

2 Entwicklung und Bedeutung von COBIT

Diese Kapitel stellt die Entwicklung des COBIT-Rahmenwerks sowie der komplementierenden Rahmenwerke Val IT und Risk IT und die Rolle des internationalen Verbandes ISACA und seiner Forschungseinrichtung, dem IT Governance Institute, dar.

2.1 ISACA und das IT Governance Institute

Die Information Systems Audit and Control Association (ISACA) ist heute ein internationaler Verband von IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Experten. Primäres Ziel des Verbandes ist die Verbreitung von Berufsstandards und Arbeitstechniken sowie die Zertifizierung und Weiterbildung von Fachleuten, die sich mit der Kontrolle und der Sicherheit sowie dem Management und der Steuerung von Informationssystemen befassen.

Der Verband, dem zum Zeitpunkt der Entstehung dieses Buches über 82.000 Mitglieder weltweit angeschlossen waren, wurde ursprünglich 1969 als Berufsverband der IT-Revisoren – EDP Auditors Association (EDPAA) – gegründet. 1976 wurde von der EDPAA eine Forschungseinrichtung, die »EDP Auditors Foundation« (EDPAF) gegründet, die größere Forschungsvorhaben aus der Mitgliederorganisation herausgelöst vornehmen sollte. Erst 1994 erhielt der Verband seinen heutigen Namen: »Information Systems Audit and Control Association«. Die Forschungseinrichtung wurde entsprechend in »Information Systems Audit and Control Foundation« (ISACF) umbenannt. 1998 wurde von der ISACA zusätzlich das »IT Governance Institute« (ITGI) als Forschungseinrichtung auf dem Gebiet der Informationsrevision und des Informationsmanagements gegründet. Damit erweiterte sich auch der Fokus des Berufsverbandes von der IT-Revision über das IT-Management bis hin zur IT-Governance. Im Jahr 2003 wurde die ISACF auf das ITGI verschmolzen, sodass das ITGI der alleinige Herausgeber der Rahmenwerke COBIT und Val IT ist. Risk IT wurde im November 2009 unter der Herausgeberschaft von ISACA veröffentlicht. Damit trägt der Berufs-

verband ISACA der inzwischen erreichten Anerkennung des Berufsverbandes über die IT-Prüfung hinaus Rechnung.

ISACA ist in über 170 lokalen Chaptern organisiert, die in über 70 Ländern vertreten sind. In Deutschland hatte das German Chapter Ende Juli 2009 genau 1.622 Mitglieder und war damit das siebtgrößte Chapter weltweit. In der Schweiz waren dem Switzerland Chapter zu diesem Zeitpunkt 981 Mitglieder angeschlossen und in Österreich waren dem Austria Chapter 279 Mitglieder verbunden. Die lokalen Chapter bieten spezifische Fachinformationen, Weiterbildungs- und Qualifizierungsmaßnahmen sowie Veranstaltungen an, damit sich die Mitglieder fortbilden und besser vernetzen können.

Weltweite Anerkennung haben auch die Zertifizierungen der ISACA gefunden. Die seit 1978 bestehende Zertifizierung zum Certified Information Systems Auditor (CISA) wurde inzwischen über 70.000 Personen verliehen, die seit 2003 bestehende zum Certified Information Security Manager (CISM) über 11.000 Personen und die jüngste Zertifizierung zum Certified in the Governance of Enterprise IT (CGEIT) wird ebenfalls bereits gut angenommen.

2.2 Entstehung von COBIT, Val IT und Risk IT

Basis von COBIT war ein Standardwerk, in dem das Wissen und der Erfahrungsschatz des Berufsstandes der IT-Revisoren gebündelt war: »Control Objectives – Controls in an Information Systems Environment: Objectives, Guidelines und Audit Procedures«. Dieses Werk wurde bereits im Jahr 1976 erstmals von der EDPAF (später ISACF) herausgegeben und von dieser ständig weiterentwickelt. Im April 1992 erschien die vierte und letzte Ausgabe [EDPAF 1992], in der die allgemeinen IT-Kontrollen in Kontrollen

- des Managements (management controls),
- der IT-Systementwicklung, Beschaffung und Wartung (information system development, acquisition, and maintenance controls) sowie
- des Betriebs (information system operations controls)

gegliedert worden sind, was bereits im Wesentlichen der Domänenstruktur von COBIT entsprach. Daneben gab es noch eine Darstellung der Anwendungskontrollen (application controls) sowie einen eigenen Abschnitt mit technologieorientierten Kontrollen (technology specific controls). Letzterer ist aufgrund seiner Technikorientierung nicht in das Rahmenwerk COBIT eingeflossen.

Seit dem Jahr 1993 wurde an einem neuen Rahmenwerk gearbeitet. Dazu wurde ein internationales Gremium der ISACA (COBIT Steering Committee) eingesetzt, das die erste Version von COBIT entwickeln sollte. Dies geschah in Zusammenarbeit mit der Free University of Amsterdam, der California Polytechnic University und der University of New South Wales. Die erste Version von COBIT wurde im April 1996 von der damaligen ISACA-Forschungseinrichtung

ISACF (Information Systems Audit and Control Foundation) veröffentlicht. COBIT umfasste damals 32 Prozesse mit 271 detaillierten control objectives [ISACF 1996]. Zum Zeitpunkt der Veröffentlichung waren die nächsten Schritte der Weiterentwicklung bereits klar definiert. Die control objectives sollten nochmals auf Basis weiterer Referenzmaterialien überarbeitet werden und vor allem sollten noch Richtlinien zur Selbsteinschätzung und Metriken für das Management entwickelt werden. Im April 1998 erschien die überarbeitete und erweiterte zweite Version mit 302 detaillierten control objectives in 34 Prozessen [ISACF 1998] sowie einem zusätzlichen »Implementation Tool Set«, bestehend aus einer Anleitung zur Implementierung von COBIT und unterstützenden Materialien.

Das Rahmenwerk wurde anfangs hauptsächlich von der internen und externen Revision verwendet, da COBIT für das ganze Spektrum der IT-Aktivitäten eines Unternehmens homogene Anforderungen (control objectives) als »Good Practices« beschrieben hatte, die als Sollvorgaben zur Beurteilung der Situation in der geprüften Einheit verwendet werden konnten. Weiterhin wurden detaillierte Prüfungshandlungen zu den Prozessen in separaten »Audit Guidelines« beschrieben.

Um das Potenzial von COBIT, sich auch zu einem Rahmenwerk für das IT-Management und das Business Management zu entwickeln, besser zu unterstützen, wurde von der ISACA im Jahr 1998 das IT Governance Institute gegründet und die Entwicklung von COBIT dort angesiedelt. Im Juli 2000 wurde COBIT in der dritten Auflage vor allem um Aspekte des IT-Managements durch die sog. »Management Guidelines« erweitert. Diese umfassten ein Reifegradmodell (maturity model), kritische Erfolgsfaktoren (critical success factors) sowie wesentliche Zielindikatoren (key goal indicators) und Leistungsindikatoren (key performance indicators). Damit wurden in COBIT Kriterien integriert, um dem Management zu ermöglichen, den Status und die Effektivität der eigenen IT-Prozesse im Hinblick auf die 34 übergeordneten Prozessbereiche und die 318 detaillierten control objectives beurteilen zu können, einen Sollzustand zu definieren, die notwendigen Schritte zur Erreichung des gewünschten Sollzustandes festzulegen und die Zielerreichung zu überwachen [ITGI 2000].

Nach Erscheinen der dritten Auflage haben die Unternehmen COBIT zunehmend sowohl als Leitfaden bei der Implementierung des internen Kontrollsystems in der Unternehmens-IT als auch für die Durchführung von Prozesszustandsbeurteilungen in Form von »Self-Assessments« oder »Health Checks« angewandt.

Im Jahr 2004 starteten die Entwicklungsarbeiten an der nächsten Version von COBIT mit der Integration von diversen Forschungsprojekten, u.a. von der Antwerp Management School und der University of Hawaii. Im Dezember 2005 kam die Version 4.0 heraus, die vor allem eine deutliche Verschlankung und Reduzierung der control objectives auf 215 bedeutete und auch explizit die Aspekte der IT-Governance integrierte [ITGI 2005g]. In der Folge wurde COBIT 4.0 nochmals in einigen Details überarbeitet und zusammen mit ergänzenden Büchern – wie den COBIT Control Practices [ITGI 2007b], dem IT Governance Implementation Guide: Using COBIT and Val IT [ITGI 2007c] sowie dem IT Assurance

Guide: Using COBIT [ITGI 2007d] – im Mai 2007 in der Version COBIT 4.1 veröffentlicht [ITGI 2007a].

Das IT Governance Institute erachtete dieses Paket sich ergänzender und aufeinander referenzierender Bücher als weitgehend stabil und konzentrierte seine Forschungsbemühungen seitdem auf COBIT und die IT-Governance-Ansätze ergänzende Produkte.

Parallel dazu begann die Entwicklung am Rahmenwerk Val IT, das im Jahr 2006 erstmals veröffentlicht wurde [ITGI 2006e]. Die zweite, besser mit COBIT integrierte Version erschien im Jahr 2008 [ITGI 2008b]. In diesem Jahr startete auch die Entwicklung des jüngsten Rahmenwerks der ISACA: Risk IT. Dieses erschien erstmals im Entwurf im Mai 2009 und in der endgültigen Version im November 2009 [ISACA 2009a].

Zum Zeitpunkt der Erstellung dieses Buches wurde gerade wieder begonnen, über eine Weiterentwicklung von COBIT nachzudenken, und eine entsprechende Task Force ins Leben gerufen.

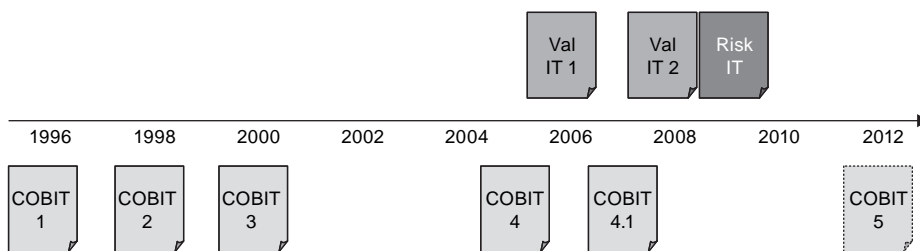


Abb. 2-1 Entwicklung von COBIT, Val IT und Risk IT

Der Zeitstrahl in Abbildung 2-1 verdeutlicht die Entwicklung der drei Rahmenwerke COBIT, Val IT und Risk IT seit dem Jahr der Erstveröffentlichung von COBIT. Ob die nächste Version von COBIT die Nummer 5 trägt und ob diese im Jahr 2012 herauskommen wird, darüber kann natürlich nur spekuliert werden.

2.3 Anspruch von COBIT

COBIT (Control Objectives for Information and Related Technology) ist ein Rahmenwerk für das Management und die Überwachung und Steuerung der IT. COBIT beinhaltet ein Prozessmodell mit generell anwendbaren und international akzeptierten IT-prozessbezogenen Anforderungen (control objectives), die in einem Unternehmen beachtet und umgesetzt werden sollten, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten. Die Idee dahinter: Erst wenn Informationen, Anwendungen, Infrastruktur und Menschen richtig organisiert sind, werden die Geschäftsprozesse die an sie gestellten Anforderungen erfüllen.

Die control objectives sind nach einem alle IT-Funktionen umfassenden Prozessmodell strukturiert. Dieses unterscheidet innerhalb der Funktion Informationstechnologie 34 Prozesse, die jeweils einem der vier nachfolgend aufgelisteten Bereiche oder Domänen (domains) zugeordnet sind:

- Planen und Organisieren
- Beschaffen und Implementieren
- Erbringen und Unterstützen
- Überwachen und Beurteilen

Für jeden der 34 IT-Prozesse formuliert COBIT zwischen drei und 15 normative Aussagen (control objectives). Werden die 210 in COBIT 4.1 enthaltenen control objectives konsequent umgesetzt, kann damit eine geordnete Planung, Beschaffung, Abwicklung und Überwachung aller in den IT-Prozessen eingesetzten IT-Ressourcen sichergestellt werden.

Als prozessorientiertes Modell ist COBIT unabhängig von der eingesetzten Technologie oder der Branche des Unternehmens und lässt sich unabhängig vom jeweiligen geschäftlichen und technischen Umfeld anwenden.

COBIT richtet sich nicht nur an IT-Fachleute, sondern stellt über die Ausrichtung an die Geschäftsprozesse auch den Geschäftsprozesseigentümern ein Rahmenwerk für das Management der IT sowie dem Topmanagement durch die vorhandenen Prozessmerkmale und -kennzahlen ein ganzheitliches IT-Governance-Modell zur Verfügung.

COBIT hat sich auch international als anerkanntes Rahmenwerk für das interne Kontrollsystem in der Informationstechnologie etabliert. COBIT wurde inzwischen sowohl von namhaften Unternehmen in das eigene interne Kontrollsystem integriert (u.a. von Daimler, Philips) als auch von Behörden (u.a. vom amerikanischen Verteidigungsministerium, vom European Agricultural Guidance and Guarantee Fund (EAGGF)) und anderen Institutionen (u.a. META-Group, Gartner) als Standard empfohlen.

Als offener Standard steht ein Großteil von COBIT zum kostenfreien Download auf der Webseite des IT Governance Institute (<http://www.itgi.org>) und auf der Webseite der ISACA (<http://www.isaca.org/cobit>) bereit.

2.4 COBIT-Produktfamilie

Die COBIT-Produktfamilie ist in den letzten Jahren immer größer geworden. Wichtig ist es jedoch, zwischen den vier Kernbüchern und den weiteren dem Umfeld von COBIT zugehörigen (related) Werken zu differenzieren. Das vorliegende Buch fokussiert vor allem auf die Inhalte der Kernbücher, behandelt jedoch auch die Bücher der erweiterten COBIT-Produktfamilie.

COBIT-Kernbücher	Inhalte	Anwendungsbeispiele
COBIT 4.1 [ITGI 2007a]	Rahmenwerk für das Management und die Governance der IT mit Control Objectives, Management Guidelines und Reifegradmodellen	<ul style="list-style-type: none"> ■ Aufgaben und Verantwortlichkeiten festlegen ■ Verlässlichkeit der IT-Prozesse erhöhen ■ Internes IT-Kontrollsystem etablieren ■ Richtlinien erstellen
COBIT Control Practices [ITGI 2007b]	Hinweise, wie jedes Control Objective umgesetzt werden kann	<ul style="list-style-type: none"> ■ Konzeption von konkreten Kontroll- und Steuerungsmaßnahmen
IT Governance Implementation Guide: Using COBIT and Val IT [ITGI 2007c]	Vorgehensmodell und Prozessbeschreibungen zur Umsetzung von IT-Governance-Vorhaben	<ul style="list-style-type: none"> ■ Einrichtung eines COBIT-basierten IT-Governance-Rahmenwerks ■ Geschäftsrelevante Prozessverbesserungen in der IT umsetzen
IT Assurance Guide: Using COBIT [ITGI 2007d]	Vorgehensmodell für eine strukturierte Prüfungsdurchführung	<ul style="list-style-type: none"> ■ Erstellung einer Prüfungsplanung ■ Prüfung von IT mithilfe von COBIT

Tab. 2-1 COBIT-Kernbücher des IT Governance Institute

Die in Tabelle 2-1 aufgeführten Kernbücher sind nach und nach mit den COBIT-Versionen entstanden, sind aber seit COBIT 3 vollständig vorhanden. Für die Version COBIT 4.1 wurden alle vier Kernbücher komplett überarbeitet und auch in der Namensgebung der Neuausrichtung von COBIT 4 angepasst. Insbesondere seit der Version 3 von COBIT sind darüber hinaus weitere COBIT-bezogene Bücher vom IT Governance Institute für bestimmte Zielgruppen und Anwendungssituationen veröffentlicht worden. Tabelle 2-2 enthält eine Übersicht der Inhalte und der typischen Anwendungsgebiete der Bücher der erweiterten COBIT-Produktfamilie.

COBIT-Bücher	Inhalte	Anwendungsbeispiele
Board Briefing on IT Governance [ITGI 2003]	Beschreibung der wesentlichen IT-Governance-Konzepte	■ Anstoß zur Initiierung und nachhaltigen Einrichtung eines IT-Governance-Programms
IT Control Objectives for Sarbanes-Oxley [ITGI 2006a]	Beschreibung von Maßnahmen zur Einhaltung der Anforderungen von SOX im IT-Bereich	■ Einrichtung und Prüfung von SOX-Kontrollen im IT-Bereich
IT Control Objectives for Basel II [ITGI 2007g]	Beschreibung von Maßnahmen zur Einhaltung der Anforderungen von Basel II im IT-Bereich	■ Einrichtung von Kontrollen im IT-Bereich zur Reduzierung der Eigenkapitalanforderungen aus dem operationellen Risiko
Information Security Governance [ITGI 2006f]	Beschreibung von wesentlichen Elementen der Informationssicherheit	■ Anstoß zur Aufdeckung von sicherheitsbezogenen Problemen
COBIT Security Baseline [ITGI 2007i]	Einfache Darstellung von IT-Sicherheitsrisiken und entsprechender Maßnahmen	■ Schnelle Einführung der Kernelemente zur IT-Sicherheit
COBIT Quickstart [ITGI 2007h]	Zusammengefasste, vereinfachte Version von COBIT	■ Erste und schnelle Einführung der Kernelemente von COBIT
Val IT [ITGI 2008b]	Rahmenwerk für die Governance von IT-bezogenen Investitionen	■ Governance und Management des unternehmensweiten Portfolios der IT-bezogenen Investitionen
Risk IT [ISACA 2009a]	Rahmenwerk für die Governance von IT-bezogenen Risiken	■ Governance und Management von IT-bezogenen Unternehmensrisiken
The Risk IT Practitioner Guide [ISACA 2009b]	Leitfaden zur Anwendung von Risk IT	■ Management von IT-bezogenen Unternehmensrisiken

Tab. 2-2 Übersicht der weiteren COBIT-Bücher von ISACA und IT Governance Institute

Die in Tabelle 2-2 aufgeführten COBIT-bezogenen Bücher stellen die Anwendung des COBIT-Rahmenwerks für spezielle Zwecke dar oder referenzieren auf COBIT bei der Behandlung eines IT-Governance-bezogenen Themenbereichs. Alle Dokumente der COBIT-Produktfamilie stehen ISACA-Mitgliedern auf der Internetseite www.isaca.org kostenfrei als PDF-Dateien zum Download zur Verfügung gestellt. Weiterhin bietet ISACA die Dokumente größtenteils auch als gedruckte Versionen zum Kauf an.

Neben diesen Büchern ist auf der Internetseite der ISACA noch eine Vielzahl von weiteren Publikationen von der ISACA und dem IT Governance Institute veröffentlicht, die spezielle Themen im Umfeld von IT-Governance und IT-Management aufgreifen. Diese gehören im Sinne dieses Buches jedoch nicht zur engeren oder erweiterten COBIT-Produktfamilie.