IT GOVERNANCE

CobiT als Framework für die IT Governance

Als De-facto-Standard für IT Governance steht zunehmend CobiT® (Control Objectives for Information and related Technology) [1] im Vordergrund. CobiT wird beispielsweise auch von der Arbeitsgruppe IT Government Audit der Schweizerischen Finanzkontrollen empfohlen [2].

Im Verständnis von CobiT ist das Hauptziel der IT Governance, „die Anforderungen an die IT und ihre strategische Bedeutung zu verstehen, um den IT-Betrieb sicherzustellen und Strategien für eine auf die Unternehmensziele ausgerichtete Weiterentwicklung festzulegen“ [3]. Damit fasst IT Governance Aufgaben und Fragestellungen rund um die IT-Strategie und -Organisation, die Wertorientierung der IT, IT Sicherheit und IT Risiken sowie gesetzliche Vorgaben (Compliance) in einer gesamtheitlichen Sicht zusammen. Im Zusammenhang mit den seit Anfang 2008 im Art. 728a OR definierten Anforderungen an ein internes Kontrollsystem (IKS) sind die Themen IT Risikomanagement und Compliance von besonderer Aktualität.

Im Framework von CobiT setzt sich IT Governance mit vier Kernfragen auseinander:

Strategie:

- Entspricht die IT unserer Geschäftsvision und ist sie auf die strategischen Ziele ausgerichtet?
- Liefert die IT optimalen Nutzen bei angemessenen Kosten und akzeptablen Risiken?

Organisation:

- Passt die IT zu unserer Struktur und unserer Organisation?
- Unterstützt die IT die laufenden geschäftlichen Initiativen?

Umsetzung:

- Haben wir effektive Prozesse zur Umsetzung der IT-Vorhaben?
- Verfügen wir über die nötigen technischen und organisatorischen Ressourcen?

Kontrolle:

- Sind der angestrebte Nutzen und die verantwortlichen Stellen für seine Realisierung definiert?
- Wie messen und verfolgen wir den Nutzen über die Lebensdauer der Investition?

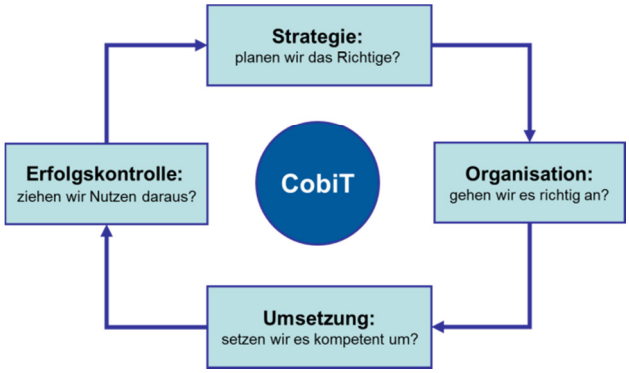

Abbildung 1: Kernthemen von CobiT

CobiT ist prozessorientiert aufgebaut, mit 34 Prozessen in 4 Prozess-Domains. Controlling wird als integrierter Teil dieser IT Prozesse betrachtet; aus den Aufgaben der IT Governance leiten sich auch die Controlling-Aufgaben („Control Objectives“ bzw. „Kontrollziele“ in CobiT) ab.

Bereiche der IT Governance

Unter dem Gesichtspunkt „Lebenszyklus von IT Investitionen“ lassen sich drei Teilbereiche der IT Governance abgrenzen:

Die **strategische IT Governance steuert** die IT Investitionen, stimmt Geschäfts- und IT Ziele miteinander ab (Alignment), legt die IT-Strategie und -Organisation fest, und definiert den Umgang mit IT Risiken (Stichwort IKS) und gesetzlichen Rahmenbedingungen (Compliance).

Die **Projekt-Governance überprüft** IT-Portfolios und IT-Projekte und stellt die zielkonforme Umsetzung der IT Investitionen sicher.

Betriebs-Governance überwacht die operative IT bezüglich Sicherheit, Integrität, Verfügbarkeit, Zuverlässigkeit, Wirksamkeit und Aufgabenerfüllung.

Diese drei Bereiche entsprechen inhaltlich den drei CobiT Prozess-Domains

- „Plan and Organize“;
- „Acquire and Implement“;
- “Deliver and Support”.

Der vierte Prozess-Domain, „Monitor and Evaluate”, ist für alle Governance Bereiche relevant. Abbildung 2 zeigt diese Zusammenhänge sowie mit CobiT kompatible weiterführende Richtlinien [4-5] und „Mappings“ zu „Best Practice“ Standards [6-11].

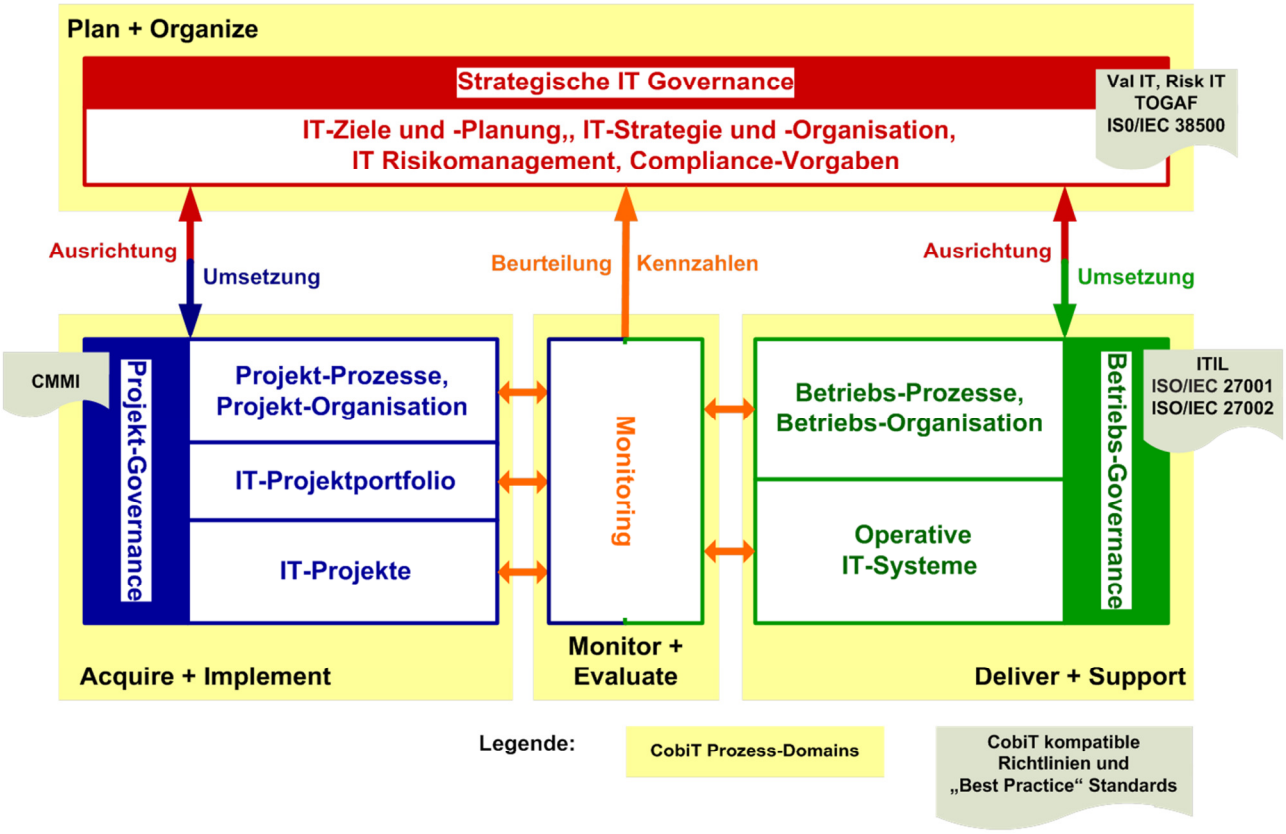

Abbildung 2: IT Governance Bereiche und CobiT

Governance und Controlling

IT Governance, Umsetzung, Monitoring und Controlling über einen Regelkreis miteinander verbunden:

- die Governance gibt die SOLL-Werte vor und ergreift bei Abweichungen von den IST-Werten korrigierende Massnahmen;
- die Umsetzung (in neuen Projekten oder im Betrieb) liefert Ergebnisse;
- das Monitoring misst die Ergebnisse in Form von definierten Kennzahlen;
- das Controlling beurteilt die Ergebnisse und schlägt ev. Handlungsoptionen für die Governance vor.

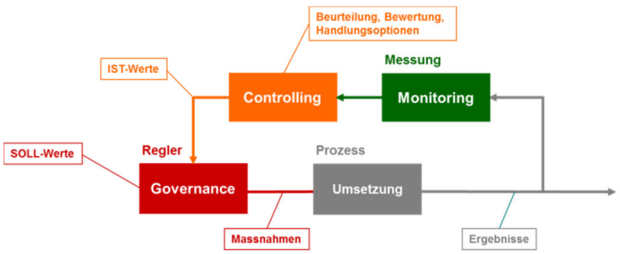

Abbildung 3: Controlling-Regelkreis

Das Controlling übernimmt damit eine Unterstützungsfunktion im Rahmen der Governance.

IT Controlling mit CobiT

Übersicht CobiT Prozesse

CobiT liegt ein gesamtheitliches, umfassendes Kontrollmodell zugrunde. Tabelle 4 zeigt im Detail, wie sich die CobIT Prozesse inhaltlich den drei Bereichen der IT Governance zuweisen lassen; daraus ergeben sich dann auch die jeweiligen Controlling-Aufgaben. Die Projekt-Governance wurde hier weiter unterteilt in Aufgaben auf Stufe IT-Projekte und IT-Portfolios.

Verschiedene Prozesse sind in mehreren Governance-Bereichen von Bedeutung, aber typischerweise in unterschiedlicher inhaltlicher Ausprägung (andere Prozessaktivitäten, Inputs und Outputs, Metriken).

Tabelle 4 zeigt auch die Wichtigkeit der Prozesse (gemäss CobiT - je nach Organisation können die Schwerpunkte anders sein).

CobiT Prozesse / Controlling-Themen	Projekt-Governance		Strategische IT Governance	Betriebs-Governance	Wichtigkeit
	IT Projekte	IT Portfolio			
Plan and Organise					
PO1 Define a strategic IT plan.					**H**
PO2 Define the information architecture.					L
PO3 Determine technological direction.					**M**
PO4 Define the IT processes, organisation and relationships.					L
PO5 Manage the IT investment.					**M**
PO6 Communicate management aims and direction.					**M**
PO7 Manage IT human resources.					L
PO8 Manage quality.					**M**
PO9 Assess and manage risks.					**H**
PO10 Manage projects.					**H**
Acquire and Implement					
AI1 Identify automated solutions.					**M**
AI2 Acquire and maintain application software.					**M**
AI3 Acquire and maintain technology infrastructure.					L
AI4 Enable operation and use.					L
AI5 Procure IT resources.					**M**
AI6 Manage changes.					**H**
AI7 Install and accredit solutions and changes.					**M**
Deliver and Support					
DS1 Define and manage service levels.					**M**
DS2 Manage third-party services.					L
DS3 Manage performance and capacity.					L
DS4 Ensure continuous service.					**M**
DS5 Ensure systems security.					**H**
DS6 Identify and allocate costs.					L
DS7 Educate and train users.					L
DS8 Manage service desk and incidents.					L
DS9 Manage the configuration.					**M**
DS10 Manage problems.					**M**
DS11 Manage data.					**H**
DS12 Manage the physical environment.					L
DS13 Manage operations.					L
Monitor and Evaluate					
ME1 Monitor and evaluate IT performance.					**H**
ME2 Monitor and evaluate internal control.					**M**
ME3 Ensure compliance with external requirements.					**H**
ME4 Provide IT governance.					**H**
					H = hoch, **M** = mittel, L = tief

Tabelle 4: Mapping der CobIT Prozesse auf Governance Bereiche

Controlling-Themen

Während konventionelles IT Projektcontrolling auf die Einhaltung von **Zielen** in den Projektdimensionen Ergebnisse, Kosten, Termine und die Beachtung interner und externer Einflussfaktoren wie Risiken, Ressourcen etc. fokussiert ist, zielt das Controlling mit CobiT zusätzlich auf die Einhaltung von **Prozessaktivitäten**. Es kann auf einen oder mehrere Governance Bereiche angewendet werden.

Beim Controlling von **IT-Projekten** vertieft und erweitert CobiT den Kontrollumfang. Neben dem Projektstatus (Ergebnisse, Kosten, Termine) werden auch das Projektvorgehen (u.a. Qualitätssicherung, Risikomanagement) und die IT Prozesse bei der Projektabwicklung beurteilt. Basis für die Überprüfung der Ergebnisse sind die definierten Metriken und Kennzahlen.

Für das Controlling von **IT-Portfolios** wird in CobiT ein Projekt-/Programmmanagement-Framework vorausgesetzt, welches das Projektvorgehen, die IT Prozesse und den organisatorischen Rahmen festlegt. CobiT enthält dafür ein konkretes Modell, das Vorgaben der strategischen IT Governance umsetzt, und auf gemeinsamen Metriken für alle IT-Projekte aufbaut. Dadurch lässt sich der Projekterfolg messen und steuern, und ein Quervergleich der Projekte wird möglich.

Im Bereich **Betriebs-Governance** legt CobiT ein eigenes Prozessmodell zugrunde, das alle Betriebs- und Support-Aufgaben abdeckt. Die Prozesse sind ähnlich definiert wie im verbreiteten ITIL-Modell, und es besteht ein Mapping zwischen den beiden Modellen [10].

Bei der **Strategischen IT Governance** steht die Wertorientierung der IT im Vordergrund [4]. CobiT definiert geeignete Planungsprozesse (Strategische IT Planung, Informations-Architektur, Technologie-Standards), Führungsgrundlagen (IT Projekt Portfolio, IT Prozess Framework, IT Organisation mit dokumentierten Rollen und Verantwortlichkeiten) und Methoden zur Messung und Beurteilung der Ergebnisse von IT-Projekten und vom IT-Betrieb.

Tailoring des Kontrollumfangs

Für viele Organisationen wäre eine integrale Umsetzung von CobiT für die IT Governance zu aufwändig und nicht zielführend. Je nach den Zielsetzungen und Bedürfnissen einer Organisation sind aber ausgewählte Teile von CobiT von Interesse. Tailoring bestimmt diese Teilmenge. Zu empfehlen ist ein 2-stufiges Vorgehen:

1. Auswahl der Prozesse (Breite)

Ausgangspunkt kann das Mapping in Tabelle 5 sein. Der Anhang von CobiT [1] enthält weitere Mappings nach den Kriterien Governance Fokus, kritische IT Ressourcen, Geschäftsanforderungen sowie Technologie. Dadurch lassen sich die zu betrachtenden CobiT Prozesse, ausgerichtet auf die konkreten Gegebenheiten und Schwerpunkte einer Organisation, bereits auf grober Ebene reduzieren.

2. Grad der Umsetzung (Tiefe)

In der zweiten Stufe erfolgt für jeden betrachteten Prozess eine auf die detaillierten Anforderungen abgestimmte inhaltliche Beschränkung der Controlling-Themen. Sie umfasst

- die Auswahl der Kontrollziele;
- die zu erstellenden Outputs;
- die zu erhebenden Metriken.

Dies ergibt ein Controllingsystem für die IT Governance mit massgeschneidertem Umfang.

Die Tabellen 5 und 6 zeigen die 2 Tailoring-Stufen beispielhaft für eine öffentliche Verwaltung mit wenigen IT-Projekten, extern entwickelten Lösungen, und mit in ein Rechenzentrum ausgelagertem Betrieb.

Tailoring CobiT Prozesse	Projekt-Governance	Strategische IT Governance	Betriebs-Governance	Wichtigkeit
Plan and Organise				
PO1 Define a strategic IT plan.				**M**
PO5 Manage the IT investment.				**H**
PO9 Assess and manage risks.				**M**
PO10 Manage projects.				**H**
Acquire and Implement				
AI2 Acquire and maintain application software.				**M**
AI6 Manage changes.				**M**
Deliver and Support				
DS1 Define and manage service levels.				**H**
DS2 Manage third-party services.				**M**
DS11 Manage data.				**M**
Monitor and Evaluate				
ME1 Monitor and evaluate IT performance.				**H**
				H = hoch, **M** = mittel

Tabelle 5: Beispiel Tailoring Controllingprozesse

Tailoring Kontrollziele			Kontroll-ziele (*)	Resultate, Dokumente
PO1		**Define a strategic IT plan**		
PO1	1	IT value management	NEIN	
PO1	**2**	**Business-IT alignment**	**JA**	
	3	Assessment of Current Capability and Performance	NEIN	
PO1	**4**	**IT strategic plan**	**JA**	**Strategic IT plan**
PO1	5	IT tactical plans	NEIN	Tactical IT plans
PO1	6	IT portfolio management	NEIN	IT project portfolio, IT service portfolio
PO10		**Manage projects**		
PO10	1	Programme management framework	NEIN	Updated IT project portfolio
PO10	**2**	**Project management framework**	**JA**	**Project management guidelines**
PO10	3	Project management approach	NEIN	
PO10	4	Stakeholder commitment	NEIN	
PO10	**5**	**Project scope statement**	**JA**	
PO10	6	Project phase initiation	NEIN	
PO10	**7**	**Integrated project plan**	**JA**	**Detailed project plans**
PO10	8	Project resources	NEIN	
PO10	**9**	**Project risk management**	**JA**	**Project risk management plan**
PO10	10	Project quality plan	NEIN	
PO10	**11**	**Project change control**	**JA**	
PO10	12	Project planning of assurance methods	NEIN	
PO10	**13**	**Project performance measurement, reporting and monitoring**	**JA**	**Project performance reports**
PO10	14	Project closure	NEIN	

Tabelle 6: Beispiel Tailoring Kontrollziele

(*) JA/NEIN bei den Kontrollzielen bezieht sich nicht auf das Vorliegen eines entsprechenden Lieferobjekts, sondern seine Prüfung; typischerweise werden weitere Lieferobjekte vorliegen.

In der Praxis wird mit dem Tailoring ein dem angestrebten „Minimal-Standard“ im Projektmanagement entsprechender Prüfraster definiert.

Fazit

Das Framework von CobiT bietet einen gesamtheitlichen Ansatz zur Sicherstellung der IT Governance, der alle Governance Bereiche abdeckt. Es werden aber ausgebaute IT Prozesse und damit ein relativ hoher Reifegrad der IT Organisation vorausgesetzt.

Eine integrale Umsetzung von CobiT kommt deshalb eher für grosse Organisationen mit hohen Ansprüchen an die Governance in Frage. CobiT basiertes IT Controlling sollte aber wie jede Methode pragmatisch angewendet werden. Mit geeignetem Tailoring des Kontrollumfangs und Beschränkung auf bestimmte Governance Bereiche passt CobiT auch für kleinere Organisationen.

Zwei besondere Stärken von CobiT sind dabei der wertorientierte Blickwinkel im Bereich Strategische IT Governance und beim Controlling von IT-Portfolios, und die gesamtheitliche Sicht beim Risikomanagement.

Endnotes

[1] ISACA, COBIT Framework for IT Governance and Control, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[2] Empfehlungen der Schweizerischen Finanzkontrollen für Informatikprojekte, http://www.efk.admin.ch

[3] ITIG, IT Governance für Geschäftsführer und Vorstände, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT Governance-2nd-Edition.aspx

[4] ISACA, Val IT Framework for Business Technology Management, http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx

[5] Risk IT Framework for Management of IT Related Business Risks, http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx

[6] ISO 38500, International Standard for Corporate Governance of IT, http://www.iso.org

[7] The Open Group, TOGAF Framework for Enterprise Architecture Development, http://www3.opengroup.org/standards

[8] Software Engineering Institute, Capability Maturity Model Integration (CMMI), http://www.sei.cmu.edu/cmmi

[9] ITIL, V3 best practice framework for IT service management, www.itil-officialsite.com

[10] ISACA, COBIT Mapping of ITIL V3 With COBIT 4.1, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Mapping-Mapping-of-ITIL-V3-With-COBIT-4-11.aspx

[11] ISO/IEC 27001:27002, International Standard for Information Security Management, http://www.iso.org/iso/iso_catalogue.htm