d-fine

IT-Governance mit COBIT ® 2019

Rückschau und Ausblick nach 5 Jahren

analytisch. technologisch. quantitativ.

Mai 2024

Inhalt

IT-Governance mit COBIT ® 2019, Mai 2024

1. Die IT auf der Suche nach Orientierung Seite 3

2. Mit dem ersten Eindruck wird gepunktet Seite 3

3. COBIT überzeugt das Management Seite 5

4. Der Weg zur erfolgreichen Einführung Seite 6

5. COBIT wächst und gedeiht Seite 7

01. Die IT auf der Suche nach Orientierung

IT-Governance und -Management dient in Unternehmen dazu, IT zu organisieren, IT-Verantwortlichkeiten festzulegen, IT-bezogene Verhaltensweisen und -Abläufe zu koordinieren und zu steuern und damit einen Mehrwert für das gesamte Unternehmen zu schaffen. Im Idealfall wird dieser Mehrwert durch gutes Management im Laufe der Zeit optimiert.

Diese Zielsetzung ins Auge fassend könnte nun jeder CIO vorangehen und jeder für sich die IT nach seinem eigenen Geschmack organisieren. Doch halt! IT wäre nicht IT, wenn es nicht auch für diesen Fall entsprechende Standards gäbe. Und tatsächlich gibt es diese Standards, doch leider nicht nur einen. So tummeln sich im Zoo der Standards für IT-Governance und -Management Begriffe wie ITIL, CMMI, TOGAF, NIST, diverse ISO-Standards, PMBOK, usw. Diese setzen in aller Regel Maßstäbe für einen Teil oder auch für mehrere Teile der Themen, mit denen man sich in der IT beschäftigt. Ein Standard sticht dabei jedoch besonders hervor, weil er den Anspruch erhebt, ganzheitlich zu sein und eine Klammer um alle anderen Standards bilden zu wollen. Das ist COBIT.

COBIT ist ein von der internationalen Vereinigung der IT-Auditoren, der ISACA, herausgegebener Standard, welcher nach langjähriger Vorgeschichte in der momentanen Version seit fünf Jahren unverändert vorliegt. Die grundlegenden Dokumente von COBIT stehen kostenfrei bei der ISACA zum Download zur Verfügung.

Auf Grund des umfassenden, d.h. ganzheitlichen Ansatzes eignet sich eine Auseinandersetzung mit COBIT insbesondere für Unternehmen, die sich die folgenden Fragen stellen:

- Haben wir an alles gedacht, als wir unsere IT organisiert haben?
- Tun wir in der IT alles so, wie es andere Unternehmen auch tun? Und wenn ja, wollen wir es auch so machen oder wenn nein, warum nicht?
- Warum tun wir uns so schwer unsere gesetzten IT-Ziele zu erreichen?

Eine Beschäftigung mit COBIT ist also für die meisten Unternehmen in einer gewissen Phase ihrer Entwicklung lohnend. Allerdings ist COBIT kein einfaches Kochrezept, welches nach schrittweiser Anwendung zu einem gewünschten Ergebnis führt. COBIT verlangt vielmehr ein hohes Maß an Erfahrung und Augenmaß bei der Nutzung und Umsetzung. Dieser Artikel gibt einen kurzen Einblick, ob und wie COBIT in einem Unternehmen schnellen Nutzen stiften kann.

02. Mit dem ersten Eindruck wird gepunktet

An was erinnert sich ein Leser als erstes, wenn er die Einführung in COBIT aufmerksam studiert hat, diese aber vielleicht für einige Monate hat liegen lassen? Vermutlich dürfte dies das COBIT Core Model sein. Das Core Models liefert einen schnellen Überblick über alles, was eine Unternehmen mit IT tun kann. Dies deckt neben Klassikern wie IT-Projekten und dem IT-Betrieb auch Themenbereiche zur finanziellen und personellen Ausstattung, IT-Strategien und Unternehmensarchitekturen, IT-Sicherheit und -Risiken ab.

Hierin besteht dann auch gleich der erste Anwendungsfall von COBIT: Das Unternehmen hat mit dem Core Model ein Mittel sich selbst zu bewerten und Rechenschaft darüber abzulegen, welche IT-Themen es organisiert hat oder haben sollte bzw. bei welchen es dies bewusst nicht tun will oder unbewusst nicht getan hat.

Im Core Model werden die IT-Themen in sogenannten Governance und Management Objectives unterteilt, wie z.B. Managed Strategy oder Managed Risk. Diese Begriffsbildung wirkt auf den ersten Eindruck etwas sperrig. Für die meisten Zwecke ist es ausreichend sich unter Governance und Management Objectives einen bestimmten die IT betreffenden Geschäftsprozess des Unternehmens vorzustellen. Die Zusammenfassung mehrerer Objectives in einem Prozess ist jedoch ebenso möglich.

Zur weiteren Beschäftigung mit dem Standard bietet es sich an, einzelne Prozesse genauer zu betrachten. Als erstes liefert einem der Standard zu jedem Prozess eine einfache, kompakte Beschreibung. Diese kann leicht für die Dokumentation der unternehmenseigenen IT-Prozesse ggf. unter Anpassung an die jeweils individuellen Bedürfnisse übernommen werden. So ist COBIT mindestens immer als gute Inspirationsquelle für textuelle Beschreibungen verwendbar.

COBIT Core Model

Das COBIT Core Model unterteil das, was eine IT bzw. ein Unternehmen zur IT tun soll, in 40 Ziele auf, die in 5 Domänen zusammengefasst sind.

Jedem Ziel ist ein Prozess im Unternehmen zuzuordnen, welcher das jeweilige Ziel zu verfolgen hat.

Beispielhafte Ziele bzw. Prozesse sind:

- Sicherstellen der Ressourcenoptimierung
- Managen der Strategie
- Managen von Sicherheit
- Managen von Risiko
- Managen von Projekten
- Managen des Betriebs
- Managen des internen Kontrollsystems

und viele weitere.

Es lohnt sich jedoch auch, die Beschreibungen aus COBIT eingehender zu studieren. So verrät die Beschreibung von „Managed Risk“, dass dieser Prozess in einer kontinuierlichen Identifizierung, Bewertung und Reduzierung von IT-bezogenen Risiken innerhalb der von der Unternehmensleitung festgelegten Toleranzgrenzen besteht. In dieser Aussage sind die wesentlichen Vorgaben des Standards bereits zusammengefasst.

Weitere Details zur Erfüllung von COBIT liefern die den Management Objectives unterliegenden sogenannten Managementpraktiken (siehe Abbildung 1 für ein Beispiel). Die Praktiken, ihre Beschreibungen und die den Praktiken der zu Grunde liegenden Aktivitäten liefern weitere Informationen über die Inhalte der Prozesse.

Durch Übernahme von Praktiken und Aktivitäten aus COIBT in die eigenen Prozesse wirkt COBIT überzeugend sowohl für einzelne Prozessverantwortliche im IT-Bereich als auch in kleinen Organisationen insgesamt.

03. COBIT überzeugt das Management

Um COBIT flächendeckend in der Organisation zu etablieren, muss das eigene Management von COBIT überzeugt werden. Hierzu bietet es sich an, eine schnelle Einschätzung der Relevanz der COBIT-Prozesse für das eigene Unternehmen vorzunehmen. Für relevante Prozesse sollte außerdem eine mindestens grobe Einschätzung eines bereits vorliegenden Erfüllungsgrads der COBIT-Anforderungen vorgenommen werden.

COBIT bietet verschiedene Hilfestellungen wie z.B. eine Zielkaskade zur Ableitung relevanter Prozesse und ein Performance Management mit Capability- und Maturity-Leveln zur Bewertung des Erfüllungsgrads der Anforderungen aus COBIT an. Zu Beginn ist der Aufwand für eine Anwendung dieser Methoden in aller Regel jedoch zu hoch, da dazu die Inhalte des Standards mit dem Status Quo der Organisation auf sehr detaillierter Ebene z.B. auf Ebene der Managementpraktiken einander zugeordnet und abgeglichen werden müssen.

Mit COBIT beginnen

Zur schnellen Ersteinschätzung des Erfüllungsgrads von COBIT bietet sich ein Workshop-basiertes Vorgehen mit ausgewählten Experten zur Ermittlung folgender Ergebnisse an:

1 Identifikation der relevanten COBIT-Prozesse:

Für jeden der vierzig COBIT-Prozesse wird bewertet, ob er für das Unternehmen relevant und wichtig ist. Sofern der Prozess bereits eingerichtet ist, werden die Eigentümer der Prozesse midentifiziert.

2 Bewertung der Capabilty-Level pro Prozess:

Für jeden relevanten COBIT-Prozess wird mit Hilfe von Capability Levels bewertet, ob und wie gut der Prozess in der Organisation umgesetzt ist.

3 Etablierung eines Vorgehens zur Verankerung des COBIT Performance Managements in der Organisation.

Idealerweise wird bereits ein Strategieprozess eingerichtet, welcher die Ergebnisse der Schritte 1. und 2. regelmäßig aktualisiert, verfeinert und den Status Quo an das Management berichet.

Besser bewährt hat sich eine zunächst grobe Einschätzung durch ausgewählte Wissensträger des Unternehmens auf Ebene der Prozesse, ohne im Detail auf die darunterliegenden Managementpraktiken einzugehen. Die Ergebnisse dieser Analyse mögen zunächst noch oberflächlich und nicht frei von Fehlern sein; sie sind jedoch mit verhältnismäßig geringem Aufwand zu erstellen und eröffnen den Raum für weitere Diskussionen und in der Folge tiefergehende Analysen.

Als erstes fallen bei der Analyse die größten Lücken in Prozessen auf, die zwar als relevant erkannt wurden, für die aber bis dato keine gelebte Praxis in der Organisation exisitiert.

Sich mit diesen Prozessen auseinanderzusetzen, stellt allein schon einen erheblichen Mehrwert für die Organisation dar.

Die Analyse liefert dem Management eine gesamthafte Sicht auf die eigene IT-Organisation und zeigt die Verbesserungspotentiale explizit auf. Dies ist für die Geschäftsführung sofort und leicht nachvollziehbar und verständlich.

04 Der Weg zur erfolgreichen Einführung

Hat die Organisation den Mehrwert von COBIT erkannt, so folgt ein Projekt zur Umsetzung des Standards. Dieses kann anhand des von COBIT vorschlagenen Vorgehensmodells oder eines anderen in der Organisation bereits etablierten Projektvorgehens erfolgen.

Es bietet sich dabei an, möglichst frühzeitig den in COBIT vorgesehenen Strategieprozess zu etablieren, da dieser die Ergebnisse des Projekts nach Projektende im laufenden Betrieb übernehmen und fortschreiben soll.

Der Strategieprozess weist die Orientierung am COBIT-Standard als Ziel aus und beurteilt die Zielerreichung regelmäßig. Dabei kann er die Beurteilung der Leistungsfähigkeit der Prozesse auf Basis des von COBIT vorgesehenen Performance Managements mit Capability- und Maturity-Leveln vornehmen.

Im Zuge der Umsetzung sollten erstmalig die Eigentümer der vorhandenen und der zu etablierenden Prozesse identifiziert, über das Vorgehen und den COBIT-Standard informiert und an der Festlegung eines Ambitionsniveaus für die Prozess-Performance und die Messung der Performance zur Beurteilung der Leistungsfähigkeit beteiligt werden. Dem ober(st)en Management wird über die Performance berichtet. Auf der Basis des Berichts wird über weitere Maßnahmen zur Verbesserung entschieden. Abbildung 1 veranschaulicht dieses Vorgehen.

Nach der erfolgreichen Ersteinführung werden die Prozesse unter Orientierung an COBIT im Rahmen etablierter Prozesse kontinuierlich weiterentwickelt, bis sie ein Nieveau erreichen, dass keine Verbesserung mehr erfordert.

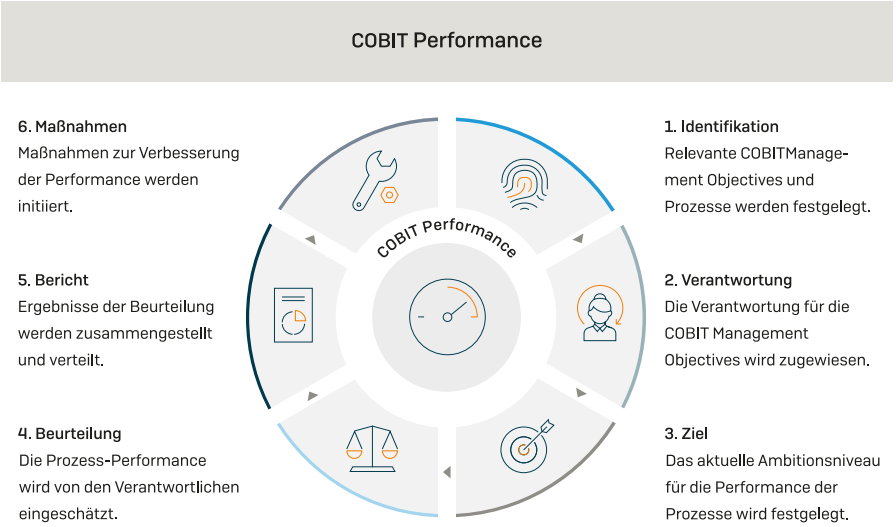

Abbildung 1: COBIT Performance

05 COBIT wächst und gedeiht

Viele Organisationen haben COBIT eingeführt oder zur Orientierung verwendet. Für internationale Großkonzerne erfolgt die Anwendung von Standards wie COBIT erfahrungsgemäß zeitnah nach dessen Veröffentlichung und die Berücksichtigung von Aktualisierungen gehören zum Standardprogramm bei der Weiterentwicklung des internen Kontrollsystems. Die Anwendung einer Zielkaskade oder andere Methoden der Priorisierung bleiben bei diesen Unternehmen aus, da ohnehin alle Management Objectives abgedeckt sein sollten und auch der Anspruch besteht, eine Optimierung der zugehörigen gut dokumentierten Prozesse anhand von Performance-Kennzahlen vorzunehmen. Nach einigen Jahren erreicht die Performance dann ein so hohes Niveau, dass eine weitere Verbesserung nur in den Teilen der Organisation noch möglich ist, die z.B. durch Übernahmen im Laufe der Zeit neu hinzugekommen sind.

Kleine Organisationen verwenden meist nur Teile von COBIT. Dies ist darauf zurückzuführen, dass für diese der Auslöser der Orientierung an COBIT meist nicht die gesamthafte Überarbeitung der IT-Governance, sondern eine bestimmte einzelne Fragestellung wie etwa die Einführung eines IT-Riskoprozesses ist.

Insgesamt hat die aktuelle COBIT-Version auch nach fünf Jahren ihres Bestehens nichts an Aktualität eingebüßt, wenn auch bestimmte Teile des Standards, wie z.B. die explizite Zuordnung von Verantwortlichkeiten für Managementpraktiken zu vordefinierten COBIT-Rollen und organisatorischen Strukturen, nicht 1:1 in die eigene Organisation übernommen werden können.

Eine Aktualisierung von COBIT ist schon auf Grund der Neuerungen in den referenzierten Standards wie z.B. von ITIL v3 auf ITIL v4 erforderlich.

Die Notwendigkeit von Erweiterungen für zusätzliche Objectives kann diskutiert werden. Bei der Aktualisierung der Vorgängerversion COBIT 5 auf COBIT 2019 kamen 3 Objectives zum Datenmanagement, Projektmanagement und Auditmanagement hinzu, für die es schon damals außerhalb von COBIT entsprechende Standards gab. Für neue Technologien und Entwicklungen wie z.B. zum Energie- und Umweltmanagement (z.B. nach ISO 50001, ISO 14001), zur künstlichen Intelligenz, zu Cloud oder zu Blockchains werden Standards mit Bezug zur Informationstechnologie entstehen oder sind bereits entstanden, für welche eine Einbettung in COBIT erwogen werden kann. Es bleibt spannend, die weitere Entwicklung abzuwarten.

Autor

Dr. Matthias Döring
Senior Manager und Experte für IT Governance
d-fine GmbH, München
Matthias.Doering@d-fine.com

d-fine

Berlin
d-fine GmbH
Kranzler Eck
Kurfürstendamm 21
10719 Berlin
Deutschland
berlin@d-fine.de

Düsseldorf
d-fine GmbH
Dreischeibenhaus 1
40211 Düsseldorf
Deutschland
duesseldorf@d-fine.de

Frankfurt
d-fine GmbH
An der Hauptwache 7
60313 Frankfurt
Deutschland
frankfurt@d-fine.de

Hamburg
d-fine GmbH
Am Sandtorpark 6
20457 Hamburg
Deutschland
hamburg@d-fine.de

London
d-fine Ltd
14 Aldermanbury Square
London, EC2V 7HR
United Kingdom
london@d-fine.co.uk

Mailand
d-fine s.r.l.
Via Giuseppe Mengoni 4
20121 Milano MI
Italien
milano@d-fine.com

München
d-fine GmbH
Bavariafilmplatz 8
82031 Grünwald
Deutschland
muenchen@d-fine.de

Stockholm
d-fine AB
Brahegatan 10
114 37 Stockholm
Schweden
stockholm@d-fine.se

Utrecht
d-fine BV
Stadsplateau 7
3521 AZ Utrecht
Niederlande
utrecht@d-fine.nl

Wien
d-fine Austria GmbH
Seilerstätte 13
1010 Wien
Österreich
wien@d-fine.at

Zürich
d-fine AG
Brandschenkestrasse 150
8002 Zürich
Schweiz
zuerich@d-fine.ch