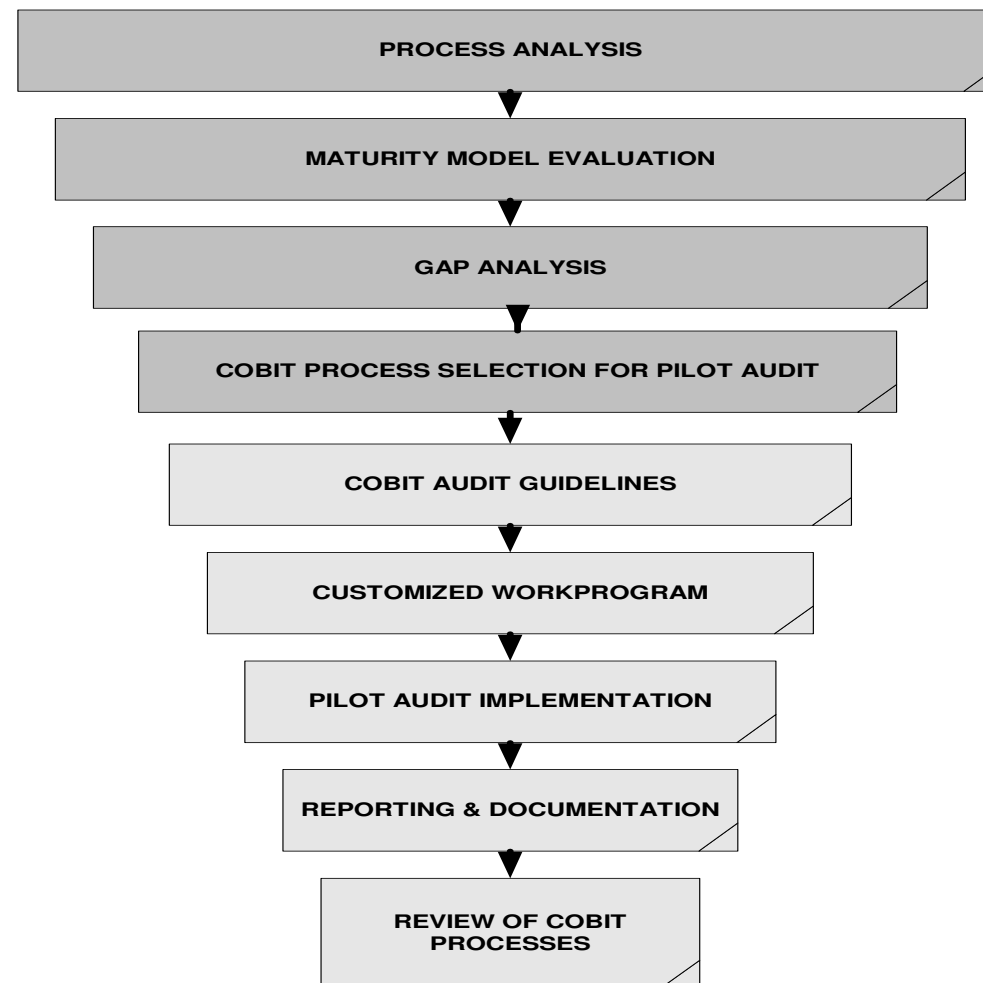
Monitor and Evaluate

BEISPIEL ME1 „Monitor and Evaluate IT-Performance“

Inhalt

- Grundlagen COBIT
- COBIT Domains
- COBIT Einführung
- COBIT und IT Governance

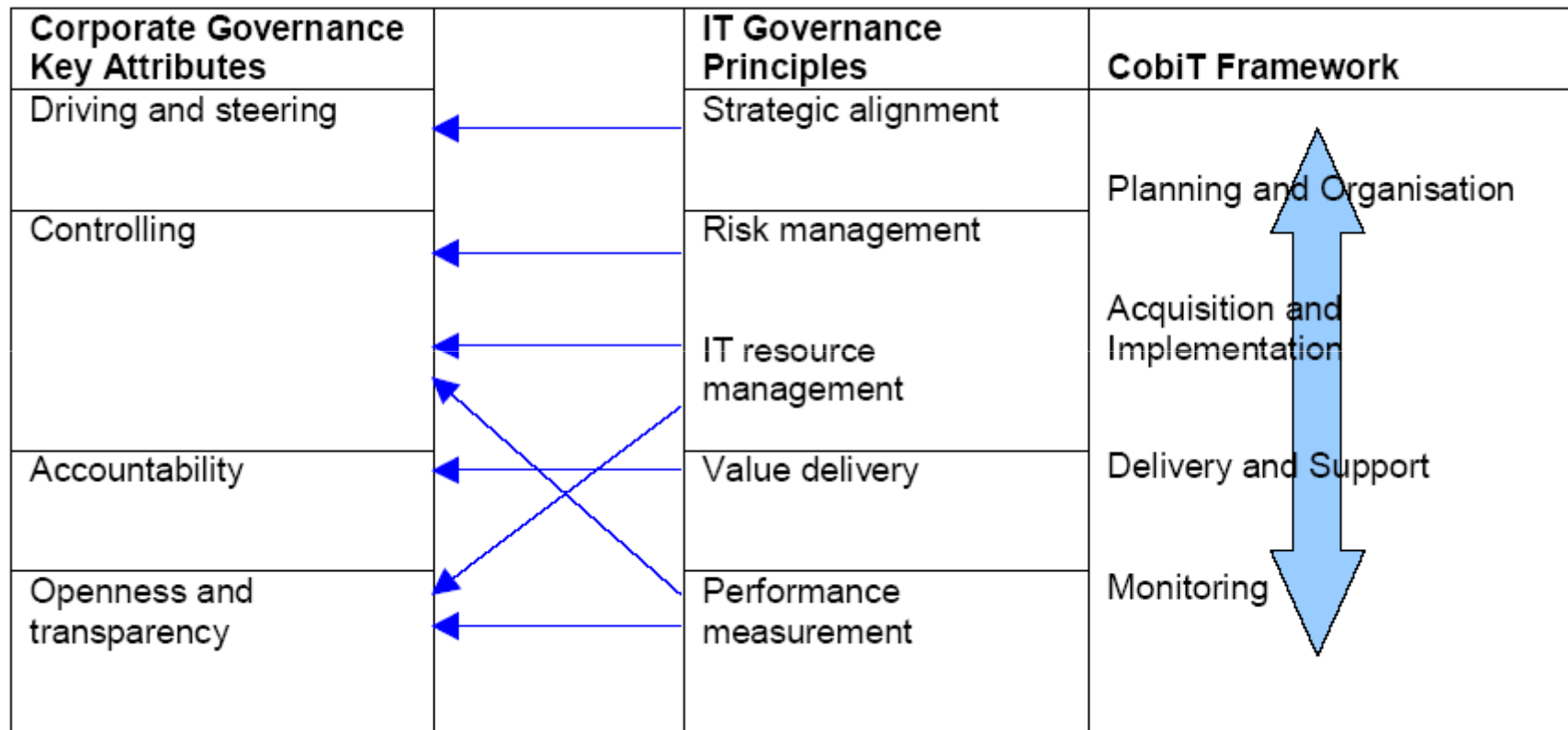
COBIT Einführung



Inhalt

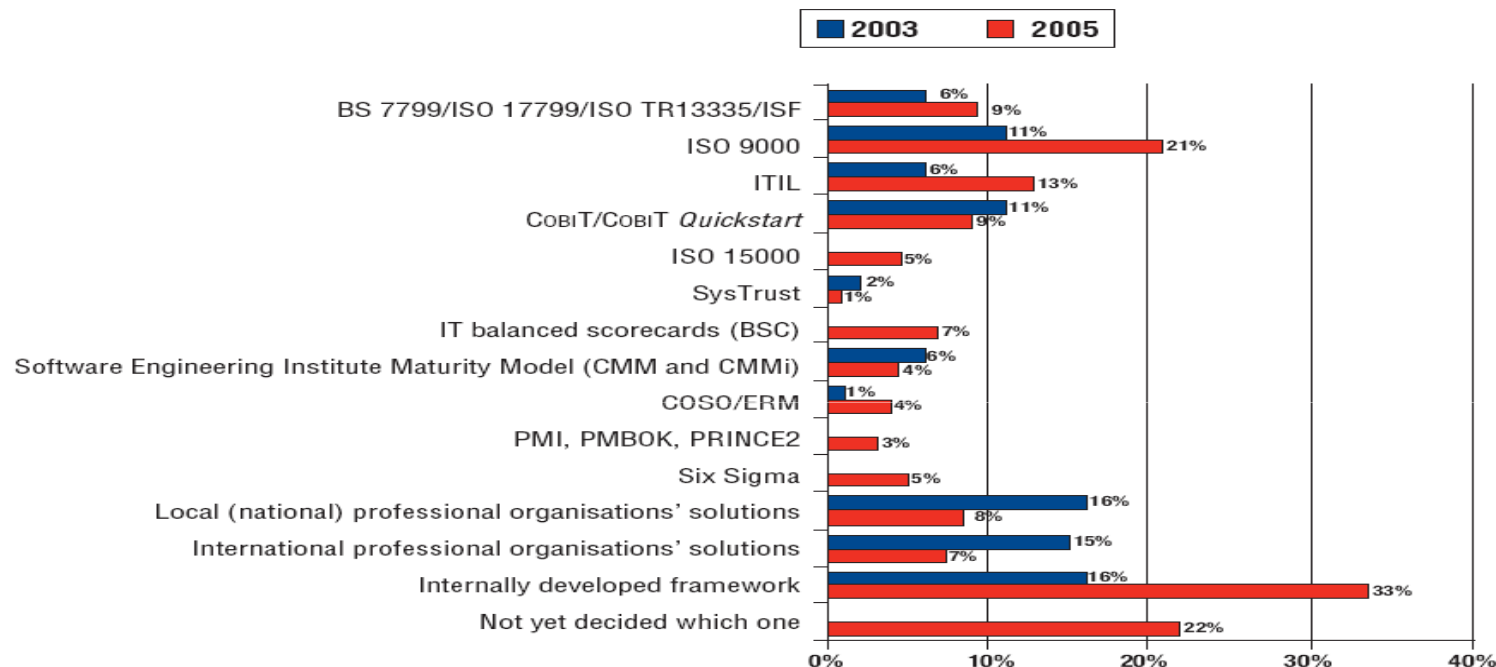
- Grundlagen COBIT
- COBIT Domains
- COBIT Einführung
- COBIT und IT Governance

Governance und COBIT



What solutions/frameworks do you use or are you considering using?

Figure 30—Selected IT Governance Frameworks

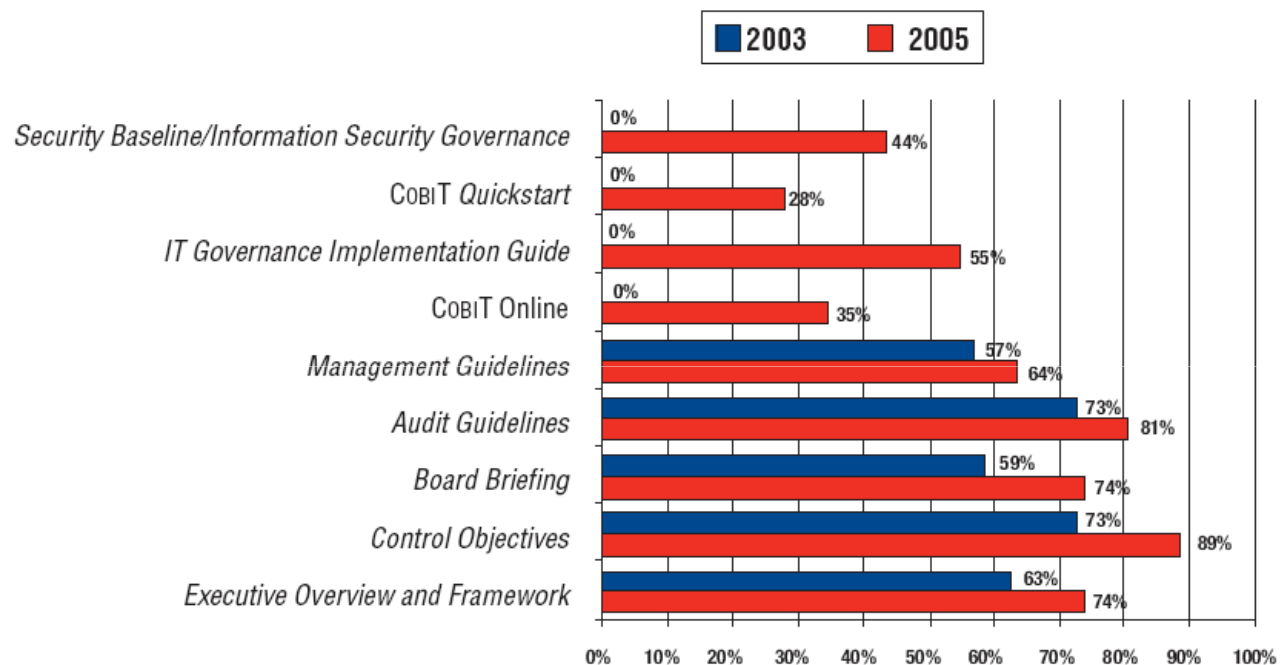


(Based on 440 respondents of the overall sample)

Observation: One-third of the participants use or are considering using an internally developed framework. Compared with 2003, the use of COBIT has decreased slightly. A possible explanation for this evolution could be that COBIT often acts as a baseline, in partial or complete form, to further elaborate an internally developed framework. Therefore, COBIT may be an integral (but not publicly acknowledged) part of the internally developed frameworks reflected in these responses.

2.5.5 Which parts of COBIT does your organisation use?

Figure 37—Use of Portions of COBIT



(Based on 89 respondents of the COBIT sample and the COBIT users in the random sample)

Weiterführende Informationen

www.itgovernance.org
www.isaca.org

Fragen / Diskussion

