CobiT

Proseminar IT Kennzahlen und Softwaremetriken

19.07.2010

Erik Muttersbach

Gliederung

- Motivation
- Komponenten des Frameworks
  - Control Objectives
  - Goals
  - Prozesse
- Messen in CobiT
  - Maturity Models
  - Outcome Measures und Performance Indicators
- Beispielprozess *DS5: Ensuring system security*
- CobiT in der Praxis
- Entwicklung und Ausblick
- Quellen

Motivation

- In vielen Unternehmen sind Informationen und IT einer der wichtigsten, aber auch einer der am wenigsten verstandenen Teile

> „Erfolgreiche Unternehmen erkennen den Nutzen der Informationstechnologie und verwenden sie, um den Stakeholder-Value zu erhöhen […]“
>
> *IT Governance Institute: CobiT 4.0, Deutsche Ausgabe, 2005*

- Daher sollten Organisationen
  - Qualität der IT und Sicherheit der Informationen sicherstellen
  - über Steuerungsmöglichkeiten bzgl. IT verfügen
  - IT Ressourcen optimieren
  - Status der unternehmensweiten IT verstehen

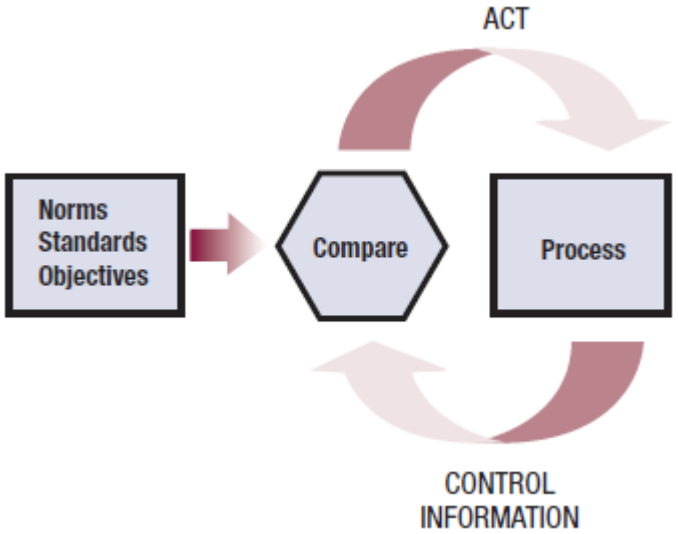
- Hierbei hilft CobiT !

Motivation

- CobiT: Control Objectives for Information and Related Technology
- IT Governance Framework
  - Steuerung der IT aus Sicht der Unterehmensführung
  - Angewendet von Führungskräften und Unternehmensleitung
- CobiT bietet Unternehmen
  - Verbindung von Unternehmensanforderungen und IT Anforderungen
  - Sichtweise auf IT, die vom Management verstanden wird
  - Einheitl. Geschäftssprache um mit allen Stakeholdern zu kommunizieren
  - Metriken und Kennzahlen die eine zuverlässige Messung der IT erlauben
- Kein Ersatz für reine unternehmensspezifische oder IT-spezifische Frameworks wie z.B.
  - COSO (Committee of Sponsoring Organizations of the Treadway Commission)
  - ITIL (IT Infrastructure Library)

Control Objectives

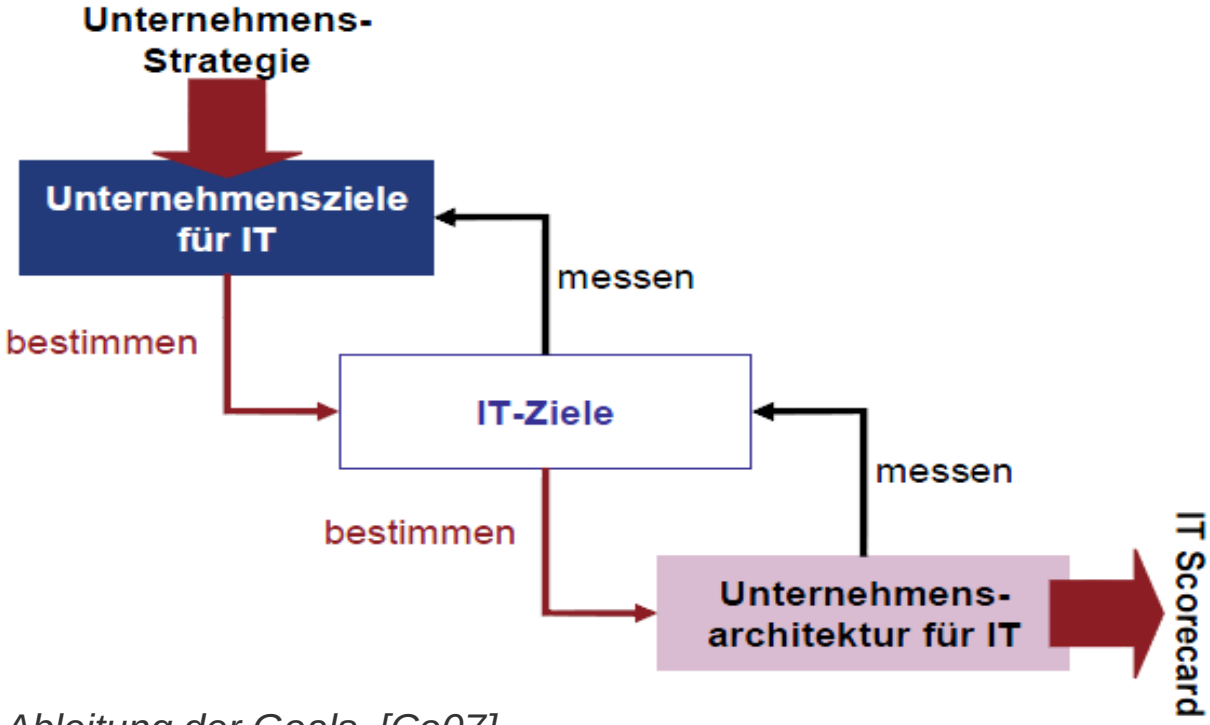
- Control Objective: Aussage über ein gewünschtes Ergebnis oder zu erreichenden Zweck einer Aktivität
- High-Level Anforderungen an IT
- Jedes Control Objective wird mit einem Prozess realisiert



Control Modell in CobiT, [Co07]

Goals

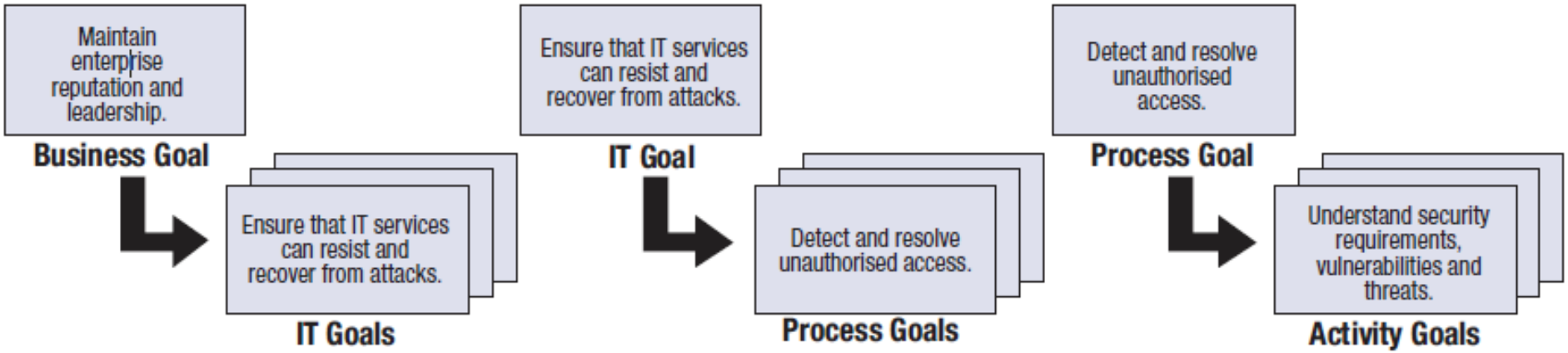
- werden Top-Down abgeleitet
- Messen der Effektivität Bottom-Up
- Formulierung der Goals in einheitlicher „Geschäftssprache“



Ableitung der Goals, [Co07]

Goals

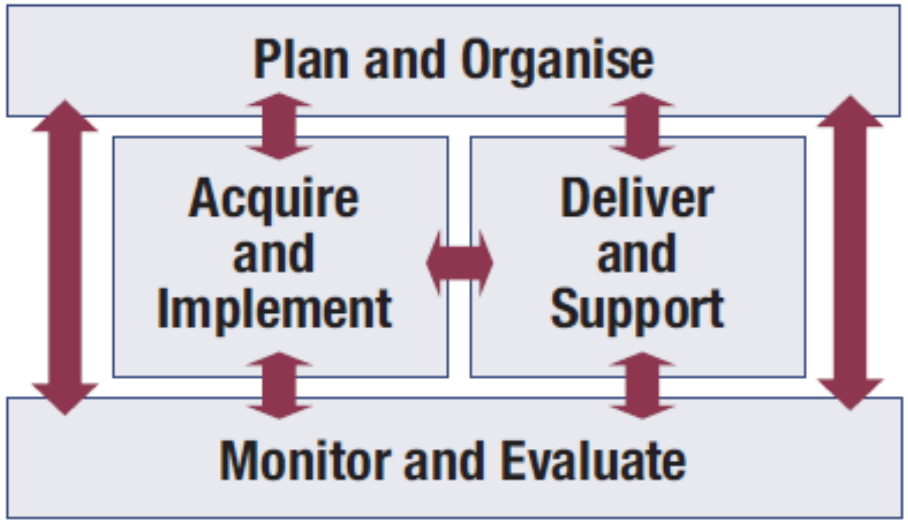
- Goals werden in 4 Ebenen definiert
- IT-interne Goals werden unterteilt in
  - IT Goals
  - Process Goals
  - Activity Goals



Beispiel-Goals des CobiT Prozesses DS5 Ensure systems security, [Co07]

Prozesse

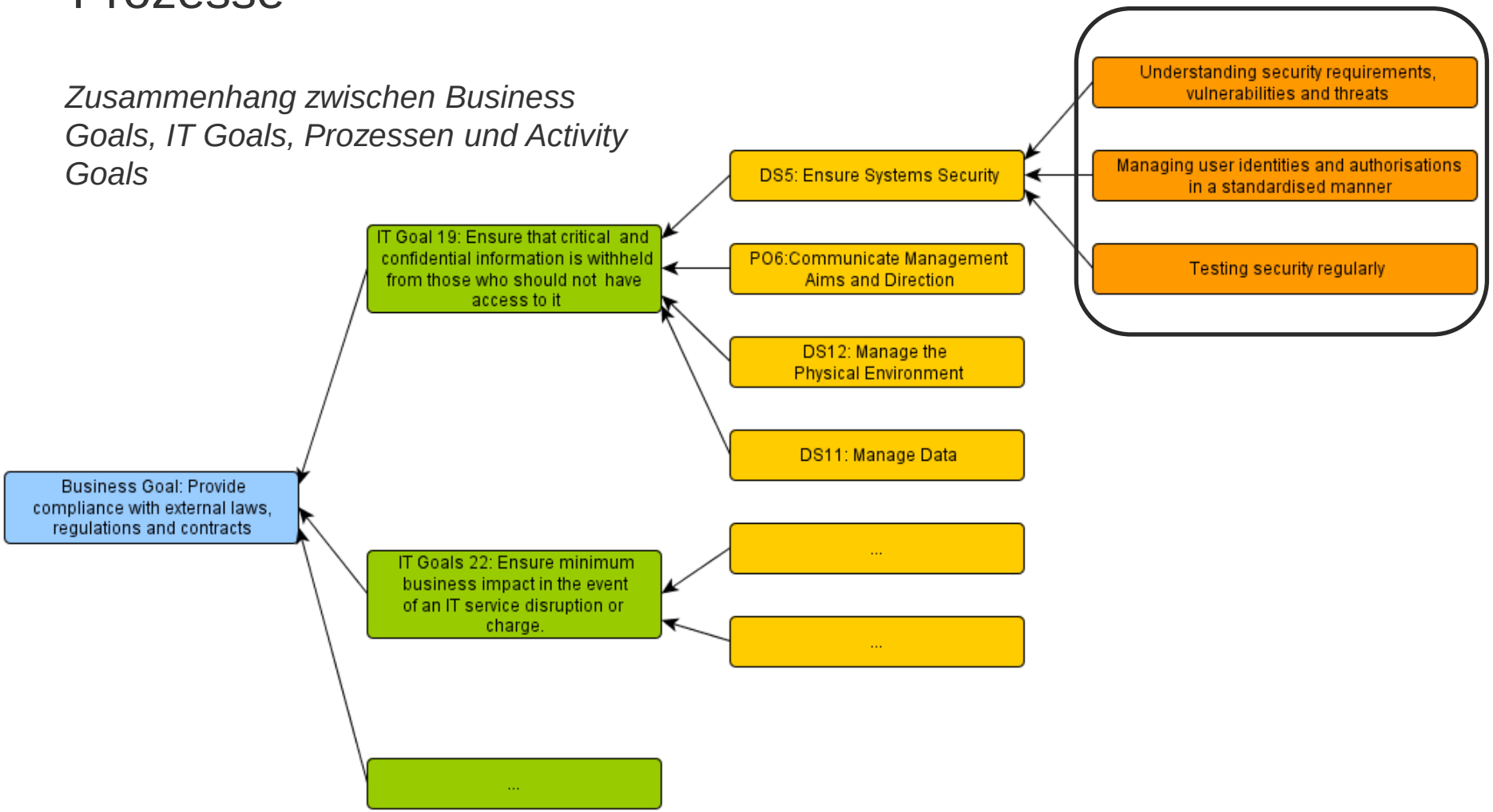
- Prozesse dienen der Erreichung der von den Business Goals abgeleiteten IT Goals
- Jeder Prozess hat Process Goals welche durch Activities und deren Activity Goals erreicht werden
- CobiT definiert 34 Prozesse die in 4 Domänen aufgeteilt sind:
  - PO – Plan and Organize
  - AI – Acquisition and Implementation
  - DS – Delivery and Support
  - ME – Monitoring and Evaluation



Die 4 Domänen von Cobit sind nicht voneinander getrennt, Sondern stehen in gegenseitiger Beziehung zueinander, [Co07]

Prozesse

Zusammenhang zwischen Business Goals, IT Goals, Prozessen und Activity Goals



Prozess im Detail

Teil 1	• Prozessnummer, -Name, -Beschreibung, -Domäne
Teil 2	• Detaillierte Control Objectives
Teil 3	• Process Inputs, Outputs • RACI Chart • Process Goals • Metriken
Teil 4	• Maturity Model

- RACI Chart bestimmt die Rollen der Personen an bestimmten Aktivitäten:
  - Responsible, Accountable, Consulted, Informed

Cobit – Messen in CobiT

- Das Management muss die IT verstehen (sh. Motivation CobiT), daher wird in CobiT folgendes gemessen:
- Benchmarking der Reife der Implementierung, bzw. Umsetzung eines Prozesses mittels **Reifegradmodell**
- Messung der Effektivität von Goals mit **Outcome Measures**

  Zu wieviel Prozent ist dieses Goal umgesetzt?

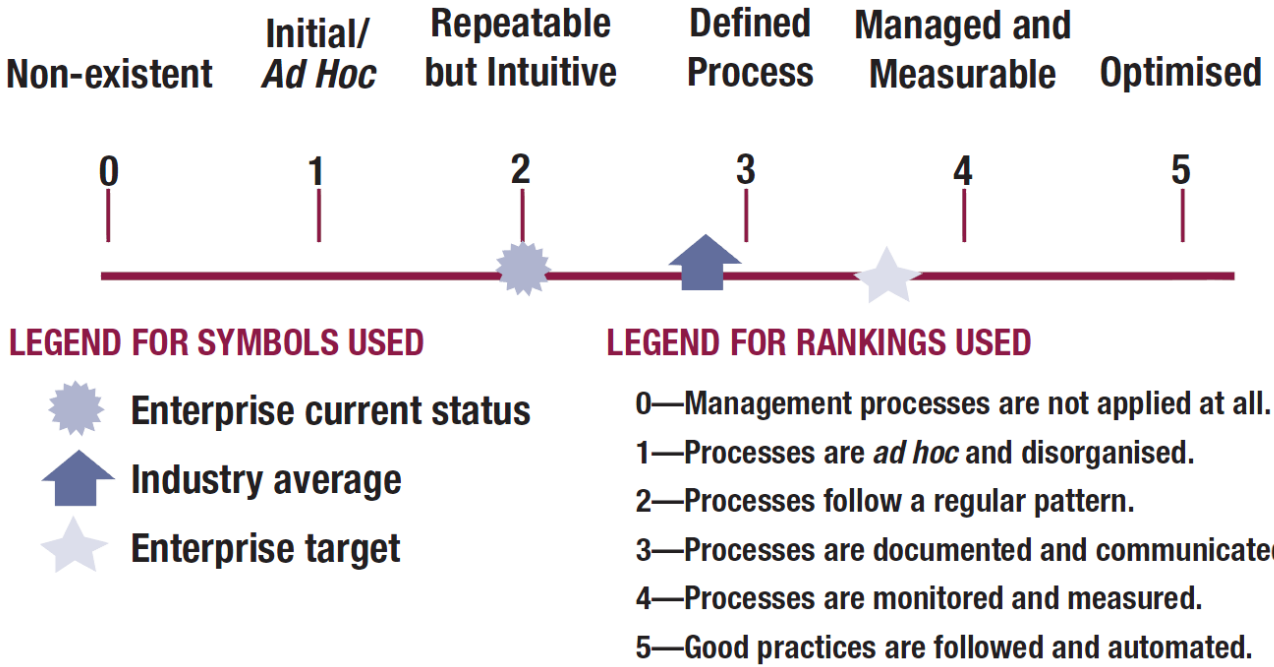
- Messung der Effizienz von Goals mit **Performance Indicators**

  Wie wahrscheinlich ist die Erreichung des Goals?

- Jede dieser Metriken wird von CobiT unterstützt!

Maturity Models

- Bewertung des Implementierungsgrads eines Prozesses von 0 (nicht existent/-implementiert) bis 5 (optimiert)
- Prozessbeschreibung enthält detaillierte Beschreibung wie ein Prozess zu klassifizieren ist



CobiT Maturity Model, [Co07]

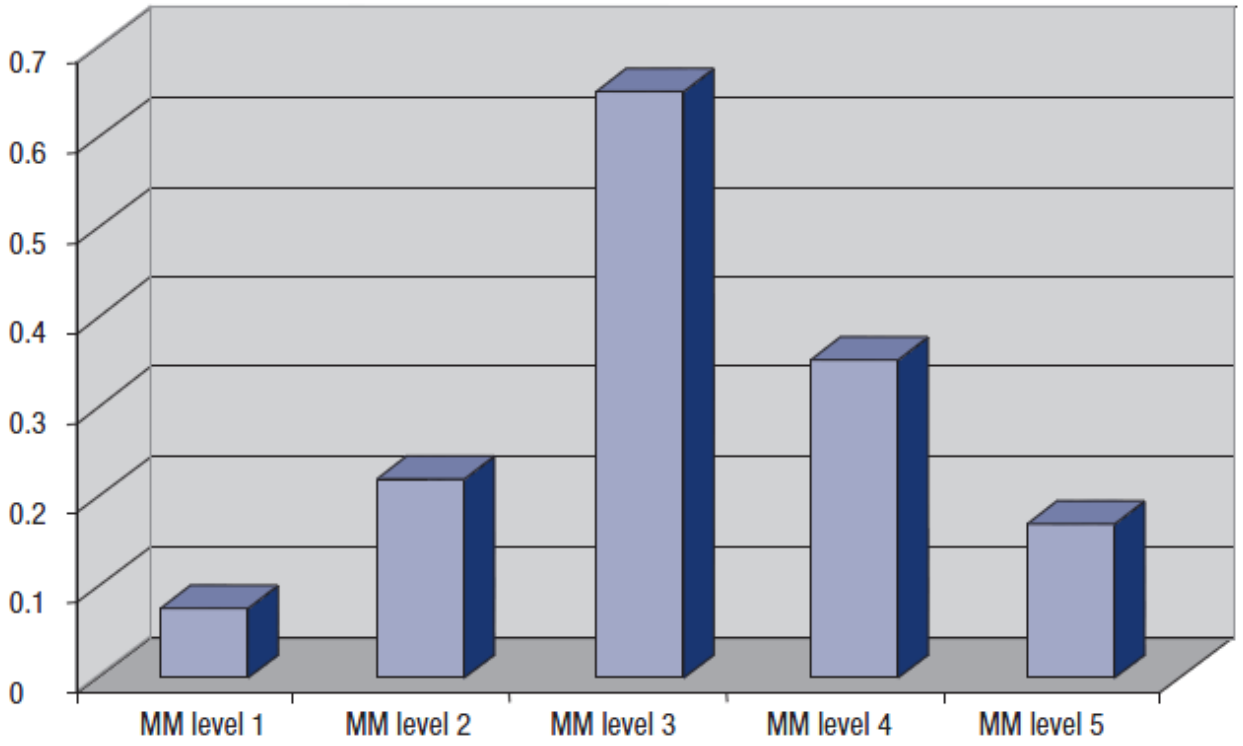
	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
1	Recognition of the need for the process is emerging. There is sporadic communication of the issues.	There are *ad hoc* approaches to processes and practices. The process and policies are undefined.	Some tools may exist; usage is based on standard desktop tools. There is no planned approach to the tool usage.	Skills required for the process are not identified. A training plan does not exist and no formal training occurs.	There is no definition of accountability and responsibility. People take ownership of issues based on their own initiative on a reactive basis.	Goals are not clear and no measurement takes place.
2	There is awareness of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitive because of individual expertise. Some aspects of the process are repeatable because of individual expertise, and some documentation and informal understanding of policy and procedures may exist.	Common approaches to use of tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelfware.	Minimum skill requirements are identified for critical areas. Training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	An individual assumes his/her responsibility and is usually held accountable, even if this is not formally agreed. There is confusion about responsibility when problems occur, and a culture of blame tends to exist.	Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.
3	There is understanding of the need to act. Management is more formal and structured in its communication.	Usage of good practices emerges. The process, policies and procedures are defined and documented for all key activities.	A plan has been defined for use and standardisation of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Skill requirements are defined and documented for all areas. A formal training plan has been developed, but formal training is still based on individual initiatives.	Process responsibility and accountability are defined and process owners have been identified. The process owner is unlikely to have the full authority to exercise the responsibilities.	Some effectiveness goals and measures are set, but are not communicated, and there is a clear link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard ideas are being adopted, as is occasional intuitive application of root cause analysis.
4	There is understanding of the full requirements. Mature communication techniques are applied and standard communication tools are in use.	The process is sound and complete; internal best practices are applied. All aspects of the process are documented and repeatable. Policies have been approved and signed off on by management. Standards for developing and maintaining the processes and procedures are adopted and followed.	Tools are implemented according to a standardised plan, and some have been integrated with other related tools. Tools are being used in main areas to automate management of the process and monitor critical activities and controls.	Skill requirements are routinely updated for all areas, proficiency is ensured for all critical areas, and certification is encouraged. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal domain experts are involved, and the effectiveness of the training plan is assessed.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions noted by management and root cause analysis is being standardised. Continuous improvement is emerging.
5	There is advanced, forward-looking understanding of requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied, and integrated communication tools are in use.	External best practices and standards are applied. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end management and improvement.	Standardised tool sets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions.	The organisation formally encourages continuous improvement of skills, based on clearly defined personal and organisational goals. Training and education support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture, and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Process owners are empowered to make decisions and take action. The acceptance of responsibility has been cascaded down throughout the organisation in a consistent fashion.	There is an integrated performance measurement system linking IT performance to business goals by global application of the IT balanced scorecard. Exceptions are globally and consistently noted by management and root cause analysis is applied. Continuous improvement is a way of life.

Figure 15—Maturity Attribute Table

Maturity Model Attribute Table, CobiT 4.1, ISACA 2007

Maturity Models

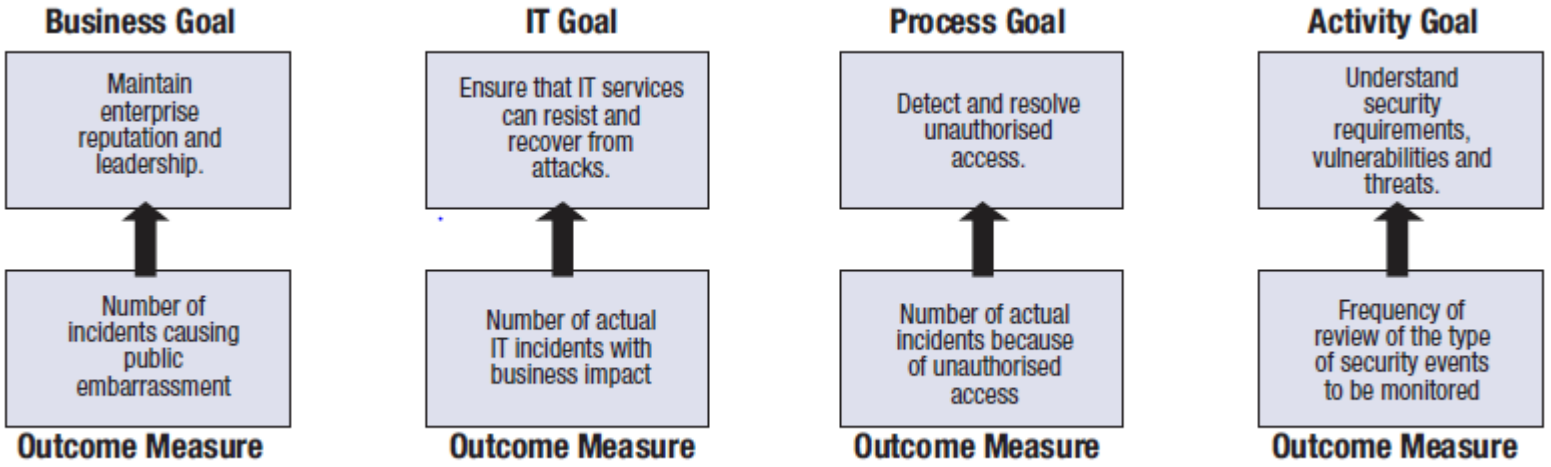
- Mögliche Klassifikation eines Prozess nach dem Reifegradmodell:



Maturity Beispielausprägung, CobiT 4.1, ISACA 2007

Outcome Measures und Performance Indicators

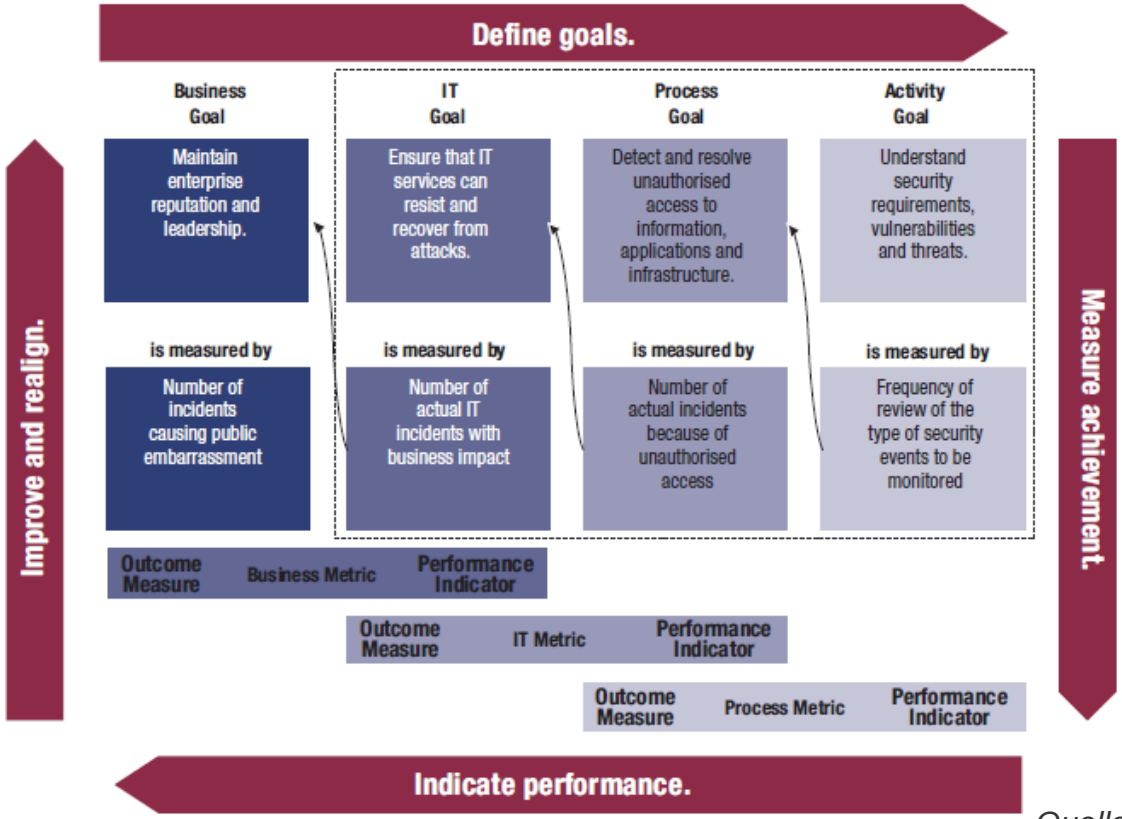
- Outcome Measures messen die Effektivität eines Goals
- Performance Indicators messen die Effizienz
- Zu jedem IT Goal, Process Goal und Activity Goal werden Outcome Measures angegeben



Outcome Measures des Prozesses DS5 Ensure systems security, CobiT 4.1, ISACA 2007

Zusammenhang Goals, Outcome Measures und Performance Indicators

- Outcome Measures messen die Performance des übergeordneten Goals

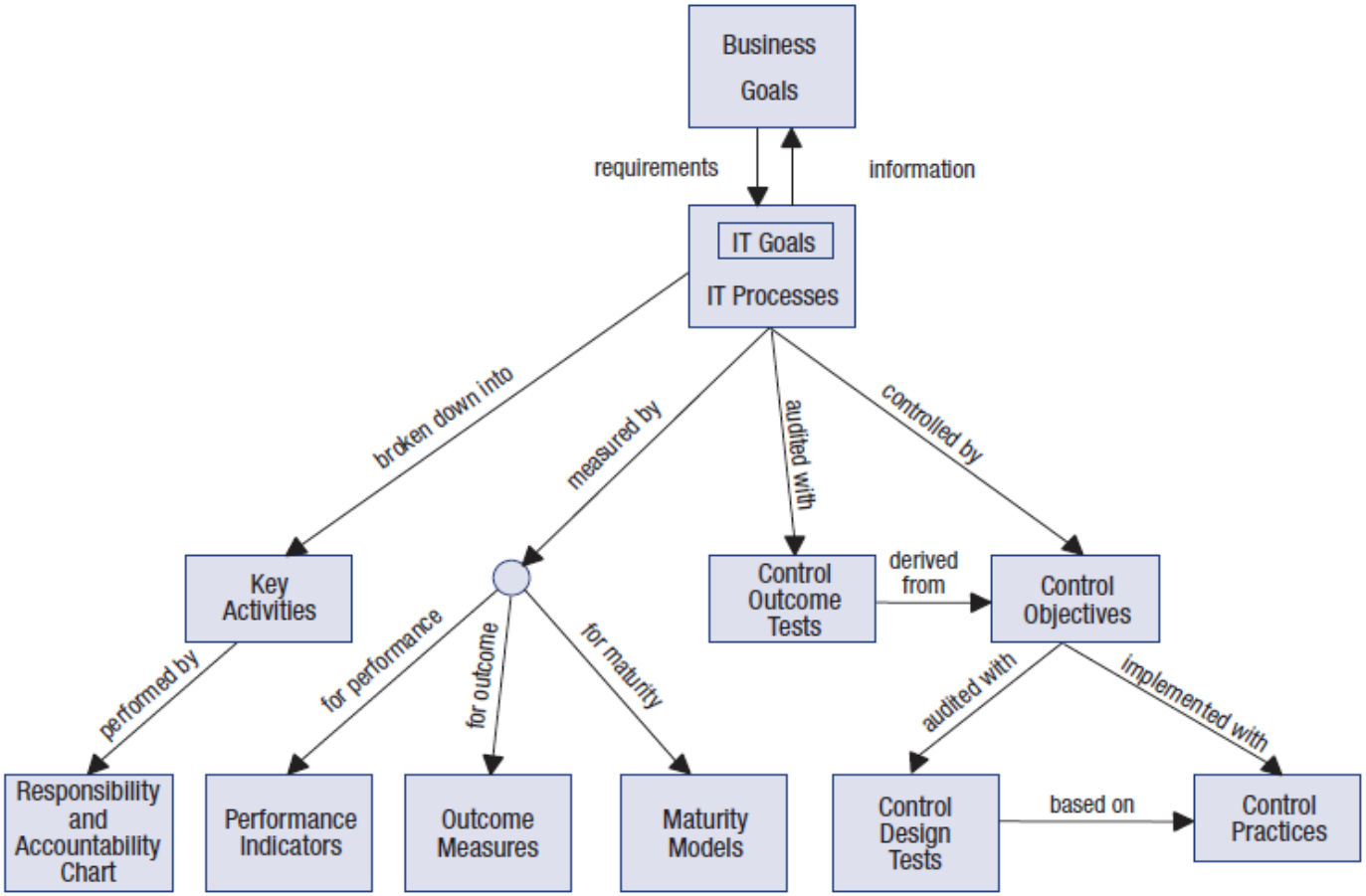


Quelle: CobiT 4.1, ISACA 2007

Beispielprozess: DS5 Ensure Systems Security

- CobiT_4.1.pdf

CobiT – Komponenten des Frameworks



Komponenten des CobiT Frameworks, [Co07]

Maturity Model Attribute Table, CobiT 4.1, ISACA 2007

CobiT in der Praxis

- 95% der amerikanischen Großunternehmen setzen CobiT ganz oder teilweise um (Quelle: ISACA Studie, 2008)
- Seit CobiT 3.0: CobiT Quickstart Guide für mittelständische Unternehmen
- Integration mit anderen Frameworks
  - Mapping of ITIL V3 With COBIT 4.1
  - Mapping of ISO/IEC 17799: 2005 With COBIT 4.0
  - COSO
  - …

Entwicklung und Ausblick

- 1993 von der ISACA (Information Systems Audit and Control Association) entwickelt
- Weiterentwicklung obliegt seit 2000 dem ITGI (IT Governance Institute)
- Aktuelle Version 4.1
- Ergebnis 15jähriger Forschung und Kooperation zw. Wirtschafts- und IT Experten
- Version 5.0 voraussichtlich 2011
  - Integration mit Val IT, IT Risk Management Framework

Quellen

- *[Co05] CobiT 4.0. Deutsche Version, ITGI 2005*
- *[Co07] CobiT 4.1, ITGI 2007*
- *[GH05] Van Grembergen, Wim and De Haes, Steven: COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade, ISACA 2005*
- *[Ga07] Technology Concerns to Management, Gartner Group 2007*
- http://www.monitor.co.at/index.cfm/storyid/11536_COBIT_in_der_Praxis-Messen_in_Prozess-Systemen, 17.07.2010
- http://www.itgovernance.co.uk/cobit.aspx , 17.07.2010
- http://en.wikipedia.org/wiki/Responsibility_assignment_matrix , 17.07.2010
- http://www.isaca.org/Journal/Past-Issues/2009/Volume-3/Pages/IT-Governance-and-Process-Maturity1.aspx , 17.07.2010
- http://www.isaca.org/Journal/Past-Issues/2009/Volume-3/Pages/Moving-From-IT-Governance-to-Enterprise-Governance-of-IT.aspx , 17.07.2010
- http://www.isaca.org/Journal/Past-Issues/2008/Volume-5/Pages/Implementing-Information-Technology-Governance-Models-Practices-and-Cases.aspx , 17.07.2010