Klotz, Michael

Working Paper

IT-Compliance nach COBIT 2019

SIMAT Arbeitspapiere, No. 11-19-034

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Klotz, Michael (2019) : IT-Compliance nach COBIT 2019, SIMAT Arbeitspapiere, No. 11-19-034, Hochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund

This Version is available at:
https://hdl.handle.net/10419/204448

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 11-19-034

IT-Compliance nach COBIT® 2019

Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

August 2019

ISSN 1868-064X

Klotz, Michael: IT-Compliance nach COBIT® 2019. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: Hochschule Stralsund, SIMAT Stralsund Information Management Team, 2019 (SIMAT AP, 11 (2019), 34), ISSN 1868-064X

Impressum

Hochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.hochschule-stralsund.de

Herausgeber

Prof. Dr. Michael Klotz
Hochschule Stralsund, Fakultät für Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@hochschule-stralsund.de

Print

Digitaldruck: www.dokuteam-x.de
Behrndt & Herud GmbH
Anklamer Straße 98
17489 Greifswald

Autoren

Prof. Dr. Michael Klotz lehrt, forscht und publiziert an der Fakultät für Wirtschaft der Hochschule Stralsund auf den Gebieten der Unternehmensorganisation und -überwachung, der IT-Governance und der IT-Compliance. Er ist Mitglied zahlreicher Fachorganisationen, u. a. Mitglied des wissenschaftlichen Beirats und Academic Advocate der ISACA sowie Mitherausgeber der Zeitschrift „IT-Governance“.

IT-Compliance nach COBIT® 2019

Prof. Dr. Michael Klotz[1]

Zusammenfassung: Das Ende 2018 von der ISACA publizierte Framework „COBIT® 2019“ knüpft in seinem Verständnis von IT-Compliance an die Vorgängerversionen 4.1 und 5 an. Trotzdem sind in der neuen COBIT®-Version zahlreiche Änderungen und Ergänzungen enthalten, die in diesem Arbeitspapier diskutiert werden sollen. Im Ergebnis umfasst das Compliance-Verständnis von COBIT® 2019 nach wie vor sowohl die IT-Compliance als auch die IT-gestützte Corporate Compliance. Die grundlegenden Compliance-Ziele bleiben genauso erhalten, wie die Governance- und Managementpraktiken mit ihren Aktivitäten zur Sicherstellung von Compliance. Die Enabler finden sich jetzt als „Komponenten“ wieder, werden dafür aber systematisch und komplett abgehandelt. Die Änderungen der COBIT® 2019-Produktfamilie beinhalten Erweiterungen wie Streichungen gleichermaßen. Insgesamt fällt die Compliance-Thematik ähnlich umfangreich wie in COBIT® 5 aus. In COBIT® 5 beinhalteten 26 von 37 IT-Prozessen Compliance-Aufgaben, während in COBIT® 2019 15 von 40 IT-Governance- und IT-Managementzielen das Erreichen der compliance-bezogenen IT-Ziele unterstützen. Des Weiteren stellen Compliance-Anforderungen einen eigenständigen Designfaktor dar bzw. sind Teil weiterer Designfaktoren für die IT-Governance. Trotz aller Veränderungen und Anpassungen kann COBIT® 2019 nach wie vor den mit IT-Compliance betrauten Funktionen und Personen als Orientierung und Hilfsmittel für die praktische Arbeit dienen.

Gliederung

[1] Prof. Dr. Michael Klotz, Hochschule Stralsund, Fakultät für Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@hochschule-stralsund.de

Schlüsselwörter: COBIT® – IT-Compliance – IT-Governance – IT-Management – IT-Prozesse – IT-Ziele – Prozessmodell – Unternehmensziele

JEL-Klassifikation: L21, M14, M21, M42

Vorwort des Herausgebers

Das vorliegende Arbeitspapier schließt an das Arbeitspapier Nr. 25 vom Januar 2014 an. Dort wurden die vierte (4.1) und die fünfte Version von COBIT® hinsichtlich IT-Compliance analysiert und beschrieben. Mit COBIT® 2019 liegt abermals eine umfassende Überarbeitung vor, so dass sich die Frage stellt, wie sich die Thematik „IT-Compliance“ in der aktuellen Version entwickelt hat. Damit das vorliegende Arbeitspapier eigenständig lesbar ist, werden wesentliche Änderungen und Weiterentwicklungen im Vergleich zu COBIT® 5 ausgeführt. Wer einen detaillierten Vergleich zu den beiden Vorgängerversionen anstellen will, muss beide Arbeitspapiere nebeneinanderlegen.

Aus Gründen einer besseren Verständlichkeit wurden die Texte aus COBIT® 2019 überwiegend ins Deutsche übersetzt. Als Übersetzungstool fand „deepl.com“ Verwendung. Der Einpassung in die deutsche Begrifflichkeit wurde der Vorzug vor einer wortwörtlichen Übersetzung gegeben. Dies birgt jedoch die Gefahr begrifflicher Unschärfen. Die Leser sind also aufgefordert (schon da der Autor kein Fachübersetzer ist), selbst immer wieder die Originaltexte zwecks kritischer Prüfung und besserem Verständnis der Ausführungen zur Hand zu nehmen.

Ich hoffe, dass mit diesem Arbeitspapier wiederum dem IT-Praktiker, der COBIT® 2019 in seiner Arbeit verwendet, eine Hilfestellung an die Hand gegeben wird. Wie immer sind Rückmeldungen jeglicher Art willkommen.

Prof. Dr. Michael Klotz

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

3LoD	Three Lines of Defense
AG	Alignment Goal
APO	Align, Plan and Organise
BAI	Build, Acquire and Implement
BSC	Balanced Scorecard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIO	Chief Information Officer
CMMI	Capability Maturity Model® Integration[2]
COBIT®	Control Objectives for Information and Related Technology[3]
COSO ERM	Committee of Sponsoring Organizations Enterprise Risk Management
CPM	COBIT Performance Management
DSB	Datenschutzbeauftragter
DSGVO	Datenschutz-Grundverordnung
DSS	Deliver, Service and Support
EAM	Enterprise Architecture Management
EDM	Evaluate, Direct and Monitor
ERM	Enterprise Risk Management
EU	Europäische Union
GRC	Governance – Risk – Compliance
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
IP	Intellectual Property
ISACA®	Information Systems Audit and Control Association[4]
ISO	International Organization for Standardization
IT	Informationstechnik / Informationstechnologie
ITIL®	Information Technology Infrastructure Library
KMU	Kleine und mittlere Unternehmen
MEA	Monitor, Evaluate and Assess
NIST	National Institute of Standards and Technology

[2] Capability Maturity Model® ist ein eingetragenes Warenzeichen der Carnegie Mellon University.
[3] COBIT® ist ein eingetragenes Warenzeichen der Information Systems Audit and Control Association.
[4] ISACA® ist ein eingetragenes Warenzeichen der Information Systems Audit and Control Association.

p	primär
PMBOK® Guide	A Guide to the Project Management Body of Knowledge[5]
RACI	Responsible, Accountable, Consulted, Informed
Rev.	Revision
s	sekundär
SFIA	Skills Framework for the Information Age
SIMAT	Stralsund Information Management Team
V	Version

[5] PMBOK® ist ein eingetragenes Warenzeichen des Project Management Institute.

1 Überblick über die generellen Änderungen in COBIT® 2019

Umfassende Überarbeitung

COBIT® 2019 wurde Ende des Jahres 2018 veröffentlicht. Trotz umfassender Überarbeitung finden sich inhaltlich viele Modelle, Konzepte und Strukturen aus COBIT® 5 grundsätzlich wieder, so z. B. die Unterscheidung zwischen IT-Governance und IT-Management, die Prinzipien für die Ausgestaltung von IT-Governance und IT-Management, die Zielkaskade, das Reifegradmodell, der Lebenszyklus der kontinuierlichen Verbesserung und – auf den zweiten Blick – auch das Referenzmodell für die IT-Prozesse mit Praktiken und Aktivitäten, Beispielmetriken, Verantwortlichkeiten im RACI-Modell und zugeordneten Standards und Normen. Beim genaueren Hinsehen wurden aber die allermeisten Elemente mehr oder minder verändert und an die neue Struktur der COBIT®-Dokumente und der Beschreibungssystematik angepasst.[6]

Neuerungen in COBIT® 2019

Die ins Auge springende wesentliche Neuerung im Vergleich zur vorherigen Version besteht in der Dokumentenstruktur von COBIT® 2019. Diese wurde nicht evolutionär weiterentwickelt, sondern abermals grundlegend verändert. Die COBIT® 2019-Produktfamilie ist mit vier Dokumenten an den Start gegangen, wobei die Dokumente untereinander in Verbindung stehen, vgl. Abbildung 1.

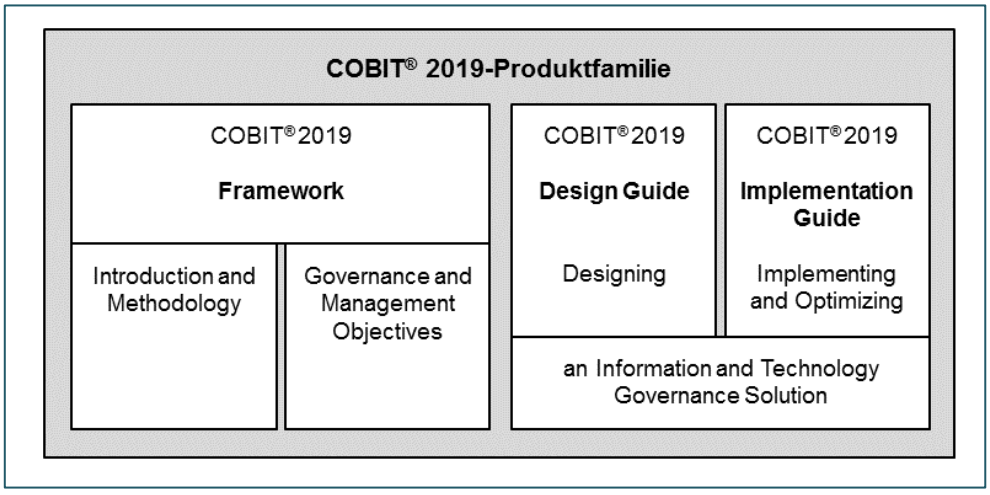

Abbildung 1
COBIT® 2019-Produktfamilie[7]

[6] Bis auf gelegentliche Vergleiche mit COBIT 5 soll keine weitere Rückschau auf frühere COBIT-Versionen erfolgen. Für einen geschichtlichen Abriss der Entwicklung von COBIT s. *Johannsen/Goeken 2011*, S. 42f. und *Gaulke 2014*, S. 9ff.
[7] Vgl. *ISACA 2018a*, S. 19; eigene Darstellung.

Situativer Ansatz

Das „COBIT® 2019 Framework“ besteht aus der grundlegenden Einführung sowie der Darstellung der IT-Governance- und IT-Management-Zielsetzungen. Dagegen richten sich der „COBIT® 2019 Design Guide“ und der „COBIT® 2019 Implementation Guide“ auf die IT-Governance-Lösung, die vom Unternehmen zu entwickeln, zu implementieren und zu optimieren ist. Hierin ist ein Schwerpunkt der Weiterentwicklung von COBIT® zu erkennen: Die Gestaltungsvorgaben von COBIT® 2019 sollen besser und leichter auf die jeweilige Unternehmenssituation angepasst werden können.[8] COBIT® 2019 verfolgt damit einen situativen Ansatz und bietet hierfür ein Instrumentarium an. Für diese Ausrichtung von COBIT® 2019 stehen insbesondere der Design und der Implementation Guide. Als Design-Faktoren berücksichtigt der Design Guide beispielsweise Unternehmensziele und -strategien, die Unternehmensgröße oder die Rolle der IT, aber eben auch die Compliance-Anforderungen eines Unternehmens.[9] Neben die Designfaktoren treten künftig flexibel zu ergänzende Schwerpunktbereiche[10] („focus areas“), z. B. KMU, IT-Sicherheit und IT-Risikomanagement, für die bereits jeweils eigene Dokumente in Arbeit befindlich sein sollen.[11]

Von Enablern zu Komponenten

Im Vergleich mit der Struktur der COBIT® 5-Produktfamilie zeigt sich, dass die Enabler-Handbücher, die in der Vergangenheit ohnehin nicht komplettiert worden sind, entfallen. Die Enabler selbst sind nunmehr in die Beschreibungsstruktur der IT-Governance- und IT-Management-Ziele integriert. Dort werden sie jetzt als interagierende „Komponenten“ bezeichnet, die in ihrer Ausgestaltung letztlich das IT-Governance-System eines Unternehmens ausmachen, vgl. Abbildung 2. Als Komponenten werden berücksichtigt:

(1) Prozesse

(2) Aufbauorganisation

(3) Grundsätze, Richtlinien und Verfahren

(4) Information

(5) Kultur, Ethik und Verhalten

(6) Menschen, Fähigkeiten, Kompetenzen

(7) Services, Infrastruktur, Anwendungen.

---

[8] Vgl. *Gaulke 2019*, S. 3.
[9] Nach *ISACA 2018a*, S. 23.
[10] Nach *Gaulke 2019*, S. 8.
[11] Nach *ISACA 2018a*, S. 20.

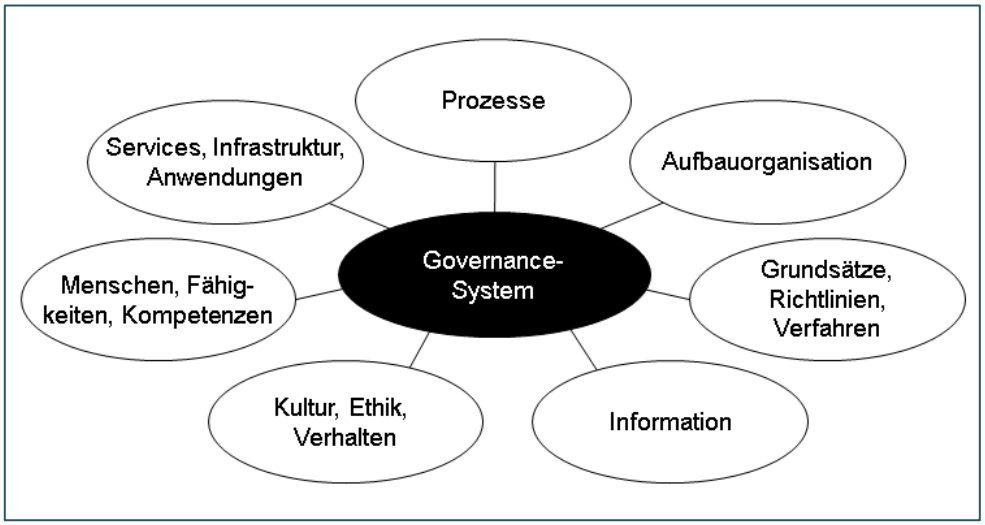

Abbildung 2
Komponenten eines Governance-Systems nach COBIT® 2019[12]

Bezüge zu IT-Compliance ergeben sich in all diesen Komponenten, was als deutliche Erweiterung gegenüber COBIT® 5 anzusehen ist.

2 Compliance-Verständnis von COBIT® 2019

Compliance als Ziel der Governance

COBIT® 2019 sieht Compliance ausdrücklich als ein wichtiges Ziel der Governance an. Governance hat sicherzustellen, dass Leistung und Compliance im Hinblick auf die Unternehmensziele und die vereinbarte Richtung der Unternehmensentwicklung überwacht werden.[13] Veränderte Compliance-Anforderungen stellen zudem einen wichtigen externen Treiber für IT-Governance dar. Neue Gesetze und regulatorischen Vorgaben haben oft Auswirkungen auf ein bestehendes IT-Governance-System. So lösen beispielsweise erweiterte Berichtsanforderungen, z. B. seitens einer Aufsichtsbehörde, angesichts der Durchgängigkeit der IT häufig einen Veränderungsbedarf für das IT-Governance-System aus.[14]

Externe Compliance in COBIT® 2019

Wie schon bei COBIT® 5 findet sich auch in COBIT® 2019 keine explizite Definition für IT-Compliance. Gefordert wird jedoch durchgängig die Compliance mit verschiedensten Anforderungen. Diese stammen vor allem aus Gesetzen und regulativen Vorgaben. Die diesbezügliche Compliance stellt das IT-Ziel AG01 (I&T compliance and support for business compliance

[12] Nach *ebd.*, S. 22; eigene Darstellung.
[13] Vgl. *ebd.*, S. 13.
[14] Nach *ISACA 2018d*, S. 28.

with external laws and regulations) dar.[15] Als Rechtsbereiche werden ausdrücklich genannt: Datenschutz, Finanzberichterstattung, Urheberrecht, Gesundheit und Arbeitssicherheit sowie allgemein branchenspezifische Vorschriften.[16] Zu dieser externen Compliance zählen jedoch auch vertragliche Verpflichtungen. Dies ergibt sich einerseits aus den beispielhaften Zielmetriken zu AG01, wo die Zahl der Non-Compliance-Vorfälle im Zusammenhang mit vertraglichen Vereinbarungen mit IT-Dienstleistern genannt ist.[17] Andererseits werden als spezielle und damit wichtige Verträge Lizenzvereinbarungen genannt.[18] Auch zur externen Compliance gehörig, aber seltener genannt, ist die Compliance mit Normen und Standards[19]. Beim Enterprise Architecture Management (EAM) fordert COBIT® 2019 die Compliance mit entsprechenden Normen und Richtlinien,[20] beim Facilitymanagement auch mit Herstellerspezifikationen.[21]

Interne Compliance in COBIT® 2019

Die Compliance mit internen IT-Richtlinien stellt das IT-Ziel AG11 (I&T compliance with internal policies) dar. Hierunter sind alle Formen interner Vorgaben zu verstehen, z. B. Unternehmensrichtlinien, Hausstandards oder interne Verfahren und Methoden, die in den verschiedenen Unternehmensfunktionen zum Einsatz gelangen.[22]

Compliance-Verständnis wie in COBIT® 5

Da COBIT® 2019 auf die Einhaltung der Compliance-Anforderung abstellt und diese insbesondere an Fällen von Non-Compliance und damit verbundenen monetären und nicht-monetären Schadensfolgen misst, folgt COBIT® eher einem zustandsorientierten Compliance-Begriff. Danach wäre IT-Compliance dann gegeben wenn das Unternehmen die Vorgaben aus den im Einzelnen von COBIT® genannten Quellen nachweislich erfüllt.[23] Im Ergebnis hat sich hier im Vergleich zu COBIT® 5 keine Veränderung ergeben.[24] Dies gilt auch für die Bezugnahme auf das Conformance-Prinzip der ISO/IEC 38500, das auf die Konformität mit rechtlichen und behördlichen Anforde-

[15] Vgl. z. B. *ISACA 2018a*, S. 30.
[16] Vgl. die Auflistung in MEA03.01, Aktivität 2, s. *ISACA 2018b*, S. 285.
[17] Vgl. z. B. *ISACA 2018a*, S. 30.
[18] Vgl. die Beschreibung der Zielsetzung von BAI09, s. *ISACA 2018b*, S. 209.
[19] Der englische Begriff „Standard“ in COBIT® 2019 steht für Normen, bspw. von ISO/IEC oder NIST, Standards werden dagegen eher mit den Begriffen „framework“ und „guidance“ bezeichnet.
[20] Vgl. APO03.05, Aktivität 5, s. *ISACA 2018b*, S. 76.
[21] Vgl. DSS01.05, Aktivität 9, s. *ISACA 2018b*, S. 233.
[22] Vgl. MEA03.03, s. *ISACA 2018b*, S. 286.
[23] Vgl. Begriff und Begriffsdiskussion in *Klotz 2017*, S. 858f.
[24] Vgl. *Klotz 2014*, S. 26.

rungen und ihre Berücksichtigung in internen Richtlinien und Verfahren sowie in Verträgen mit Dritten abstellt.[25]

Prinzipien für Governance-Rahmenwerke

COBIT® 2019 versteht sich weiterhin als Integrator für verschiedenste IT-Normen und -Standards. Dies stellt jedoch nicht mehr wie in COBIT® 5 eines der Prinzipien für Governance-Systeme dar. Dort wurde COBIT® noch als „einheitliches, integriertes Rahmenwerk“ bezeichnet.[26] In COBIT® 2019 wird zwischen Prinzipien für Governance-Systeme und Prinzipien für Governance-Rahmenwerke unterschieden. Nach dem dritten Prinzip für Governance-Rahmenwerke sollten sich diese an den relevanten, wichtigen Normen bzw. Standards, Rahmenwerken und Vorschriften orientieren.[27] Während COBIT® 5 lediglich 17 Dokumente, die Eingang in die Entwicklung von COBIT® 5 genommen haben, auflistet,[28] sind dies in COBIT® 2019 nunmehr 32 Dokumente. Zu ihnen gehören beispielsweise CMMI®-Standards, COSO ERM, ISO/IEC-Normen der Normenreihen 2700x und 3850x, NIST-Standards, der PMBOK® Guide, Standards der Open Group und das Skills Framework for the Information Age (SFIA).[29]

3 IT-Compliance als Teil der COBIT® 2019-Zielkaskade

3.1 Unternehmens- und IT-Ziele in COBIT® 2019

Treiber und Bedürfnisse als Ausgangspunkt

Die Zielkaskade ist in COBIT® 2019 an mehreren Stellen verändert worden. Ausgangspunkt sind immer noch die Treiber und Bedürfnisse der Stakeholder. Diese werden jedoch nicht mehr wie in COBIT® 5 systematisch in Unternehmensziele überführt. Dort wurden die Treiber in Anforderungen bzgl. Nutzenrealisierung sowie Risiko- und Ressourcenoptimierung transformiert[30] und anschließend mittels einer Zuordnungsmatrix auf die Unternehmensziele gemappt.[31] Dieses Vorgehen ist in COBIT® 2019 nicht mehr vorgesehen, was bedeutet, dass die Ableitung von priorisierten Unternehmenszielen aus den Treibern und Bedürfnissen der Stakeholder nun unternehmensindividuell und situationsspezifisch erfolgen muss. Dies dürfte all den-

[25] Vgl. *ISO/IEC 38500:2015*, S. 10.
[26] Vgl. *ISACA 2012a*, S. 27.
[27] Nach *ISACA 2018a*, S. 18.
[28] Vgl. *ISACA 2012a*, S. 49.
[29] Vgl. *ISACA 2018a*, S. 63f.
[30] Vgl. *ISACA 2012a*, S. 19f.
[31] Vgl. *ebd.*, S. 57f.

jenigen zupass kommen, denen das bisherige Vorgehen als allzu „mechanistisch“ erschien.

Unternehmensziele und IT-Ziele

Die Unternehmensziele („Enterprise Goals“ – EG) wurden in COBIT® 2019 auf 13 Zielsetzungen reduziert, wobei sie weiterhin den einzelnen Ebenen einer Balanced Scorecard (BSC)[32] zugeordnet sind. Die IT-Ziele wurden in Ausrichtungsziele[33] („Alignment Goals“ – AG) umbenannt, da sie für die Ausrichtung aller IT-Bemühungen auf die Unternehmensziele stehen.[34] Auch die IT-Ziele wurden von 17 auf 13 Zielsetzungen verringert. Die Ableitung von IT-Zielen aus Unternehmenszielen erfolgt wie in COBIT® 5 auf Basis einer Zuordnungsmatrix. Im letzten Kaskadierungsschritt werden aus den Ausrichtungszielen die IT-Governance- und IT-Managementziele abgeleitet, vgl. Abbildung 3. Auch hier kommt wieder die bisherige, angepasste Zuordnungsmatrix zum Einsatz.

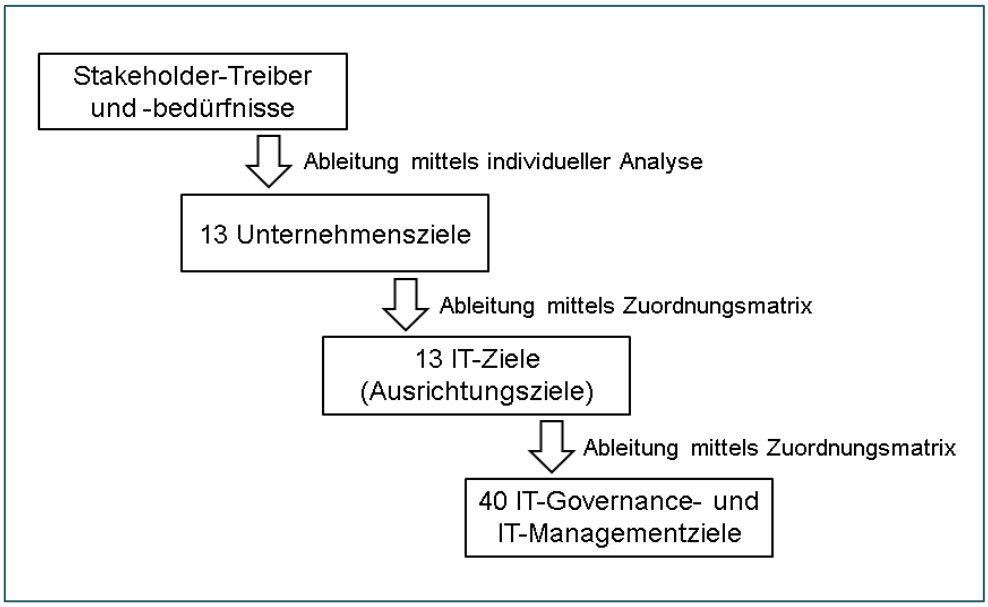

Abbildung 3
Zielkaskade nach COBIT® 2019[35]

IT-Governance- und IT-Managementziele

Hinter den IT-Governance- und IT-Managementzielen „verstecken“ sich die IT-Prozesse aus COBIT® 5. Hierfür erfolgte lediglich eine Umformulierung der Prozesstitel aus COBIT® 5, so dass der Titel jetzt nicht mehr eine Aufgabenbenennung umfasst, sondern eine Zielbeschreibung i. S. eines erreich-

[32] Diese sind: Financial, Customer, Internal, Growth, vgl. *ebd.*, S. 24. Die “Growth”-Perspektive umfasst häufig auch das organisatorische Lernen.
[33] Nach *Gaulke 2019*, S. 7.
[34] Vgl. *ISACA 2018a*, S. 28.
[35] Nach *ebd.*; eigene Darstellung.

ten Zustands. So hieß beispielsweise der IT-Prozess APO12 in COBIT® 5 „Manage risk“, das betreffende IT-Managementziel in COBIT® 2019 wird dagegen mit „Managed risk“ bezeichnet. Mitunter fällt die Umformulierung etwas umfangreicher aus. So hatte der IT-Prozess MEA03 in COBIT® 5 den Titel „Monitor, evaluate and assess compliance with external requirements”, während das IT-Managementziel in COBIT® 2019 lediglich mit “Managed compliance with external requirements” bezeichnet wird.

Da Compliance ein Ziel von Governance darstellt, findet Compliance folgerichtig auch Eingang in die Unternehmensziele. Unverändert beziehen sich zwei Unternehmensziele auf Compliance:

- Unternehmensziel 3: Compliance mit externen Gesetzen und Bestimmungen;
- Unternehmensziel 11: Compliance mit internen Richtlinien.

Entsprechend ist die Gewährleistung von IT-Compliance nach wie vor Gegenstand von zwei der 13 IT-Ziele:

- IT-Ziel 1: IT-Compliance und Unterstützung bei der Einhaltung externer Gesetze und Vorschriften;
- IT-Ziel 11: IT-Compliance mit internen Richtlinien.

BSC-Perspektive

Die beiden IT-Ziele entsprechen weiterhin inhaltlich den Unternehmenszielen. Dies gilt auch für die Zuordnung zu den Perspektiven der Balanced Scorecard (BSC); die IT-Compliance und die Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen (IT-Ziel 1) ist der Finanzperspektive und die IT-Compliance mit internen Richtlinien (IT-Ziel 11) der internen Perspektive zugeordnet.[36] Die Formulierung von IT-Ziel 1 stellt weiterhin auf IT-Compliance einerseits und die IT-Unterstützung der Compliance des Unternehmens andererseits – also die Unterscheidung zwischen IT-Compliance und IT-gestützter Compliance – ab.[37]

Die beiden IT-Ziele unterstützen die beiden compliance-bezogenen Unternehmensziele, vgl. Tabelle 1. Die Qualität dieser Unterstützung wird nach wie vor in zwei Gruppen unterteilt: Die primäre Unterstützung steht für eine wichtige Beziehung, die sekundäre Unterstützung für eine immer noch starke, aber im Vergleich weniger wichtige Beziehung.

---

[36] Vgl. *ebd.*, S. 29ff.
[37] Zu dieser Unterscheidung s. *Klotz 2017*, S. 868ff.

IT-Ziel \ Unternehmensziel	03 Compliance mit externen Gesetzen und Bestimmungen	11 Compliance mit internen Richtlinien
01 IT-Compliance und Unterstützung bei der Einhaltung externer Gesetze und Vorschriften	primär	sekundär
11 IT-Compliance mit internen Richtlinien	primär	primär

Tabelle 1
Unterstützung der compliance-bezogenen Unternehmensziele durch IT-Ziele[38]

Indikatoren

Die Indikatoren zur Messung der Zielerreichung wurden in COBIT® 2019 überarbeitet. Für die IT-Compliance und die Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen (IT-Ziel 1) werden folgende Indikatoren genannt:

- Kosten für Non-Compliance der IT, einschließlich Vergleichs- und Bußgeldzahlungen sowie Auswirkungen von Reputationsverlusten;
- Anzahl der IT-bezogenen Verstöße, die der Unternehmensleitung gemeldet wurden oder die eine öffentliche Kritik bzw. Blamage gegenüber der Öffentlichkeit verursachen;
- Anzahl der Non-Compliance-Vorfälle im Zusammenhang mit vertraglichen Vereinbarungen mit IT-Dienstleistern.[39]

Für die IT-Compliance mit internen Richtlinien (IT-Ziel 11) werden folgende Indikatoren angegeben:

- Anzahl der Vorfälle im Zusammenhang mit der Nichteinhaltung von IT-Richtlinien;
- Anzahl der Ausnahmen von internen Richtlinien;
- Häufigkeit der Überprüfung und Aktualisierung von IT-Richtlinien.[40]

3.2 IT-Governance- und IT-Managementziele in COBIT® 2019

IT-Governance- und IT-Managementziele

Die unterste Ebene der Zielkaskade besteht in COBIT® 2019 nunmehr also aus den IT-Governance- und IT-Managementzielen, d. h. aus dem „COBIT Core Model“. Dieses besteht wie das bisherige Prozessmodell aus fünf Do-

[38] Vgl. *ISACA 2018b,* S. 297.
[39] Vgl. *ISACA 2018a*, S. 30.
[40] Vgl. *ebd.*, S. 32.

mänen, denen 40 Ziele für IT-Governance und IT-Management zugeordnet sind, s. Tabelle 2. Die Beschreibung der einzelnen IT-Governance- und IT-Managementziele gliedert sich, wie in Abbildung 2 dargestellt, in die verschiedenen Komponenten, wobei die Prozessbeschreibung nach wie vor den größten Raum einnimmt.

Tabelle 2 Domänen des COBIT Core Model [41]

Domäne	Abk.	Bereich	Anzahl Ziele
Evaluieren, Vorgeben und Überwachen (engl. „Evaluate, Direct and Monitor")	EDM	IT-Governance	5
Anpassen, Planen und Organisieren (engl. „Align, Plan and Organise")	APO	IT-Management	14
Aufbauen, Beschaffen und Implementieren (engl. „Build, Acquire and Implement"	BAI	IT-Management	11
Bereitstellen, Betreiben und Unterstützen (engl. „Deliver, Service and Support")	DSS	IT-Management	6
„Überwachen, Evaluieren und Beurteilen" (engl. „Monitor, Evaluate and Assess")	MEA	IT-Management	4

COBIT Performance Management

Als Neuerung erweist sich ein Schritt zurück, da in der Prozessbeschreibung nunmehr wieder ein Reifegradmodell enthalten ist, ähnlich wie dies bereits in COBIT® 4.1 der Fall war. Im Einzelnen werden in COBIT® 2019 den Prozessaktivitäten Befähigungsgrade („capability levels") zugeordnet. Diese Befähigungsstufen bilden das „COBIT Performance Management" (CPM), das auf der CMMI V2.0 basiert und ein Prozessfähigkeitsschema mit sechs Stufen umfasst:[42]

- (1) Incomplete,
- (2) Initial,
- (3) Managed,
- (4) Defined,
- (5) Quantitative,
- (6) Optimizing.

Ein Prozess erreicht eine bestimmte Fähigkeitsstufe von 1 bis 5, sobald alle Aktivitäten, die dieser Stufe zugeordnet sind, erfolgreich durchgeführt wer-

[41] Vgl. *ebd.*, S. 20f.
[42] Vgl. *ebd.*, S. 40.

den.[43] Damit nimmt COBIT® 2019 wieder etwas Abstand von der ISO/IEC 33000.[44] Weitere Komponenten, z. B. Aufbauorganisation und Information, sollen künftig in das CPM einbezogen werden. Zudem sollen Reifegrade für die verschiedenen Fokusbereiche angegeben werden.[45]

Identifizierung

Die compliance-relevanten IT-Governance- und IT-Managementziele in COBIT® 2019 lassen sich wie bisher durch die Zuordnung zu den von ihnen unterstützten IT-Zielen (1 und 11) identifizieren:

IT-Ziel 1

- Von 40 IT-Governance- und IT-Managementzielen richten sich zehn auf die Erreichung von IT-Compliance und Unterstützung bei der Einhaltung externer Gesetze und Vorschriften. Hiervon leisten zwei IT-Governance- und IT-Managementziele eine primäre, acht IT-Governance- und IT-Managementziele eine sekundäre Unterstützung, vgl. Tabelle 3. In COBIT® 5 waren es noch 20 von 37 IT-Prozessen mit sieben primären und 13 sekundären Unterstützungen. Auch wird IT-Ziel 1 im Vergleich zu COBIT® 5 nicht mehr von allen fünf Domänen adressiert.

Tabelle 3
IT-Ziel 1 unterstützende IT-Governance- und IT-Managementziele[46]

IT-Ziel Nr. 1: IT-Compliance und Unterstützung bei der Einhaltung externer Gesetze und Vorschriften	
wird primär unterstützt durch ...	
1. EDM01:	Ensured governance framework setting and maintenance
2. MEA03:	Managed compliance with external requirements
wird sekundär unterstützt durch ...	
1. EDM03:	Ensured risk optimization
2. APO01:	Managed I&T management framework
3. APO13:	Managed security
4. APO14:	Managed data
5. DSS05:	Managed security services
6. MEA01:	Managed performance and conformance monitoring
7. MEA02:	Managed system of internal control
8. MEA04:	Managed assurance

[43] Vgl. *Asprion/Burda 2019*.
[44] Nach *Andenmatten 2018*. COBIT® 2019 weist jedoch darauf hin, dass eine Prozessbewertung nach COBIT® 5 bzw. ISO/IEC 33000 weiterhin möglich ist. Die dafür notwendigen Informationen seien komplett in „COBIT 2019® – Framework: Governance and Management Objectives“ enthalten, weswegen es auch keine weitere Publikation zur Prozessbewertung geben wird, vgl. *ISACA 2018a*, S. 38.
[45] Vgl. *ISACA 2018a*, S. 37ff.
[46] Nach *ISACA 2018b*, S. 298.

IT-Ziel 11

In Bezug auf die IT-Compliance mit internen Richtlinien sind es ebenfalls zehn IT-Governance- und IT-Managementziele, von denen jetzt drei IT-Governance- und IT-Managementziele eine primäre, sieben IT-Governance- und IT-Managementziele eine sekundäre Unterstützung leisten, vgl. Tabelle 4. Es liegt eine weitgehend Überschneidung mit den IT-Governance- und IT-Managementzielen vor, die das IT-Ziel 1 unterstützen. Unterschiede ergeben sich im Wesentlichen bei der Qualifizierung der Unterstützung als primär oder sekundär. Nicht enthalten sind lediglich APO13 und APO14, hinzugekommen sind EDM05 (mit Fokus auf die Stakeholder) und DSS06 (mit Fokus auf die Geschäftsprozesse).

Tabelle 4
IT-Ziel 11 unterstützende IT-Governance- und IT-Managementziele[47]

IT-Ziel Nr. 11: IT-Compliance mit internen Richtlinien	
wird primär unterstützt durch ...	
1. APO01:	Managed I&T management framework
2. MEA02:	Managed system of internal control
3. MEA04:	Managed assurance
wird sekundär unterstützt durch ...	
1. EDM01:	Ensured governance framework setting and maintenance
2. EDM03:	Ensured risk optimization
3. EDM05:	Ensured stakeholder engagement
4. DSS05:	Managed security services
5. DSS06:	Managed business process controls
6. MEA01:	Managed performance and conformance monitoring
7. MEA03:	Managed compliance with external requirements

Umfang der Unterstützung

Insgesamt unterstützen 12 von 40 IT-Governance- und IT-Managementzielen das Erreichen der beiden compliance-bezogenen IT-Ziele. Dabei stammen die Prozesse aus der Governance-Domäne und den Management-Domänen APO (Anpassen, Planen und Organisieren), DSS (Bereitstellen, Betreiben und Unterstützen) und MEA (Überwachen, Evaluieren und Beurteilen). Nur in BAI (Aufbauen, Beschaffen und Implementieren) soll sich kein Compliance-Bezug finden. Insgesamt fällt damit der Compliance-Bezug der IT-Governance- und IT-Managementziele nach COBIT® 2019 geringer aus, als dies in COBIT® 5 mit 26 von 37 IT-Prozessen noch das Fall war. Aller-

[47] Nach *ebd.*

dings war doch in einigen der IT-Prozesse von COBIT® 5 der Compliance-Bezug auch nur schwer zu identifizieren.

Die zwölf identifizierten compliance-relevanten IT-Governance- und IT-Managementziele können nun als Ausgangspunkt dienen, um den IT-Compliance-Bezug der einzelnen Komponenten zu analysieren. Die Komponenten dienen damit auch als Struktur der Darstellung. Entsprechend überträgt Abbildung 4 die allgemeine Struktur des Governance-Systems auf die IT-Governance.

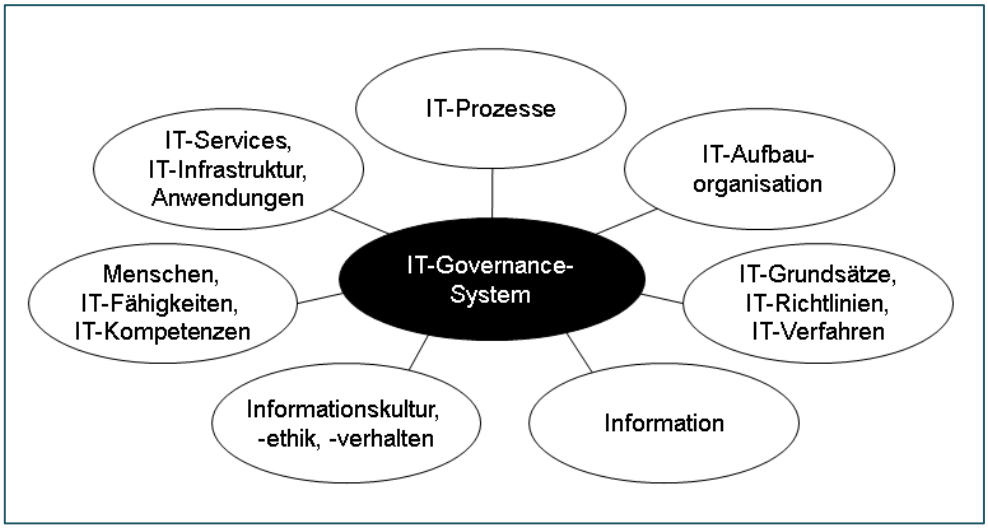

Abbildung 4
Komponenten eines IT-Governance-Systems nach COBIT® 2019[48]

4 IT-Compliance in den Komponenten des IT-Governance-Systems

4.1 Komponente „IT-Prozesse“

Compliance-Bezug in Praktiken und Aktivitäten

Jedes IT-Governance- und IT-Managementziel korrespondiert mit einem entsprechenden IT-Prozess. Die IT-Prozesse untergliedern sich weiterhin hierarchisch in Governance- und Managementpraktiken und diese wiederum in Aktivitäten. Ausgehend von den zwölf IT-Governance- und IT-Managementzielen, die das Erreichen der beiden compliance-bezogenen IT-Ziele unterstützen, gelangt man über 68 Governance- und Managementpraktiken zu letztlich 381 Aktivitäten, die für die prozessuale Ausgestaltung der IT-Compliance herangezogen werden können, vgl. Tabelle 5.

[48] Vgl. *ISACA 2018a*, S. 22; eigene Darstellung.

Domäne	EDM	APO	DSS	MEA	Summe
Prozesse	3	3	2	4	**12**
Praktiken	9	24	13	22	**68**
Aktivitäten	48	140	84	109	**381**

Tabelle 5
Zahl der compliance-relevanten Praktiken und Aktivitäten

Analyse auf der Ebene der Aktivitäten

Die inhaltliche Analyse des Compliance-Bezugs vollzieht sich sinnvollerweise auf der tiefsten Ebene, d. h. auf der Ebene der Aktivitäten. Hier besteht nach wie vor das Problem, dass der Compliance-Bezug nur dann explizit erkennbar ist, wenn Compliance-Begriffe verwendet werden. In EDM01.01 (Evaluate the governance system) sind dies beispielsweise in Aktivität 1 die rechtlichen, regulatorischen und vertraglichen Verpflichtungen oder in Aktivität 3 die Berücksichtigung von externen Vorschriften, Gesetzen und vertraglichen Verpflichtungen.[49] Aber natürlich sind bei übergeordneten Governance-Themen ebenfalls Compliance-Aspekte angesprochen, die dann aber „hineinzuinterpretieren" sind, z. B. wenn es in EDM01.02 (Direct the governance system) um das Etablieren von Governance-Strukturen und -Prozessen (Aktivität 2), die Zuordnung von Zuständigkeiten, Befugnissen und Rechenschaftspflichten (Aktivität 4) oder Kommunikations- und Berichtsmechanismen geht (Aktivität 5).

Werden die IT-Prozesse der IT-Governance- und IT-Managementziele auf diese Weise analysiert, kommt man z. B. für das IT-Governanceziel EDM01 (Ensured Governance Framework Setting and Maintenance) zu folgenden potenziellen Aktivitäten in Bezug auf IT-Compliance, zusammengestellt entlang der zugehörigen Fähigkeitsstufen (F), s. Tabelle 6.

F	Praktik	Aktivität
2	EDM 01.01	1. Analyse und Identifizierung von rechtlichen, regulatorischen u. vertraglichen Verpflichtungen und Compliance-Trends im Geschäftsumfeld, die ggf. das Governance-Design beeinflussen.
		2. Bestimmen der Bedeutung von IT-Compliance und ihrer Rolle im Hinblick auf das Geschäft.
		3. Berücksichtigung von externen Vorschriften, Gesetzen und vertraglichen Verpflichtungen sowie Festlegung, wie sie im Rahmen der IT-Compliance angewendet werden sollen.

Tabelle 6
Aktivitäten aus EDM01 nach Fähigkeitsstufen[50]

[49] Vgl. *ebd.*, S. 29.
[50] Vgl. *ebd.,* S. 29-31

F	Praktik	Aktivität
		4. Ermittlung der Auswirkungen des gesamten Kontrollumfelds des Unternehmens in Bezug auf IT-Compliance.
	EDM 01.02	1. Kommunikation der Governance von IT-Compliance-Grundsätzen und Abstimmung mit dem Top-Management, um zu einer fundierten und engagierten Führung in Bezug auf IT-Compliance zu gelangen.
		2. Etablierung oder Delegation der Einrichtung von Compliance-Strukturen, -Prozessen und -Praktiken im Einklang mit vereinbarten Designprinzipien für IT-Compliance.
		3. Einrichtung eines IT-Governance-Boards, das die IT-Compliance als Teil der Corporate Compliance sicherstellt, über die Compliance-Ausrichtung berät und IT-Compliance-Programme im Einklang mit den Compliance-Prioritäten des Unternehmens priorisiert.
3	EDM 01.01	5. Ausrichtung der ethisch verantwortbaren Informationsverarbeitung und ihrer Folgen für Gesellschaft, natürliche Umwelt und Interessen interner/externer Stakeholder auf die Complianceziele des Unternehmens.
		6. Formulierung von Prinzipien, an denen sich die Gestaltung des Compliance-Systems und die Entscheidungsfindung für IT-Compliance orientieren können.
		7. Bestimmung des optimalen Entscheidungsmodells für IT-Compliance.
		8. Festlegung geeigneter Ebenen für die Delegation von Zuständigkeiten, inklusive Reglung von Schwellwerten, für IT-Compliance-Entscheidungen.
	EDM 01.02	4. Zuweisung von Zuständigkeiten, Befugnissen und Rechenschaftspflichten für IT-Compliance-Entscheidungen im Einklang mit Governance-Designprinzipien für IT-Compliance, Entscheidungsmodelle und Übertragung von Compliance-Aufgaben.
		5. Sicherstellung, dass die Kommunikations- und Berichtsmechanismen den Verantwortlichen für Compliance-Überwachung und -Entscheidungsfindung angemessene Informationen zur Verfügung stellen.
		6. Veranlassung, dass die Mitarbeiter relevante IT-Richtlinien befolgen, und Sicherstellung, dass die Folgen von Verstößen bekannt sind und durchgesetzt werden.
		7. Anleitung der Etablierung eines Belohnungssystems zur Förderung des wünschenswerten Compliance-Wandels.
	EDM 01.03	1. Bewertung der Effektivität und Leistung von Stakeholdern, denen Zuständigkeiten und Befugnisse für die IT-Compliance übertragen wurden.

F	Praktik	Aktivität
4	EDM 01.03	2. Regelmäßige Beurteilung, ob vereinbarte IT-Compliance-Mechanismen (Strukturen, Prinzipien, Prozesse usw.) etabliert sind und effektiv funktionieren.
		3. Bewertung der Wirksamkeit des Governance-Designs für IT-Compliance und Identifizierung von Maßnahmen zur Behebung festgestellter Compliance-Mängel.
		4. Überwachung des Umfangs, in dem die IT ihren Verpflichtungen (Regulierungsvorgaben, Gesetzen, Verträgen), internen Richtlinien, Normen/Standards und professionellen Leitlinien nachkommt.
		5. Überwachung der Wirksamkeit und Einhaltung des Kontrollsystems des Unternehmens in Bezug auf IT-Compliance.
		6. Überwachung von regulären und routinemäßigen Mechanismen, um sicherzustellen, dass die IT-Nutzung den einschlägigen Verpflichtungen (Regulierungsvorgaben, Gesetzen, Verträgen), Normen/Standards und Richtlinien entspricht.
F = Fähigkeitsstufe; grau unterlegte Aktivitäten haben einen expliziten Compliance-Bezug		

Wie zu erkennen, werden im IT-Governanceziel EDM01 lediglich die Fähigkeitsstufen

- 2 (Gemanagt: Planung und Leistungsmessung finden statt, wenn auch noch nicht in standardisierter Form),
- 3 (Definiert: Unternehmensweite Standards bieten Anleitungen für das gesamte Unternehmen) und
- 4 (Quantitativ: Das Unternehmen ist datengesteuert und erzielt eine quantitative Leistungssteigerung)

adressiert.[51] Nur in vier der 21 Aktivitäten ist der IT-Compliance-Bezug ausdrücklich und damit leicht identifizierbar. In allen anderen Fällen muss eine situationsspezifische Interpretation erfolgen.

Weitere Praktiken mit offensichtlichen, compliance-bezogenen Aktivitäten in den Domänen APO, BAI und DSS enthält die Tabelle in Anhang A. Hier zeigt sich, dass wesentlich mehr IT-Managementziele das Erreichen der compliance-bezogenen IT-Ziele unterstützen, als in der Mapping-Tabelle der Zielkaskade identifiziert sind.

[51] Vgl. *ISACA 2018a*, S. 40.

Referenzierte Dokumente

Teil der Beschreibung der Prozesspraktiken ist zudem eine Auflistung der in den Praktiken referenzierten Dokumente (Standards, Normen etc.). Genannt werden für EDM01 die (nicht frei zugängliche) CMMI Cybermaturity Platform, die ISO/IEC 38500:2015, ITIL® V3 und der NIST-Standard 800-37, Revision 2 (Draft), May 2018. Hier zeigen sich nach wie vor die bekannten Probleme mit den von COBIT® referenzierten Regelwerken:

- Mangelnde Zugreifbarkeit: Verschiedene Dokumente sind nicht frei verfügbar, sondern stehen erst nach Kauf oder kostenpflichtiger Registrierung zur Verfügung.
- Mangelnde Aktualität: Die Normen und Standards ändern sich in ihrer Summe so schnell, dass sich COBIT® 2019 bereits kurz nach seinem Erscheinen auf veraltete Dokumentenversionen bezieht. So ist beispielsweise der NIST-Standard 800-37 Rev. 2 mittlerweile seit Dezember 2018 verabschiedet und publiziert, während sich COBIT® 2019 noch auf die Draft-Version vom Mai 2018 bezieht. Auch das SFIA liegt seit 2018 in einer siebten Version vor, COBIT® 2019 bezieht sich noch auf Version 5 von 2015.
- Unklare Bezüge: Die Referenzierungen weisen in COBIT® 2019 immerhin keine Lücken mehr auf. Trotzdem sind sie sehr vereinzelt und wirken damit beliebig. So wird für das IT-Governanceziel EMD01 aus der ISO/IEC 38500:2015 lediglich das Verantwortungsprinzip referenziert. In diesem ersten der von der Norm postulierten sechs Prinzipien der IT-Governance geht es um die Kenntnis und Akzeptanz der Verantwortlichkeiten für IT-Nachfrage und -Angebot.[52] Für die einzelnen Ausführungen der Norm lassen sich Bezüge zur Governancepraktik EDM01.01 herstellen, wenn nach der Norm Optionen für die Zuordnung von Verantwortlichkeiten für den IT-Einsatz bewertet werden sollen und in der 8. Prozessaktivität Ebenen für die Delegation von Zuständigkeiten festzulegen sind. Ebenso bezieht sich die Prozessaktivität 5 bzgl. der IT-Nutzung auf die Empfehlung der ISO/IEC 38500, dass sich diese an den aktuellen und künftigen Unternehmenszielen auszurichten hat. Trotzdem lassen sich diese Bezüge nicht eindeutig klären.[53]
- Mangelnde Abdeckung: Noch kritischer ist die mangelhafte Abdeckung der Regelwerke durch die Prozessbeschreibungen von COBIT® 2019.

[52] Vgl. *Klotz 2008*, S. 21.
[53] Vgl. *ISACA 2018b*, S. 29 und *ISO/IEC 38500*, S. 8.

So ist z. B. unverständlich, warum das Konformitätsprinzip der ISO/IEC 38500, bei dem es die Konformität der IT mit rechtlichen Vorgaben, Normen, professionellen Standards etc. geht,[54] keine Erwähnung in den Prozessaktivitäten von EDM01 findet. So ist beispielsweise ein Bezug von der Empfehlung der ISO/IEC 38500, eine regelmäßige Bewertung des Ausmaßes vorzunehmen, in dem die IT ihren regulatorischen, gesetzlichen und vertraglichen Verpflichtungen nachkommt, ohne Problem zur 4. Prozessaktivität der Governancepraktik EDM01.03 herzustellen, die eine Überwachung des Umfangs, in dem die IT u. a. eben diese Verpflichtungen erfüllt, fordert.[55]

- Mangelnder Umfang: Und schließlich ist auch zu konstatieren, dass COBIT® 2019 trotz der Steigerung der referenzierten Regelwerke auf 32 doch eher wenige der verbreiteten IT-Standards und -Normen berücksichtigt. Warum wurden bei der Überarbeitung nicht weitere Normen der ISO/IEC 38500er-Reihe hinzugezogen, z. B. die ISO/IEC 38505 zu Data Governance?[56] Oder auch die ISO/IEC 27014 als Governance-Norm für die IT-Sicherheit?[57] Dass nach wie vor keine gesetzlichen Vorgaben mit globaler Bedeutung, z. B. die EU-Datenschutzgrundverordnung (DSGVO), ausdrücklich adressiert werden, ist als weiterer Nachteil zu werten.

Natürlich ist nicht zu erwarten, dass deutsche Standards und Normen Eingang in COBIT® finden. Und es ist auch zu diskutieren, welches die relevanten, wichtigen Normen, Standards und Rahmenwerke sind. Trotzdem erscheint die Auswahl sowohl der Regelwerke als auch der berücksichtigten Passagen eher willkürlich. Von einer systematischen Analyse und Berücksichtigung der verschiedenen Regelwerke für IT-Governance und IT-Management kann somit keine Rede sein – was bedeutet, dass COBIT® 2019 seinem eigenen Prinzip für Governance-Rahmenwerke[58] („Aligned to Major Standards“) nur sehr ungenügend nachkommt.

---

[54] Vgl. *Klotz 2008*, S. 21.
[55] Vgl. *ISACA 2018b*, S. 31 und *ISO/IEC 38500*, S. 10.
[56] Vgl. die Darstellung der Normenreihe in *Klotz 2016a*.
[57] COBIT® 2019 führt nur sieben ISO/IEC-Normen auf. In *Klotz 2013* wurden aber bereits 25 für IT-Governance und IT-Management relevante ISO/IEC-Normen identifiziert.
[58] Siehe Kapitel 2.

4.2 Komponente „IT-Prozesse“ – MEA-Domäne

MEA-Domäne

Die MEA-Domäne "Überwachen, Evaluieren und Beurteilen" gliedert sich in COBIT® 2019 nunmehr in vier IT-Managementziele.

- MEA01 fokussiert das Erreichen von Leistungs- und Konformitätszielen,
- MEA02 befasst sich mit dem internen Kontrollsystem.
- MEA03 adressiert die Compliance mit externen Anforderungen.
- MEA04 richtet sich auf das Management von Prüfungen.

Alle vier IT-Managementziele unterstützen jeweils die beiden compliance-bezogenen IT-Ziele, vgl. Abbildung 5.

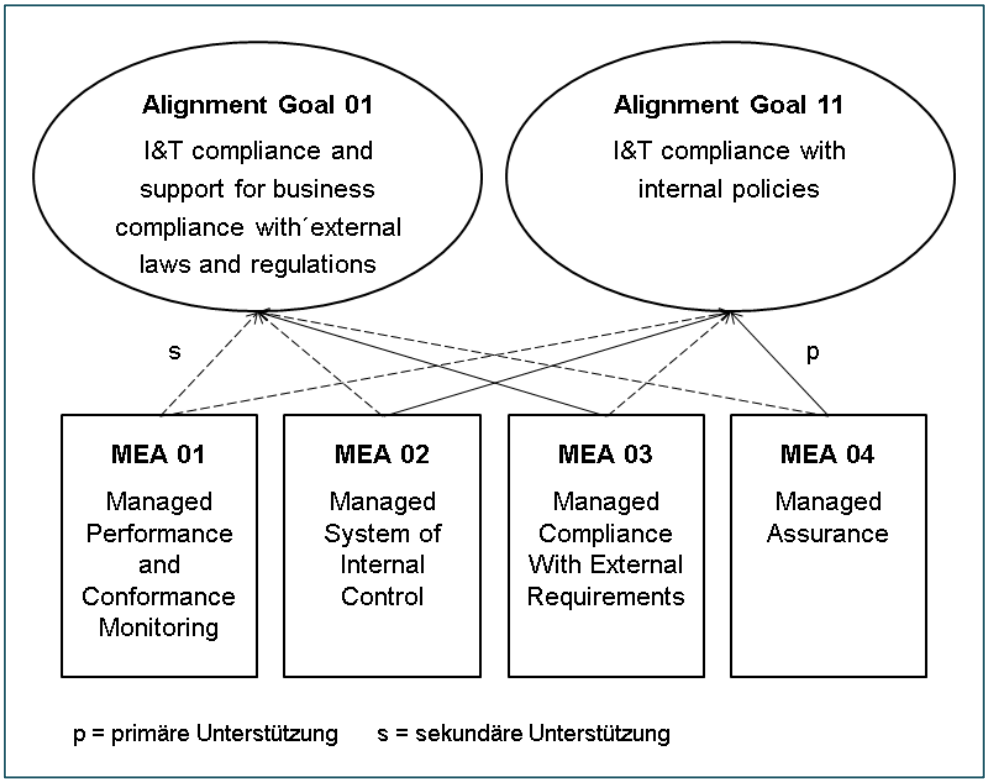

Abbildung 5
Von den MEA-Managementzielen unterstützte compliance-bezogene IT-Ziele[59]

Komponente „Prozesse“

Die vier IT-Managementziele der MEA-Domäne sind in insgesamt 22 Managementpraktiken unterteilt, denen wiederum insgesamt 109 Aktivitäten zu-

[59] Eigene Darstellung.

geordnet sind. Die Untergliederung der Prozesse in Managementpraktiken zeigt Tabelle 7.

Tabelle 7
Managementpraktiken der MEA-Domäne[60]

Nr.	MEA01	MEA02	MEA03	MEA04
.01	Einrichten eines Überwachungsansatzes	Überwachen interner Kontrollen	Identifizieren externer Compliance-Anforderungen	Sicherstellen der Unabhängigkeit und Qualifikation der Prüfer
.02	Festlegen von Leistungs- und Konformitätszielen	Überprüfen der Effektivität von Geschäftsprozesskontrollen	Optimieren der Reaktion auf externe Anforderungen	Risikobasierte Planung von Prüfinitiativen
.03	Erfassen und Verarbeiten von Leistungs- und Konformitätsdaten	Durchführen von Selbsteinschätzungen zu Kontrollen	Bestätigen der externen Compliance	Festlegung der Ziele der Prüfinitiativen
.04	Analysieren und Berichten der Leistung	Identifizieren und Melden von Kontrollschwächen	Erhalten von Compliance-Bestätigungen	Festlegen des Umfangs von Prüfinitiativen
.05	Sicherstellen der Implementierung korrektiver Maßnahmen			Festlegen des Arbeitsprogramms der Prüfinitiativen
.06				Durchführung von Prüfinitiativen mit Fokus auf die Effektivität des Prüfkonzepts
.07				Durchführung von Prüfinitiativen mit Fokus auf die operative Effektivität
.08				Bericht und Nachbereitung von Prüfinitiativen
.09				Verfolgung von Empfehlungen und Maßnahmen

MEA03-Zusammenhänge

Mit Blick auf die Bezeichnungen der IT-Managementziele beinhaltet MEA03 (Managed Compliance With External Requirements) die zentralen compli-

[60] Nach *ISACA 2018b*, S. 276, 281, 287, 293; Übersetzung weitgehend übernommen aus *ISACA 2012b*, S. 206, 210, 215.

ancebezogenen Prozesspraktiken und -aktivitäten von COBIT® 2019. Die Komponenten von MEA03 sollen sicherstellen, dass das Unternehmen alle geltenden externen Anforderungen erfüllt. Zudem ist IT-Compliance in die Corporate Compliance des Unternehmens zu integrieren.[61] In MEA01 werden die Ziele der Überwachung und damit auch die Complianceziele, in MEA02 die Kontrollumgebung und das interne Kontrollsystem (IKS) und damit die Infrastruktur der Überwachung sowie in MEA04 der Umgang mit Compliancеprüfungen festgelegt. MEA03 basiert somit notwendig auf den in MEA01 und MEA02 getroffenen Festlegungen und seine Ergebnisse bilden ggf. den Prüfungsgegenstand in MEA04.

MEA01

Der Zweck von MEA01 „Managed Performance and Conformance Monitoring“, besteht in der Transparenz über Leistung und Konformität und dem Fördern der diesbezüglichen Zielerreichung. Die Praktiken richten sich im Wesentlichen auf die Festlegung von Zielen und Metriken, die sich eben auch auf Konformität (Compliance) beziehen. Diese IT-bezogenen Complianceziele und -metriken müssen in das Überwachungssystem des Unternehmens integriert und im Unternehmen kommuniziert sein, die Zielerreichung muss systematisch gemessen und entsprechende Berichte müssen zielgruppenadäquat und zeitgerecht zur Verfügung gestellt werden. Die Angemessenheit von Zielen, Metriken und Berichten ist regelmäßig zu bewerten, Anpassungen sind im Rahmen eines Änderungsmanagements vorzunehmen. Werden bei der Messung der Zielerreichung wesentliche Abweichungen festgestellt, so sind korrektive Maßnahmen zu ergreifen und bis zur Problemlösung zu verfolgen. Auch Status und Ergebnis der Maßnahmen sind kontinuierlich zu berichten.[62]

MEA02

Im Mittelpunkt von MEA02 „Managed System of Internal Control“ steht das interne Kontrollsystem. MEA02 zielt vor allem darauf ab, die Angemessenheit und Effektivität des IKS für verschiedene Stakeholder nachzuweisen. Hierzu müssen interne Kontrollen eingerichtet und eventuelle Schwachstellen identifiziert und gemeldet werden. In Bezug auf IT-Compliance stehen Compliance-Kontrollen (und entsprechende Schwachstellen) im Vordergrund. Diese sind im Rahmen des Kontrollsystems risikoorientiert zu konzipieren, zu implementieren und in ihrer Wirksamkeit zu evaluieren. Ergebnisse sind zu kommunizieren, Schwachstellen nachvollziehbar zu beseitigen. Bei der Überwachung interner Kontrollen ist nicht nur die interne

[61] Vgl. *ISACA 2018b*, S. 285
[62] Vgl. *ebd.*, S. 273-275.

Sicht erforderlich, sondern es ist explizit darauf zu achten, dass auch beauftragte Serviceanbieter ihre gesetzlichen, behördlichen und vertraglichen Verpflichtungen erfüllen.[63]

MEA03

Durch MEA03 "Managed Compliance With External Requirements" soll sichergestellt werden, dass das Unternehmen alle anwendbaren externen Anforderungen identifiziert und einhält. Das IT-Managementziel selbst gliedert sich in vier Managementpraktiken, die den Inhalt und den Umfang des Managements der extern orientierten IT-Compliance wiedergeben.[64]

- Compliance-Anforderungen resultieren nach MEA03.01 aus nationalen und internationalen „gesetzlichen, behördlichen und sonstigen externen vertraglichen Anforderungen …, die relevant für die Nutzung von IT-Ressourcen und die Verarbeitung von Informationen innerhalb der geschäftlichen und IT-bezogenen Abläufe des Unternehmens sind“.[65] Als spezielle Bereiche werden „Datenschutz, interne Kontrollen, Finanzberichtswesen, branchenspezifische Bestimmungen, geistiges Eigentum, Gesundheit und Sicherheit“[66] genannt. Damit die maßgeblichen Anforderungen abgestimmt gemanagt werden können, wird die Führung eines integrierten Verzeichnisses („compliance requirements register“) empfohlen. Dieses stellt die Basis für die Analyse der Auswirkungen der Compliance-Anforderungen und die Festlegung erforderlicher Maßnahmen dar. Soweit erforderlich, ist auf externe Hilfe zurückzugreifen.
- MEA03.02 richtet sich auf die Anpassung an geänderte Compliance-Anforderungen. Um zeitnah auf neue oder geänderte Vorgaben reagieren und Compliance herstellen zu können, bedarf es eines internen Prozesses der Identifikation sowie der Umsetzung durch IT-Richtlinien, -Standards und -Verfahren, die regelmäßig zu bewerten und anzupassen sind. Wichtig ist die Kommunikation von Neuerungen und Änderungen in die betroffenen Stellen und Abteilungen des Unternehmens.
- Die Compliance der unternehmensintern verwendeten Richtlinien, Prinzipien, Standards, Verfahren und Methoden mit gesetzlichen, behördlichen und vertraglichen Anforderungen ist nach MEA03.03 regelmäßig

---

[63] Vgl. *ebd.*, S. 279-281.
[64] Vgl. im Folgenden *ebd.*, S.285-286.
[65] *ISACA 2012b*, S. 21. Die Beschreibung der Aktivitäten entspricht in COBIT® 2019 derjenigen in COBIT® 5 (bis auf die Änderung von „IT“ in „I&T“). Entsprechend wird die deutsche Übersetzung aus COBIT® 5 an dieser Stelle übernommen.
[66] *Ebd.*

durch interne und externe Überprüfungen zu überwachen und zu beurteilen. Die Überprüfung der Compliance hat sich sowohl auf Geschäfts- als auch auf IT-Prozesse, in denen die verschiedenen Regelwerke zum Einsatz gelangen, zu beziehen. Wurden Compliance-Lücken festgestellt, sind diese zu dokumentieren und zeitnah Maßnahmen mit dem Ziel der Anpassung der betroffenen Regelwerke, IT- oder Geschäftsprozesse einzuleiten.

- MEA03.04 richtet sich auf die Dokumentation der Compliance, die als Ergebnis aus internen und externen Überprüfungen resultiert. Eine wichtige Rolle spielen hierbei die Prozesseigner (engl. process owner), die die Compliance des von ihnen verantworteten Geschäfts- oder IT-Prozesses zu bestätigen haben. Gleiches gilt für IT-Dienstleister und Geschäftspartner. Die Ergebnisse – insbesondere zu Non-Compliance-Vorfällen und ihren Ursachen sowie zu ergriffenen Maßnahmen – sind in die generelle Berichterstattung des Unternehmens zu integrieren.

4.3 Komponente „IT-Aufbauorganisation“

Verändertes RACI-Modell

Die (IT-)Aufbauorganisation wird in COBIT® 2019 durch das RACI-Rollenmodell verkörpert (R = responsible, A = accountable, C = consulted, I = informed), allerdings nur noch durch Beteiligungsformen, die Verantwortung tragen.[67] So finden sich nunmehr nur noch A- und R-Rollen wieder, was nicht unbedingt als Verbesserung gesehen werden muss. Zwar waren die C- und I-Beteiligungen sicherlich diejenigen, die aufgrund der organisatorischen Gegebenheiten und Prioritäten – so argumentiert COBIT® 2019[68] – im praktischen Anwendungsfall am häufigsten anzupassen waren; trotzdem boten sie doch eine Orientierung. A- und R-Verantwortung unterscheidet COBIT® 2019 wie folgt:[69]

R-Verantwortung

- Träger der R-Verantwortung spielen die wichtigste operative Rolle bei der Erfüllung der Governance- oder Managementpraktik. Sie erstellen im Wesentlichen das angestrebte Ergebnis. Träger mit R-Verantwortung lassen sich durch Beantwortung der beiden Fragen identifizieren:
  - Wer hat die Aufgabe zu erledigen?
  - Wer treibt die Aufgabenbearbeitung an?

[67] Vgl. *Gaulke 2019*, S. 6.
[68] Vgl. *ISACA 2018b*, S. 22.
[69] Nach *ebd.*

- Trägern der A-Verantwortung kommt eine Gesamtverantwortung zu. Damit wird häufig eine – nicht teilbare – Rechenschaftspflicht gegenüber höheren Instanzen verbunden.[70] Aus diesem Grunde liegt auch häufig die Personal- und Budgetverantwortung bei ihnen. Trägern mit A-Verantwortung lassen sich identifizieren durch Beantwortung der Frage:

  - Wer ist für den Erfolg und die Zielerreichung der Aufgabe zuständig?

A-Verantwortung

Organisatorische Einheiten/Rollen

Das RACI-Diagramm verbindet jede IT-Governance- oder IT-Managementpraktik mit aufbauorganisatorischen Einheiten (Stellen/Gremien) bzw. Rollen. Damit ist es möglich, eine durchgängige Verantwortungsstruktur für die zahlreichen Handlungsfelder der IT-Governance und des IT-Managements zu entwickeln – auch für IT-Compliance. Gegenüber COBIT® 5 sind die aufbauorganisatorischen Einheiten und Rollen von 26 auf 33 erweitert worden.[71] Die Organisationseinheit „Compliance“ bleibt genauso wie der „Privacy Officer“ bestehen. „Compliance“ bezeichnet eine Funktion, die für alle Regelungen zur externen Compliance verantwortlich ist. Der „Privacy Officer“ ist die verantwortliche Stelle für die Überwachung von Risiken und geschäftlichen Auswirkungen von Datenschutzgesetzen. Weiterhin ist die Stelle zuständig für die Steuerung und Koordination der Umsetzung von Richtlinien und Aktivitäten, die die Einhaltung von Datenschutzrichtlinien sicherstellen. COBIT® 2019 weist – vielleicht vor dem Hintergrund der DSGVO – ausdrücklich darauf hin, dass der Privacy Officer in einigen Unternehmen als Datenschutzbeauftragter (data protection officer) bezeichnet wird.[72] Als compliance-relevante Einheit ist die Rechtsberatung (legal counsel) hinzugekommen, die verantwortlich zeichnet für die Beratung in rechtlichen und regulatorischen Fragen.

Bezug zum 3LoD-Modell

COBIT® 2019 deckt damit in noch höherem Maße als die Vorgängerversion das auf die Steuerung und Überwachung der Unternehmens-IT anwendbare Modell der „Three lines of Defense“ (3Lod-Modell) ab.[73] Aufsichtsorgan und Unternehmensleitung sind mit dem Board und Executive Committee sowie die einzelnen C-Positionen (inkl. dem Chief Information Officer – CIO) vertreten, ergänzt um Gremien, wie das I&T-Governance-Board. Die

[70] Vgl. *Gaulke 2014*, S. 62.
[71] Vgl. *ISACA 2018b*, S. 21f.
[72] Nach *ebd.*
[73] Vgl. *Klotz 2016b*.

erste Verteidigungslinie beinhaltet Geschäftsprozessverantwortliche und IT-Management, die zweite Verteidigungslinie Bereiche, wie Information Security, Compliance, Datenschutzbeauftragter (DSB), Legal, Project Management Office, und die dritte Verteidigungslinie den Audit-Bereich. COBIT® 2019 ist somit grundlegend geeignet, IT-Compliance als Funktion bzw. Stelle in der Verantwortungsstruktur für IT-Governance und IT-Management zu verorten und die organisatorischen Schnittstellen zu klären.

Umfang der Beteiligung von Compliance und DSB

In COBIT® 5 war die Organisationseinheit „Compliance“ noch an 68 % der IT-Governance- und IT-Managementpraktiken beteiligt, v. a. in den Formen C (befragt) und I (informiert), aber immerhin auch mit zwei A- und elf R-Verantwortungen in den drei Domänen APO, BAI und MEA.[74] Diese Beteiligung ist in COBIT® 2019 stark reduziert. Die Organisationseinheit „Compliance“ ist nur noch in der Managementpraktik MEA03 in einer verantwortlichen Rolle tätig. Dagegen ist die Position des Datenschutzbeauftragten immerhin noch an 39 von 228 IT-Governance- und IT-Managementpraktiken in den Domänen APO (17), BAI (11), DSS (5) und MEA (6) in einer R-Verantwortung beteiligt.

Mit Blick auf die relativ hohe Zahl der compliance-relevanten Praktiken und Aktivitäten, s. Tabelle 5, ist der geringe Umfang der operativen Beteiligung der Organisationseinheit „Compliance“ verwunderlich. Diese starken Detailveränderungen in der Abfolge der COBIT-Versionen zeigen dann aber eben auch, dass COBIT® „nur“ eine Best-Practice-Sammlung ist, die auf Meinungen und Erfahrungen vieler Fachleute und nicht auf Forschungsergebnissen beruht. Dies sollte immer wieder zur kritischen Reflexion des COBIT®-Frameworks Anlass geben.

4.4 Komponente „Information“

Informationskomponente in COBIT® 2019

Die Informationskomponente in COBIT® 2019 wird im Wesentlichen gespeist von den In- und Outputs, die in COBIT® 5 direkt bei den Praktiken angesiedelt waren und jetzt durch den Praktiken zugeordnete Informationsflüsse und -objekte („Information flows and Items“) gebildet werden. COBIT® 2019 hat aus „COBIT 5 Enabling Information“ das Referenzmodell für Information mit 15 Qualitätskriterien, die zu drei übergeordneten Kriterien gruppiert sind[75], übernommen. Diese Kriterien bilden die Basis für

[74] Vgl. *Klotz 2014*, S. 32f.
[75] Diese drei Gruppen sind: (1) intrinsisch, d. h. Ausmaß in dem die Datenwerte mit aktuel-

das Performancemanagement in Bezug auf Informationsobjekte.[76] Letztlich geht es weiterhin darum, die Informationsobjekte als In- und Outputs der Prozesspraktiken bzw. -aktivitäten effektiv und effizient zu managen.

Compliancebezogene Informationsflüsse und -objekte

Aus Sicht der IT-Compliance ist somit interessant, welche compliancebezogenen Informationsflüsse und -objekte vorliegen müssen. Dies resultiert auch daraus, dass Informationsflüsse und -objekte als Informationsinhalte und -träger Gegenstand der Prozessaktivitäten und damit auch Objekt der Beurteilung sind, ob Aktivitäten bestimmten Fähigkeitsstufen entsprechen. Für eine Analyse, welche compliancebezogenen Informationsflüsse und -objekte in COBIT® 2019 vorgesehen sind, bilden die Angaben derjenigen IT-Governance- und IT-Managementziele, die die compliancebezogenen IT-Ziele unterstützen, den Ausgangspunkt, s. Tabellen 3 und 4. Die Identifizierung ist immer dann schwierig, wenn Compliance-Inhalte nicht explizit angesprochen sind. Im IT-Governanceziel EDM01 sind beispielweise folgende Informationsin- und -outputs als Complianceobjekte leicht erkennbar:

- Gesetze, regulative Vorgaben (Input in EDM01.01)
- Compliance-Prüfberichte (Input in EDM01.03)
- Berichte zu Fällen von Non-Compliance und Ursachen (Input in EDM01.03)

Allerdings könnte sich auch das Feedback zur Governanceeffektivität und -leistung (Outut von EDM01.03) auf Complianceaspekte beziehen. Entscheidungsmodelle (Output von EDM01.01) werden auch für Compliance-Entscheidungen zum Einsatz gelangen. Der Ansatz zum Belohnungssystem (Output von EDM01.02) könnte auch Anreize für regelkonformes Verhalten umfassen. Die Resultate der Reviews von Self-Assessments (Input von EDM01.03) können auch Compliance-Bewertungen umfassen. Compliance kann also immer auch in derartigen themenneutralen Informationsflüssen oder -trägern enthalten sein.[77]

MEA03

Informationsflüsse und -objekte, deren Benennung einen offensichtlichen Compliance-Bezug haben, fallen vorwiegend im IT-Managementziel

---

len oder wahren Werten übereinstimmen; (2) kontextabhängig: Ausmaß, in dem Informationen für die Aufgabe des Informationsnutzers nutzbar sind und in verständlicher und klarer Weise dargestellt werden; (3) Sicherheit/Datenschutz/Zugänglichkeit: Das Ausmaß, in dem Informationen verfügbar oder erhältlich sind; vgl. *ISACA 2013*, S. 31ff.

[76] Vgl. *ISACA 2018a*, S. 42.

[77] Vgl. *ISACA 2018b*, S. 32.

MEA03 an, vgl. Tabelle 8.

Tabelle 8
Informationsflüsse und -objekte mit Compliance-Bezug

Lfd. Nr.	Praktik	Input/ Output	Informationsobjekt
1	EDM01.01	Input	• Gesetze, regulative Vorgaben
2	EDM01.03	Input Input	• Compliance-Prüfberichte • Berichte zu Fällen von Non-Compliance und Ursachen
3	MEA01.03	Input	• Ergebnisse von Überprüfungen bzgl. der Überwachung der Lieferanten-Compliance
4	MEA01.05	Input	• Korrekturmaßnahmen bei Fällen von Non-Compliance
5	MEA02.02	Input	• Ergebnisse von Compliance-Prüfungen
6	MEA03.01	Input	• Gesetzliche und regulatorische Compliance-Anforderungen
7		Output	• Protokoll der erforderlichen Compliance-Maßnahmen
8		Output	• Register der Compliance-Anforderungen
9	MEA03.02	Output	• Kommunikation geänderter Compliance-Anforderungen
10		Output	• Aktualisierte Richtlinien, Grundsätze, Verfahren und Standards
11	MEA03.03	Input	• Ergebnisse von Compliance-Prüfungen
12			• Ergebnisse von Prüfungen der installierten Lizenzen
13		Input	• Lizenzabweichungen
14		Output	• Compliance-Bestätigungen
15		Output	• Identifizierte Compliance-Lücken
16	MEA03.04	Output	• Compliance-Prüfberichte
17		Output	• Berichte zu Fällen von Non-Compliance und Ursachen

Wie diese einzelnen Informationsobjekte inhaltlich und formal auszugestalten sind, muss unternehmensspezifisch festgelegt werden.[78]

[78] COBIT® 5 bot hierfür noch ein informationsbezogenes Rollenmodell, das grob zwischen Informationsproduzenten, -verwaltern und -konsumenten unterschied, vgl. *ISACA 2013*, S. 28. Ein derartiger Ansatz ist in COBIT® 2019 erst einmal nicht mehr vorhanden.

4.5 Weitere Komponenten

In den weiteren Beschreibungen der Komponenten wird auf die verschiedenen von COBIT® 2019 referenzierten Regelwerke verwiesen, die zu dem IT-Governance- oder IT-Managementziel passende Bezüge beinhalten bzw. als Input in COBIT 2019® eingegangen sind. Da sich die Ausführungen auf das jeweilige IT-Governance- oder IT-Managementziel insgesamt beziehen, sind hier i. d. R. kaum spezifische Bezüge zu IT-Compliance herzustellen. Für Compliance relevante Verweise finden sich – wie zu erwarten – lediglich in der MEA-Domäne:

Menschen, IT-Fähigkeiten, IT-Kompetenzen

- Für die Komponente „Menschen, IT-Fähigkeiten, IT-Kompetenzen" verweist MEA01 auf das „Skills Framework for the Information Age V6" und fordert Kompetenz zur Durchführung von Konformitätsprüfungen.[79] SFIA versteht hierunter die Fähigkeit zur unabhängigen Bewertung der Konformität von Aktivitäten, Prozessen, Ergebnissen, Produkte oder Services mit Kriterien von Standards, Best Practices oder anderen dokumentierten Anforderungen.[80] Diese Fähigkeiten werden in SFIA für vier unterschiedliche Verantwortungsebenen beschrieben.[81]

IT-Grundsätze, IT-Richtlinien, IT-Verfahren

- Für die Komponente „IT-Grundsätze, IT-Richtlinien, IT-Verfahren" beinhaltet MEA01 Richtlinien zu Self-Assessments einerseits und zu Hinweisgebersystemen andererseits.[82] Den Kern dieser Komponente bilden jedoch zwei Richtlinien: eine Datenschutzrichtlinie und eine Compliance-Richtlinie. Die Datenschutzrichtlinie trifft Regelungen zur Sammlung, Verwendung, Offenlegung, Weitergabe und Verwaltung von personenbezogenen Daten. Hierdurch sichert sie vor allem die Umsetzung gesetzlicher Datenschutzvorschriften.[83] Die Compliance-Richtlinie trifft Regelungen
  - zur Identifizierung regulatorischer, vertraglicher und interner Compliance-Anforderungen,
  - zum Prozess der Beurteilung der Compliance mit regulatorischen, vertraglichen und internen Anforderungen und den Rollen und Verantwortlichkeiten im Rahmen der Prozessdurchführung,

[79] *ISACA 2018b*, S. 277.
[80] Nach *SFIA 2018*, S. 116.
[81] Vgl. *ebd.*, S. 116f. Insgesamt werden Fähigkeiten in SFIA mittels sechs Verantwortungsebenen beschrieben.
[82] Vgl. *ISACA 2018b*, S. 278.
[83] Nach *ebd.*, S. 149.

- zu Leitlinien für Kennzahlen zur Messung der Compliance,
- zu Compliance-Berichten und
- zur Überprüfung von Compliance- oder Korrekturmaßnahmen zur Behebung von Compliance-Lücken.[84]

IT-Kultur, -ethik, -verhalten

- Für die Komponente „IT-Kultur, -ethik, -verhalten“ fordert MEA03 eine compliance-bewusste Kultur, zu der vor allem eine Null-Toleranzpolitik hinsichtlich Non-Compliance bzgl. gesetzlicher und regulatorischer Vorgaben zählt.[85] In der Zusammenarbeit mit IT-Dienstleistern sind diesbezüglich Vertragsstrafen bei Non-Compliance vorzusehen.[86]

IT-Services, IT-Infrastruktur, Anwendungen

- Für die Komponente „IT-Services, IT-Infrastruktur, Anwendungen“ empfiehlt MEA01 den Einsatz von Self-Assessment-Tools.[87] MEA03 sieht die Nutzung von Dienstleistungen für Compliance-Prüfungen durch Dritte vor.[88] Weitere Systeme, die IT-Compliance unterstützen, sind Vertragsmanagementsysteme[89] sowie Tools für Governance, Risk und Compliance (GRC)[90].

5 IT-Compliance im Rahmen des COBIT® 2019 Design Guide

5.1 Design-Ansatz von COBIT® 2019

Individuelles IT-Governance-System

COBIT® 2019 geht für seinen Design-Ansatz davon aus, dass jedes Unternehmen sein eigenes IT-Governance-System gemäß seinen individuellen Besonderheiten entwickeln muss. Jedes Unternehmen unterscheidet sich von anderen Unternehmen beispielsweise hinsichtlich seiner Unternehmensgröße, Branche, Regulierungs- und Bedrohungssituation. All diese Aspekte, die COBIT® 2019 als Designfaktoren bezeichnet, erfordern, dass Unternehmen ihr IT-Governance-System situationsspezifisch ausrichten, so dass sie den größtmöglichen Nutzen aus dem IT-Einsatz erzielen.[91] Dementspre-

[84] Nach *ebd.*, S. 288.
[85] Nach *ebd.*
[86] Nach *ebd.*, S. 117.
[87] Vgl. *ebd.*, S. 278.
[88] Vgl. *ebd.*, S. 288.
[89] Vgl. *ebd.*, S. 117.
[90] Vgl. *ebd.*, S. 137.
[91] Nach *ISACA 2018c*, S. 15.

chend haben die von COBIT® 2019 formulierten Designfaktoren, vgl. Abbildung 6, wesentlichen Einfluss auf das Design des IT-Governance-Systems eines Unternehmens.

Einfluss von Compliance über Designfaktoren

Es springt ins Auge, dass Compliance-Anforderungen einen der Designfaktoren darstellen. Compliance nimmt jedoch auch über andere Designfaktoren Einfluss auf die Gestaltung des IT-Governance-Systems. Das ist zum einen bei den Unternehmenszielen der Fall, von denen ja zwei Compliance-Ziele darstellen. Hierbei ist auch zu berücksichtigen, dass das Potenzial für Compliance-Fehler und das damit verbundene Risiko zu minimieren ein explizites Teilziel des IT-Governance-Ziels EDM03 (Ensured Risk Optimization) darstellt.[92] Dieser Zusammenhang zwischen Compliance und Risikomanagement verweist zudem auf die Beeinflussung über den Designfaktor „Risikoprofil". Weiterhin wird die Non-Compliance als ein mögliches IT-Problem adressiert. Insgesamt beeinflusst Compliance also über vier der Designfaktoren die Ausgestaltung des IT-Governance-Systems.[93]

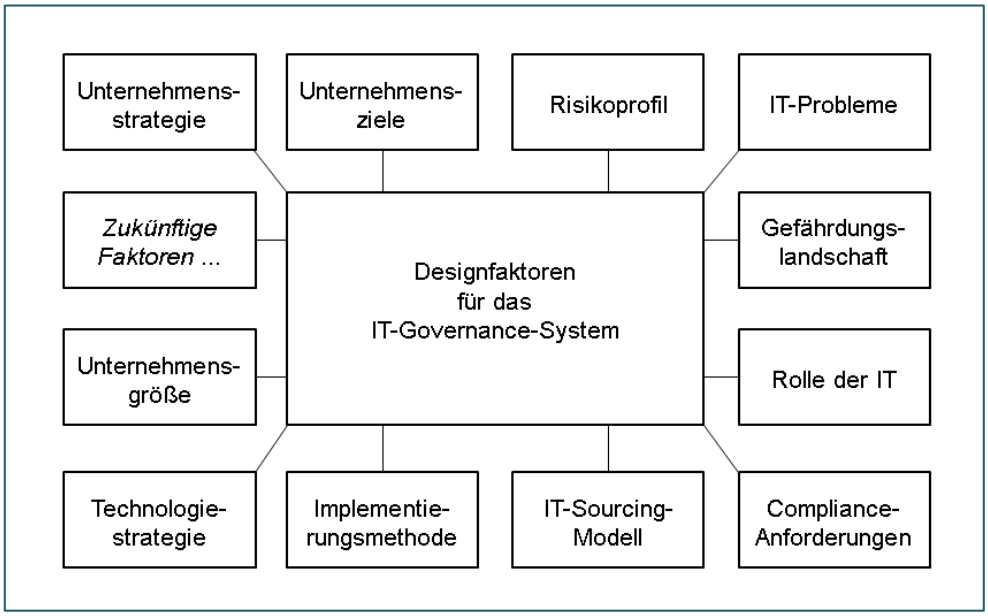

Abbildung 6
Designfaktoren nach COBIT® 2019[94]

Gestaltung des IT-Governance-Systems

Das Design des IT-Governance-Systems besteht hauptsächlich in der Auswahl der relativ wichtigeren IT-Governance- und IT-Managementziele mit ihren Komponenten. Besonders wichtig sind die Prozessbeschreibungen

[92] Nach *ISACA 2018b*, S. 39.
[93] Vgl. *ISACA 2018c*, S. 21ff.
[94] Eigene Darstellung.

mit den Zuordnungen der Aktivitäten zu Befähigungsstufen. Hat ein Unternehmen mittels der Designfaktoren die prioritären IT-Governance- und IT-Managementziele bestimmt und hat es eine Soll-Befähigungsstufe definiert, gibt COBIT® 2019 die umzusetzenden Aktivitäten vor. Auch die anderen Komponenten sind spezifischen Ausprägungen von Designfaktoren anzupassen. Als ein Beispiel hierfür sieht COBIT® 2019 ein Unternehmen, das in einem stark regulierten Umfeld tätig ist. Dieses wird dokumentierten Arbeitsprodukten, -richtlinien und -verfahren sowie einigen Rollen, z. B. der Compliance-Funktion, eine größere Bedeutung zumessen.[95]

Gestaltung des IT-Governance-Systems

COBIT® 2019 sieht für die situationsspezifische Gestaltung des IT-Governance-Systems ein mehrstufiges Phasenmodell („Governance System Design Workflow“) vor. Die erste Phase soll ein grundlegendes Verständnis für die Unternehmenssituation schaffen. Hierfür sind die Unternehmensziele und -strategie, das Risikoprofil und die aktuellen IT-Probleme zu analysieren. Auf dieser Basis sind für diese vier Designfaktoren die prioritären IT-Governance- und IT-Managementziele zu bestimmen. Diese Auswahl ist anschließend in zwei weiteren Phasen anhand der Anwendung der weiteren Designfaktoren kritisch zu überprüfen und das IT-Governance-System ist entsprechend anzupassen.[96]

5.2 Designfaktor „Unternehmensziele“

Anwendung der Zielkaskade

Der Einfluss der beiden compliance-bezogenen Unternehmensziele erfolgt – wie in Kapitel 3 gezeigt – über die Zielkaskade. Das Ergebnis besteht dann in der Ableitung derjenigen IT-Governance- und IT-Managementziele, die die beiden compliance-bezogenen IT-Ziele unterstützen, s. Tabellen 3 und 4. Die Qualifizierung der Unterstützung der IT-Ziele anhand der Einstufung als „primär“ oder „sekundär“ ermöglicht eine Priorisierung, nach der die primär unterstützenden IT-Governance- und IT-Managementziele mit höherer Priorität im Rahmen der Ausgestaltung des IT-Governance-Systems in ihren einzelnen Komponenten umzusetzen wären.

Berücksichtigung von Erfahrungen

COBIT® 2019 weist selbst daraufhin, dass die Technik der Zielkaskade rein mechanisch ist und generische Mapping-Tabellen verwendet. In der An-

[95] Nach *ISACA 2018c*, S. 30. Spezifische Ausprägungen von Designfaktoren können nach COBIT® 2019 zur Anpassung des COBIT® Core Model führen. Derartige Spezialisierungen bezeichnet COBIT® 2019 als „fokus area“. Compliance ist derzeit jedoch nicht als Thema für einen Schwerpunktbereich vorgesehen.
[96] Vgl. *ebd.*, S. 31.

wendung müssen die Ergebnisse sorgfältig interpretiert werden. Es wird sogar empfohlen, die Mapping-Tabellen aufgrund eigener Erfahrungen und Zusammenhänge anzupassen.[97]

5.3 Designfaktor „Risikoprofil“

Non-Compliance als Risikokategorie

Der COBIT® 2019 Design Guide beinhaltet insgesamt 19 Risikokategorien. Eine diese Kategorien (Nr. 13) wird mit „Noncompliance“ bezeichnet. Als beispielhafte Risikoszenarien werden genannt:

- Non-Compliance mit nationalen oder internationalen Vorschriften;
- Mangelndes Bewusstsein für potenzielle regulatorische Änderungen mit Auswirkungen auf das Unternehmen;
- Behinderung des Geschäftsbetriebs durch Vorschriften;
- Non-Compliance mit internen Verfahrensanweisungen.[98]

Ausmaß der Risikomitigation

In Bezug auf die 19 Risikokategorien lassen sich durch eine Mapping-Tabelle diejenigen IT-Governance- und IT-Managementziele bestimmen, die durch ihr Erreichen eine Risikomitigation für die als relevant erachteten Risiken bewirken.[99] Für die Zuordnung von IT-Governance- und IT-Managementzielen zu einem Risikoprofil bietet COBIT® 2019 eine Priorisierung mit einer Skala von 0 bis 4 an. Bei einem Wert „4“ ist das Ausmaß der mit der Zielerreichung verbundenen Risikomitigation am höchsten. Ziele mit einem Wert „0“ sind für die Risikomitigation irrelevant. Tabelle 9 zeigt die der Risikokategorie „Noncompliance“ zugeordneten IT-Governance- und IT-Managementziele. Danach ist – wie zu erwarten – MEA03 das für die Mitigation des Risikos „Noncompliance“ wichtigste IT-Managementziel.

Vergleich mit Zielkaskade

Bemerkenswert ist, dass diese Auflistung von der Ableitung der IT-Governance- und IT-Managementziele im Rahmen der Zielkaskade abweicht und umfangreicher ist als diese (16 ggü. 12 Zielen). Im Vergleich zu den Tabellen 3 und 4 sind nunmehr zusätzlich die IT-Managementziele APO10 und DSS04 enthalten. Dies mag an einer risikoorientierten Betrachtungsweise liegen, bei der die Zusammenarbeit mit IT-Dienstleistern und der Kontinuität des IT-Betriebs hohe Risiken zugemessen werden. Die Relevanz von APO10 für die Vertrags-Compliance steht außer Frage. Bei DSS04 ist

[97] Nach *ebd.*, S. 35
[98] Nach *ebd.*, S. 25.
[99] Vgl. *ebd.*, S. 36.

es eher die Konformität mit Kontinuitätsstandards, wie z. B. der Norm ISO 22301 oder dem BSI-Standard 100-4, die einen engen Compliance-Bezug begründet.

Tabelle 9
IT-Governance- und IT-Managementziele für die Risikokategorie „Non-compliance“[100]

Skalenwert	IT-Governance- und IT-Managementziele
4	• MEA03 – Managed compliance with external requirements
3	• EDM01 – Ensured governance framework setting and maintenance • EDM03 – Ensured risk optimization • EDM05 – Ensured stakeholder engagement • APO01 – Managed I&T management framework • APO13 – Managed security • APO14 – Managed data • DSS05 – Managed security services
2	• APO10 – Managed vendors • DSS04 – Managed continuity • DSS06 – Managed business process controls • MEA01 – Managed performance and conformance monitoring • MEA02 – Managed system of internal control • MEA04 – Managed assurance
1	• EDM02 – Ensured benefits delivery • EDM04 – Ensured resource optimization

5.4 Designfaktor „IT-Probleme“

IT-Probleme als Designfaktor

Ähnlich den Risikokategorien beinhaltet der COBIT® 2019 Design Guide ein Set an IT-Problemen („I&T-Related Issues“), für die wiederum mittels einer Mapping-Tabelle IT-Governance- und IT-Managementziele bestimmt werden können, die zur Problemlösung beitragen. Auch hier kommt wieder eine Skala von 0 bis 4 zur Anwendung, wobei die Bewertung auch 0,5er-Stufen umfasst.

Eines der von COBIT® 2019 genannten IT-Probleme ist der Verstoß gegen IT-bezogene regulatorische oder vertragliche Anforderungen.[101] Tabelle 10

[100] Nach *ebd.*, S. 141f.
[101] Vgl. *ebd.*, S. 143.

zeigt die diesem Problem zugeordneten IT-Governance- und IT-Managementziele.

Tabelle 10
IT-Governance- und IT-Managementziele für das IT-Problem der Non-Compliance mit regulatorischen oder vertraglichen Anforderungen[102]

Skalenwert	IT-Governance- und IT-Managementziele
4	• MEA03 – Managed compliance with external requirements
3	• DSS06 – Managed business process controls • MEA04 – Managed assurance
2,5	• APO14 – Managed data • MEA01 – Managed performance and conformance monitoring • MEA02 – Managed system of internal control
2 2	• EDM01 – Ensured governance framework setting and maintenance • EDM03 – Ensured risk optimization • APO01 – Managed I&T management framework • APO05 – Managed portfolio • APO12 – Managed risk • APO13 – Managed security • DSS04 – Managed continuity • DSS05 – Managed security services
1,5	• EDM02 – Ensured benefits delivery • EDM05 – Ensured stakeholder engagement • APO06 – Managed budget and costs • APO08 – Managed relationships • APO10 – Managed vendors
1	• EDM04 – Ensured resource optimization • APO02 – Managed strategy • APO07 – Managed human resources • APO09 – Managed service agreements • APO11 – Managed quality • DSS01 – Managed operations • DSS02 – Managed service requests and incidents
0,5	• APO03 – Managed enterprise architecture • APO04 – Managed innovation • BAI02 – Managed requirements definition • BAI06 – Managed IT changes • BAI07 – Managed IT change acceptance and transitioning • BAI08 – Managed knowledge • BAI10 – Managed configuration

[102] Nach *ebd.*

Vergleich mit Zielkaskade

Hier sind noch mehr IT-Governance- und IT-Managementziele als beim Designfaktor „Risikoprofil“, insgesamt 22 von 40 Zielen – damit fast doppelt so viele wie bei der Ableitung mittels der Zielkaskade. Insbesondere sind auch IT-Managementziele aus der Domäne BAI enthalten, was z. B. im Hinblick auf die Berücksichtigung von Compliance-Anforderungen in BAI02 oder das Management von Compliance-Wissen in BAI08 als sinnvoll erscheint.

Ein weiteres IT-Compliance-Problem richtet sich auf Unkenntnis von oder Verstöße gegen Datenschutzbestimmungen. Tabelle 11 zeigt die diesem Problem zugeordneten IT-Governance- und IT-Managementziele.

Tabelle 11
IT-Governance- und IT-Managementziele für das IT-Problem der Non-Compliance ggü. Datenschutzbestimmungen[103]

Skalenwert	IT-Governance- und IT-Managementziele
4	• MEA03 – Managed compliance with external requirements
3	• APO14 – Managed data
2,5	• EDM03 – Ensured risk optimization • APO12 – Managed risk • MEA01 – Managed performance and conformance monitoring • MEA02 – Managed system of internal control • MEA04 – Managed assurance
2	• APO13 – Managed security • DSS05 – Managed security services • DSS06 – Managed business process controls
1,5	• EDM01 – Ensured governance framework setting and maintenance • APO07 – Managed human resources
1	• EDM02 – Ensured benefits delivery • EDM05 – Ensured stakeholder engagement • APO10 – Managed vendors • BAI03 – Managed solutions identification and build • BAI06 – Managed IT changes
0,5	• APO01 – Managed I&T management framework • BAI02 – Managed requirements definition • DSS03 – Managed problems

[103] Nach *ebd.*, S. 144.

Auch hier wird immerhin 20 von 40 IT-Governance- und IT-Managementzielen Compliance-Relevanz zuerkannt.

5.5 Designfaktor „Compliance-Anforderungen“

Compliance-Anforderungen als Designfaktor

Der Designfaktor „Compliance-Anforderungen“ adressiert die Compliance-Thematik direkt. In einem ersten Schritt werden die Anforderungen ordinal skaliert nach „hoch–mittel–niedrig“ unterteilt. Für hohe Anforderungen werden die IT-Governance- und IT-Managementziele

- EDM01 (Ensured governance framework setting and maintenance),
- EDM03 (Ensured risk optimization),
- APO12 (Managed risk),
- MEA03 (Managed compliance with external requirements) und
- MEA 04 (Managed assurance)

als wichtig erachtet. [104] Darüber hinaus wird jedoch auch für diesen Designfaktor eine Mapping-Tabelle angeboten. Wie beim Designfaktor „IT-Probleme“ verfügt diese über eine Skala von 0 bis 4 mit 0,5er-Bewertungsstufen. Die Besonderheit dieser Tabelle besteht darin, dass die Bedeutung der IT-Governance- und IT-Managementziele je nach der „hoch–mittel–niedrig“-Einstufung variiert. Werden z. B. die Compliance-Anforderungen an ein Unternehmen als „hoch“ eingestuft, hat das IT-Governanceziel „EDM01“ die Bewertung 3,0. Werden die Compliance-Anforderungen als „mittel“ eingestuft, beträgt der Wert 2,0 und nur noch 1,0 bei einer Einstufung der Compliance-Anforderungen als „niedrig“.

Hohe, mittlere und niedrige Compliance-Anforderungen

Alle IT-Governance- und IT-Managementziele compliance-relevant?

In der Mapping-Tabelle erhalten alle IT-Governance- und IT-Managementziele eine Bewertung und werden damit als compliance-relevant eingestuft. Bei hohen Compliance-Anforderungen an ein Unternehmen bewegen sich die Bewertungen zwischen 1,0 und 4,0, bei mittleren Compliance-Anforderungen zwischen 1,0 und 2,0. Bei niedrigen Compliance-Anforderungen erhalten alle IT-Governance- und IT-Managementziele eine Bewertung von 1,0.[105] Tabelle 11 enthält für hohe Compliance-Anforderungen die IT-Governance- und IT-Managementziele mit einer Bewertung über 1,0.

[104] Nach *ebd.*, S. 138.
[105] Nach *ebd.*, S. 146.

Tabelle 12
IT-Governance- und IT-Managementziele bei hohen Compliance-Anforderungen[106]

Skalenwert	IT-Governance- und IT-Managementziele
4	• EDM03 – Ensured risk optimization • APO12 – Managed risk • MEA03 – Managed compliance with external requirements
3,5	• MEA04 – Managed assurance
3	• EDM01 – Ensured governance framework setting and maintenance
2	• APO01 – Managed I&T management framework • APO14 – Managed data • DSS05 – Managed security services
1,5	• DSS04 – Managed continuity • APO10 – Managed vendors • APO13 – Managed security • EDM05 – Ensured stakeholder engagement

5.6 Konsolidierung der compliance-relevanten Designfaktoren

COBIT® 2019 Governance System Design Workbook

Das Tailoring von COBIT® 2019 sieht natürlich vor, dass die Designfaktoren integriert zur Anwendung kommen. Hierzu steht ein EXCEL-basiertes Tool (COBIT® 2019 Governance System Design Workbook) zur Verfügung, in dem die Bewertungen vorgenommen werden können. Das Tool ergibt jedoch nur dann sinnvolle summarische Auswertungen (in Form von Spinnengraphiken), wenn für alle (oder zumindest sehr viele) Designfaktoren Werte eingetragen werden. Werden nur die hier behandelten vier Designfaktoren in Bezug auf Compliance bewertet, werden lediglich die IT-Governance- und IT-Managementziele

- EDM03 (Ensured risk optimization),
- APO13 (Managed security),
- MEA03 (Managed compliance with external requirements)

als relevant angezeigt.[107] Dieses Ergebnis erscheint nach den bisherigen Ausführungen dann doch als zu ungenau.

[106] Nach *ebd.*
[107] Dieses Ergebnis stellt sich dann ein, wenn im COBIT® 2019 Governance System Design Workbook für die hier behandelten Designfaktoren (Maximal)Werte eingetragen werden, für die anderen Designfaktoren dagegen 0-Werte.

Manuelle Konsolidierung

Die Alternative zu einer tool-gestützten Konsolidierung ist eine manuelle Gegenüberstellung und Zusammenführung der Bewertungen für die Compliance-Relevanz der IT-Governance- und IT-Managementziele. Diese hat zudem den Vorteil, dass die Unterschiede in den Priorisierungen der Designfaktoren sichtbar werden und damit zur kritischen Diskussion anregen. Tabelle 13 versucht eine derartige Konsolidierung, indem die Ergebnisse für die Bewertungen aller Designfaktoren zusammengetragen sind.

Da lediglich die Bestimmung der IT-Governance- und IT-Managementziele durch die Zielkaskade nicht zu einer quantitativen Bewertung führt, erhält ein IT-Governance- oder IT-Managementziel je primärer Unterstützung eines IT-Ziels den Wert „4“, je sekundärer Unterstützung den Wert „2“. Hierdurch ist es möglich, die Bewertungen zu summieren und eine Reihenfolge zu bilden.

Tabelle 13
Konsolidierung der für IT-Compliance relevanten Designfaktoren

IT-Governance- und IT-Managementziele	IT-Compliance-relevante Designfaktoren						
	AG 1	AG 11	Risikoprofil	IT-Prob. 1	IT-Prob. 2	Compl.-Anford.	Σ
EDM01	4,0	2,0	3,0	2,0	1,5	3,0	15,5
EDM02			1,0	1,5	1,0	1,0	4,5
EDM03	2,0	2,0	3,0	2,0	2,5	4,0	15,5
EDM04			1,0	1,0		1,0	4,0
EDM05		2,0		1,5	1,0	1,5	6,0
APO01	2,0	4,0	3,0	2,0	0,5	2,0	13,5
APO02				1,0		1,0	2,0
APO03				0,5		1,0	1,5
APO04				0,5		1,0	1,5
APO05				2,0		1,0	3,0
APO06				1,5		1,0	2,5
APO07				1,0	1,5	1,0	3,5
APO08				1,5		1,0	2,5
APO09				1,0		1,0	2,0
APO10			2,0	1,5	1,0	1,5	6,0
APO11				1,0		1,0	2,0
APO12				2,0	2,5	4,0	8,5
APO13	2,0		3,0	2,0	2,0	1,5	10,5
APO14	2,0		3,0	2,5	3,0	2,0	12,5
BAI01						1,0	1,0
BAI02				0,5	0,5	1,0	2,0
BAI03					1,0	1,0	2,0
BAI04						1,0	1,0
BAI05						1,0	1,0

IT-Governance- und IT-Managementziele	IT-Compliance-relevante Designfaktoren						
	AG 1	AG 11	Risiko-profil	IT-Prob. 1	IT-Prob. 2	Compl.-Anford.	Σ
BAI06				0,5	1,0	1,0	2,5
BAI07				0,5		1,0	1,5
BAI08				0,5		1,0	1,5
BAI09						1,0	1,0
BAI10				0,5		1,0	1,5
BAI11						1,0	1,0
DSS01				1,0		1,0	2,0
DSS02				1,0		1,0	2,0
DSS03					0,5	1,0	1,5
DSS04			2,0	2,0		1,5	5,5
DSS05	2,0	2,0	3,0	2,0	2,0	2,0	13,0
DSS06		2,0	2,0	3,0	2,0	1,0	10,0
MEA01	2,0	2,0	2,0	2,5	2,5	1,0	12,0
MEA02	2,0	4,0	2,0	2,5	2,5	1,0	14,0
MEA03	4,0	2,0	4,0	4,0	4,0	4,0	22,0
MEA04	2,0	4,0	2,0	3,0	2,5	3,5	17,0
Summe	10	10	15	33	20	40	

Wie in der Tabelle zu sehen ist (graue Felder), sind nur elf IT-Governance- und IT-Managementziele in allen vier Designfaktoren als relevant bewertet. Dies sind dann auch diejenigen IT-Governance- und IT-Managementziele, die die relativ höheren Bewertungen erhalten haben (in der Reihenfolge der Bewertungspunkte):

- Vier IT-Governance- und IT-Managementziele haben eine Bewertung von ≥ 15 (rote Felder), wobei MEA03 mit 22 Punkten erwartungsgemäß deutlich die Spitzenposition einnimmt.
  - MEA03 (Managed compliance with external requirements)
  - MEA04 (Managed assurance)
  - EDM01 (Ensured governance framework setting and maintenance)
  - EDM03 (Ensured risk optimization)
- Sieben IT-Governance- und IT-Managementziele haben eine Bewertung von ≥ 10 und < 15 (gelbe Felder):
  - MEA02 (Managed system of internal control)
  - APO01 (Managed I&T management framework)

- DSS05 (Managed security services)
- APO14 (Managed data)
- MEA01(Managed performance and conformance monitoring)
- APO13 (Managed security)
- DSS06 (Managed business process controls)

- Vier IT-Governance- und IT-Managementziele haben eine Bewertung von ≥ 5 und < 10 (grüne Felder):
  - APO12 (Managed risk)
  - EDM05 (Ensured stakeholder engagement)
  - APO10 (Managed vendors)
  - DSS04 (Managed continuity)

15/40 IT-Governance- und IT-Managementziele compliance-relevant

Auf diese Weise gelangt man zu insgesamt 15 von 40 IT-Governance- und IT-Managementzielen mit hoher Relevanz für IT-Compliance. Die wesentlich zahlreicheren IT-Governance- und IT-Managementziele bei den beiden Designfaktoren „IT-Probleme“ und „Complianceanforderungen“ verweisen allerdings darauf, dass die relevanten IT-Governance- und IT-Managementziele letztlich unternehmensindividuell und situationsspezifisch zu bestimmen sind.

6 IT-Compliance im Rahmen des COBIT® 2019 Implementation Guide

COBIT® 2019 Implementation Guide

Der COBIT® 2019 Implementation Guide will vor allem für ein für IT-Governance förderliches Umfeld sorgen, in dem entsprechende Vorhaben erfolgversprechend durchgeführt werden können. Dazu sollte eine angemessene Ausgestaltung und Überwachung der IT-Governance-Vorhaben gehören. Ziel ist es, ein deutliches Commitment der Unternehmensleitung und eine angemessene Steuerung und Überwachung der Aktivitäten zu gewährleisten.[108] Der Implementation Guide zielt damit auf die Etablierung und kontinuierliche Verbesserung des IT-Governance-Systems eines Unternehmens. Insofern bezieht er sich nur am Rande ausdrücklich auch auf IT-Compliance. Da aber IT-Compliance Teil der IT-Governance ist, sind viele Hinweise des

[108] Vgl. *ISACA 2018d*, S. 21.

Implementation Guide auch für IT-Compliance-Projekte anwendbar.

Kontinuierliche Verbesserung als Kern

Den Kern des COBIT® 2019 Implementation Guide bildet ein Lebenszyklus der kontinuierlichen Verbesserung. Dieser soll es Unternehmen ermöglichen, die Komplexität und die Herausforderungen zu bewältigen, die typischerweise mit der Implementierung und Weiterentwicklung eines IT-Governance-Systems verbunden sind. Der Lebenszyklus besteht aus den drei miteinander verbundenen Elementen: Kontinuierliche Verbesserung, Änderungsmanagement und Programmmanagement,

wobei das Änderungsmanagement vor allem verhaltensbezogene und kulturelle Aspekte der Implementierung oder Verbesserung berücksichtigen soll.[109] Diese drei Elemente stehen für Handlungsbereiche, in denen in insgesamt sieben Veränderungsphasen Aufgaben ausgeführt werden. Die sieben Phasen stellen die schon aus COBIT® 5 bekannte Implementierungs-Roadmap dar, s. Abbildung 7.

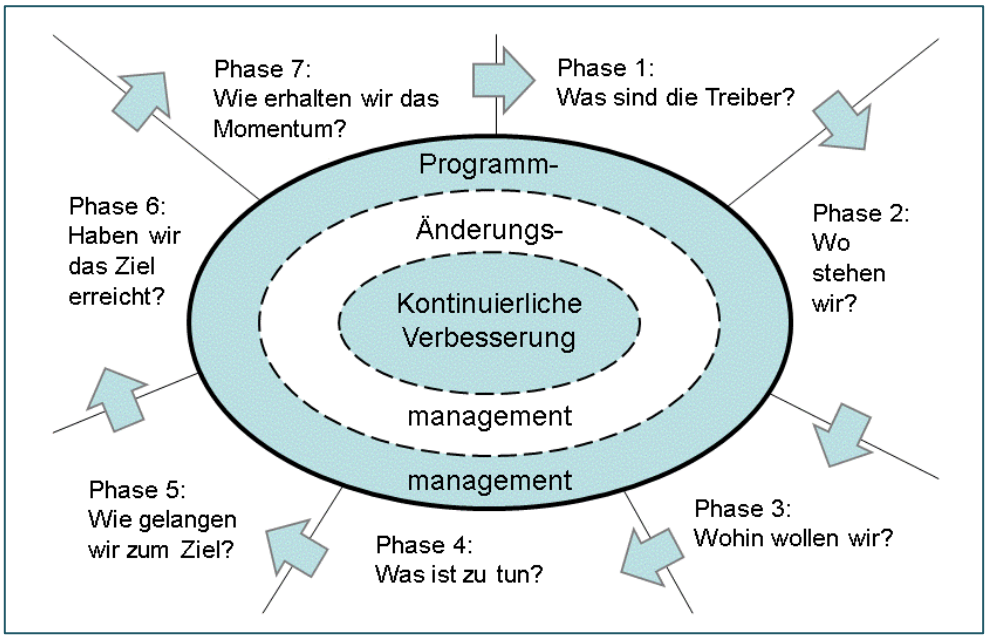

Abbildung 7
COBIT® 2019 Implementierungs-Roadmap[110]

Non-Compliance als „Pain Point“

Einer der Ausgangspunkte („Pain Points“) für eine Veränderung der IT-Governance ist Non-Compliance, hervorgerufen durch Governance-Strukturen, die sich durch die weltweite Zunahme von Vorschriften und Compliance-

[109] Nach *ebd.*, S. 23.
[110] Vgl. ebd., S. 23f.; eigene Darstellung.

Anforderungen als ineffektiv und ineffizient erweisen.[111] Gerade der Unternehmensleitung sollte klar sein, dass Ignoranz und/oder Nichteinhaltung von Vorschriften das Unternehmen ernsthaft beeinträchtigen kann.[112]

Stakeholder

Eine wichtige Aufgabe im Rahmen der Implementierung von Governance-Lösungen ist die Bestimmung der beteiligten Stakeholder, um deren Unterstützung zu erhalten. Als für IT-Compliance relevante externe Stakeholder benennt COBIT® 2019.[113]

- Regulative Einrichtungen: Im Hinblick auf diese Zielgruppe soll mithilfe von COBIT® 2019 insbesondere sichergestellt werden, dass das Unternehmen über das richtige Governance-System verfügt, um Compliance-Anforderungen zu erfüllen und diese zu überwachen.
- Geschäftspartner: Der Austausch von Geschäftsdaten soll sicher, zuverlässig und konform mit geltenden Regeln und Vorschriften erfolgen.[114]
- Externe Auditoren: Gegenstand ihrer Prüfung können auch – vor allem regulatorisch vorgeschriebene – Compliance-Aspekte sein.

Als interne Stakeholder sind relevant:

- Compliance-, Risikomanagement- und Rechtsexperten: Diese stellen vor allem sicher, dass die Ausrichtung auf den gesamten Ansatz des Enterprise Risk Management (ERM) erfolgt und dass die relevanten Compliance- und Risikomanagementziele erreicht und Compliance- und Risikoprobleme berücksichtigt werden.[115]

Diese Stakeholder sind in COBIT® 2019 explizit benannt. Selbstverständlich sind über Compliance-Risiken auch diejenigen Stakeholder betroffen, die das Risikomanagement des Unternehmens zu vertreten haben, nicht zuletzt die Unternehmensleitung (inkl. CIO).

Compliance spielt in den einzelnen Phasen der Implementierungs-Roadmap eine unterschiedliche Rolle, mal als Inhalt und Gegenstand der Veränderung, mal durch die Beteiligung der Compliance-Stakeholder.

Phase 1

- In Phase 1 (Was sind die Treiber?) besteht die Aufgabe der Compliance-experten darin, in Compliancefragen zu beraten und entsprechende Maß-

[111] Nach *ebd.*, S. 26.
[112] Vgl. *ebd.*, S. 28.
[113] Nach *ebd.*, S. 32f.
[114] Vgl. *ISACA 2018a*, S. 15.
[115] Nach *ISACA 2018d*, S. 31.

nahmen zu begleiten. Es soll sichergestellt werden, dass Compliance-Anforderungen im weiteren Verlauf des Veränderungsprozesses berücksichtigt werden.[116] Als Aufgabe der kontinuierlichen Verbesserung sind Compliance-Anforderungen zu identifizieren und die diesbezüglichen Bedarfe der Stakeholder zu bewerten. Im Rahmen des Änderungsmanagements ist der Handlungsbedarf zu verdeutlichen, u. a. auch mittels Messzahlen zur (Non-)Compliance.[117]

- In Phase 2 (Wo stehen wir?) steht für die Complianceexperten die Überprüfung, ob Compliancefragen angemessen berücksichtigt wurden, im Vordergrund.[118] Sie sind vor allem an der Bewertung von Compliance-Risiken und der Identifizierung compliance-kritischer Prozesse beteiligt, so dass kritische Compliance-Risiken vermieden werden können.[119] Phase 2
- In Phase 3 (Wohin wollen wir?) haben die Complianceexperten in einer beratenden Rolle sicherzustellen, dass in der Veränderungsplanung Compliancefragen angemessen adressiert werden, insbesondere hinsichtlich des Veränderungsbedarfs für IT-Compliance.[120] Phase 3
- In Phase 4 (Was ist zu tun?) ist durch die Complianceexperten sicherzustellen, dass alle identifizierten Compliancefragen im Rahmen der priorisierten Projekte bzw. des Programms behandelt werden und dass die Vorschläge mit allen relevanten Richtlinien oder Vorschriften übereinstimmen.[121] Phase 4
- In Phase 5 (Wie gelangen wir zum Ziel?) geben die Complianceexperten während der Implementierung bei Bedarf Hinweise zu Compliance-Aspekten. Dies kann sich auf die Entwicklung, die Anschaffung, den Test und den Roll-out einzelner compliance-bezogener Governance-Lösungen sowie die Nutzung von Best-Practices beziehen.[122] Phase 5
- In Phase 6 (Haben wir das Ziel erreicht?) ist es Aufgabe der Complianceexperten anhand von Messzahlen zu beurteilen, ob das Unternehmen durch den bisherigen Veränderungsprozess besser in der Lage ist, Phase 6

[116] Vgl. *ebd.*, S. 50.
[117] Vgl. *ebd.*, S. 51f.
[118] Vgl. *ebd.*, S. 53.
[119] Vgl. *ebd.*, S. 56.
[120] Vgl. *ebd.*, S. 57, 60.
[121] Vgl. *ebd.*, S. 61, 63.
[122] Vgl. *ebd.*, S. 64, 66.

Compliance-Anforderungen und -Risiken zu identifizieren und zu steuern. Ggf. haben die Complianceexperten Feedback und Empfehlungen für weitere Verbesserungen zu geben, z. B. zur Anpassung von Verantwortlichkeiten.[123]

- In Phase 7 (Wie erhalten wir das Momentum?) haben die Complianceexperten am formalen Projekt- bzw. Programmabschluss mitzuwirken und aus der Anwendung der Änderungen Lessons-learned abzuleiten. In Zusammenarbeit mit der IT und den Fachabteilungen sind gesetzliche und regulatorische Anforderungen zu antizipieren. Die Identifizierung und Reaktion auf IT-Compliance-Risiken gehören in dieser Phase zu den normalen Aktivitäten im Rahmen der operativen IT-Governance.[124]

Phase 7

7 Fazit zu COBIT® 2019

Letztlich wird die Compliance-Thematik in COBIT® 2019 ähnlich umfangreich behandelt wie in COBIT® 5, vgl. die Gegenüberstellung in Tabelle 14.

Vergleich

Tabelle 14 Vergleich von COBIT® 5 und COBIT® 2019 in Bezug auf Compliance

Compliance-Bezug	COBIT® 5	COBIT® 2019
Compliance-Definition	implizit in Zielen und Praktiken enthalten und durch Bezug auf ISO/IEC 38500	
Compliance-Bezug der Unternehmensziele	2 compliance-bezogene Unternehmensziele: • Einhaltung externer Gesetze und Bestimmungen (Compliance) (Nr. 4) • Compliance mit internen Richtlinien (Nr. 15) Ziel 4 ist Teil der Finanzperspektive der BSC, Ziel 15 ist Teil der internen Perspektive.	2 compliance-bezogene Unternehmensziele: • Compliance mit externen Gesetzen und Bestimmungen (Nr. 3) • Compliance mit internen Richtlinien (Nr. 11) Ziel 3 ist Teil der Finanzperspektive der BSC, Ziel 11 ist Teil der internen Perspektive.
Compliance-Bezug der IT-Ziele	2 compliance-bezogene IT-Ziele: • IT-Compliance und Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Be-	2 compliance-bezogene IT-Ziele: • IT-Compliance und Unterstützung bei der Einhaltung externer Gesetze und Bestimmungen (Nr. 1)

[123] Vgl. *ebd.*, S. 67, 69.
[124] Vgl. *ebd.*, S. 70, 72.

Compliance-Bezug	COBIT® 5	COBIT® 2019
	stimmungen (Nr. 2) • IT-Compliance mit internen Richtlinien (Nr. 15) Ziel 2 ist Teil der BSC-Finanzperspektive, Ziel 15 ist Teil der internen BSC-Perspektive.	• IT-Compliance mit internen Richtlinien (Nr. 11) Ziel 1 ist Teil der BSC-Finanzperspektive, Ziel 11 ist Teil der internen BSC-Perspektive.
Compliance-relevante IT-Prozesse bzw. IT-Governance- und IT-Managementziele	26 von 37 IT-Prozessen unterstützten die beiden compliance-bezogenen IT-Ziele nach der Zielkaskade.	Compliance-Relevanz der IT-Governance- und IT-Managementziele ergibt sich in unterschiedlichen Umfang anhand von vier Designfaktoren. Mittels einer Konsolidierung lässt sich für 15 von 40 IT-Governance- und IT-Managementzielen eine hohe Relevanz für IT-Compliance ermitteln.
Zentraler Compliance-Prozess bzw. zentrales IT-Managementziel	Prozess MEA03 (Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen) der COBIT® 5-Domäne "Überwachen, Evaluieren und Beurteilen" mit 4 Managementpraktiken und 18 Aktivitäten	IT-Managementziel MEA03 (Managed compliance with external requirements) der COBIT® 2019-Domäne "Monitor, Evaluate and Assess" mit 4 Managementpraktiken und 20 Aktivitäten
Compliance-Rollen im RACI-Modell	2 Rollen: • Compliance • Datenschutzbeauftragter	3 Rollen: • Compliance • Datenschutzbeauftragter • Rechtsberatung
Compliance-bezogene Informationsflüsse und -objekte	• Informationsflüsse sind als Input/Output den Praktiken zugeordnet • Informationsobjekte sind in den Informationsflüssen, tw. in COBIT® 5 Enabling Information enthalten	• Informationsflüsse sind als Input/Output den Praktiken zugeordnet, bilden aber die eigene Komponente „Information“ • Informationsobjekte sind in den Informationsflüssen enthalten
Weitere Komponenten des IT-Governance-Systems	entfällt	Compliance-Bezüge sind vorhanden, müssen aber identifiziert werden
Compliance als Designfaktor	entfällt	Compliance-Anforderungen sind ein expliziter Designfaktor; weiterhin ist Compliance

Compliance-Bezug	COBIT® 5	COBIT® 2019
		Teil der Designfaktoren Unternehmensziele, IT-Probleme und Risikoprofil

Die neue Beschreibungsstruktur der IT-Governance- und IT-Managementziele kommt auch der Darstellung der IT-Compliance zugute. Die Prozesspraktiken wirken fokussierter, der Compliance-Bezug muss aber nach wie vor oftmals interpretiert werden. IT-Aufbauorganisation und Informationsflüsse wurden im Detail an vielen Stellen umfangreich überarbeitet. Dass im RACI-Modell auf die C- und I-Rollen verzichtet wurde, kann verschmerzt werden, da diese Zuordnungen in hohem Maße situationsspezifisch sein dürften. In den anderen Komponenten finden sich Complance-Bezüge eher spärlich wieder, aber das liegt an dem (noch?) geringen Ausarbeitungsumfang dieser Komponenten.

Fazit

Wo IT-Compliance nach COBIT® 5 ausgestaltet wurde, ergibt sich mit der neuen Version COBIT® 2019 ein nicht geringer Anpassungsaufwand im Detail, vor allem in den Änderungen von Aktivitäten und der systematischen Berücksichtigung der weiteren Komponenten. Grundlegend hierfür ist die Analyse, welche IT-Governance- und IT-Managementziele im Anwendungsfall compliance-relevant sind. Hierfür bietet COBIT® 2019 mit den Designfaktoren ein umfangreiches Instrumentarium, welches jedoch nicht durchgängig einen konsistenten Eindruck macht. Trotzdem leistet COBIT® 2019 hilfreiche Unterstützung bei der Gestaltung der IT-Governance im Allgemeinen und der IT-Compliance im Besonderen. Es ist zu hoffen, dass eine nächste Version „COBIT® 202x“ seine Nutzer nicht mit einer abermalig neuen Dokumentenstruktur überrascht, sondern dass die jetzige Struktur lange Zeit Bestand haben und kontinuierlich ausgebaut werden wird.

Anhang

Tabelle 15 Compliance-bezogene Aktivitäten in COBIT® 2019

F	Praktik	Aktivität
2	APO 07.04	4. Erstellung von Anweisungen für die Verarbeitung personenbezogener Daten in Übereinstimmung mit datenschutz- und arbeitsrechtlichen Vorschriften.[125]
	APO 09.03	1. Analysieren der Anforderungen an neue oder geänderte Serviceverträge. Hierbei sind auch Aspekte wie Sicherheit, Datenschutz, Compliance und regulatorische Fragen zu berücksichtigen.[126]
	BAI 07.02	1. Definition eines Migrationsplans für Geschäftsprozesse, IT-Services und IT-Infrastruktur, wobei u. a. Compliance-Anforderungen zu berücksichtigen sind.[127]
	BAI 07.04	1. Erstellung einer Datenbank mit Testdaten, die für die Produktionsumgebung repräsentativ sind. Hierbei ist zu untersuchen, ob Compliance- oder regulatorische Anforderungen die Verwendung von bereinigten Daten vorschreiben.[128]
	BAI 11.08	4. Festlegung von Rollen und Verantwortlichkeiten der beteiligten Projekt-Parteien, einschließlich Compliance.[129]
	DSS 06.01	1. Identifizierung und Dokumentation der notwendigen Kontrollaktivitäten für wichtige Geschäftsprozesse, um Kontrollanforderungen u. a. für Compliance-Ziele zu erfüllen.[130]
3	APO 01.09	1. Erstellen von Richtlinien, u. a. zu Compliance-Themen, wie Sicherheit, Datenschutz, ethischem Verhalten oder Rechten an geistigem Eigentum.
		2. Einführung und Durchsetzung von IT-Richtlinien für alle relevanten Mitarbeiter, so dass die Richtlinien in den Unternehmensbetrieb integriert sind.[131]
	APO 10.02	4. Festhalten von Rechten und Pflichten aller Parteien in Verträgen zum Softwareerwerb und Durchsetzen derselben. Diese Rechte und Pflichten können sich z. B. beziehen auf Eigentum und Lizenzierung von IP, Garantien, Schiedsverfahren, Upgrade-Bedingungen, Sicherheit, Datenschutz sowie Escrow- oder Zugangsrechte.
		5. Festhalten von Rechten und Pflichten aller Parteien in Ver-

[125] Nach *ISACA 2018b*, S. 101.
[126] Nach *ebd.*, S. 114.
[127] Nach *ebd.*, S. 198.
[128] Nach *ebd.*, S. 199.
[129] Nach *ebd.*, S. 225.
[130] Nach *ebd.*, S. 266.
[131] Nach *ebd.*, S. 120.

F	Praktik	Aktivität
		trägen zur Beauftragung von Entwicklungsressourcen und Durchsetzen derselben. Diese Rechte und Pflichten können sich z. B. beziehen auf das Eigentum und die Lizenzierung von IP, Leistungsüberprüfungen, Zahlungsgrundlagen, Garantien, Schiedsverfahren und Einhaltung von Unternehmensrichtlinien.
		6. Einholen von Rechtsberatung zu Verträgen über die Entwicklung von Ressourcen in Bezug auf das Eigentum und die Lizenzierung von IP.
		7. Festhalten von Rechten und Pflichten aller Parteien in Verträgen zum Erwerb von Infrastruktur, Einrichtungen und damit verbundenen Dienstleistungen und Durchsetzen derselben. Diese Rechte und Pflichten können sich z. B. beziehen auf Zugangskontrollen, Sicherheit, Datenschutz, Zahlungs- und Schiedsverfahren.[132]
	BAI 02.01	6. Bestätigung der wichtigsten Aspekte von Anforderungen, u. a. zur Einhaltung gesetzlicher und regulatorischer Vorschriften.[133]
	BAI 03.11	2. Vorschlagen neuer oder geänderter Service-Level-Optionen (u. a. Datenschutz und Compliance), um sicherzustellen, dass die IT-Produkte und -Dienstleistungen nutzbar bleiben.[134]
	BAI 07.04	3. Einrichtung eines Prozesses zur ordnungsmäßigen Aufbewahrung oder Entsorgung von Testergebnissen, Medien und anderen zugehörigen Unterlagen unter Berücksichtigung der Auswirkungen von regulatorischen oder Compliance-Anforderungen.[135]
	BAI 09.02	7. Vereinbarung von Serviceverträgen, die alle notwendigen Sicherheits- und Datenschutzbedingungen enthalten, um die Einhaltung von Richtlinien und Standards für Unternehmenssicherheit und Datenschutz sicherzustellen.[136]
	DSS 01.05	9. Sicherstellung, dass IT-Standorte und -Einrichtungen die relevanten Gesundheits- und Sicherheitsgesetze, Vorschriften, Richtlinien und Spezifikationen von Lieferanten einhalten.[137]
	DSS 06.06	4. Identifizierung und Implementierung von Prozessen, Tools und Techniken zur angemessenen Überprüfung der Compliance mit IT-Sicherheitsrichtlinien.[138]

[132] Nach *ebd.*, S. 59.
[133] Nach *ebd.*, S. 164.
[134] Nach *ebd.*, S. 175.
[135] Nach *ebd.*, S. 199.
[136] Nach *ebd.*, S. 210.
[137] Nach *ebd.*, S. 233.
[138] Nach *ebd.*, S. 268.

F	Praktik	Aktivität
4	APO 01.09	3. Bewertung und Aktualisierung der Richtlinien, um diese an Änderungen im Geschäftsumfeld anzupassen (mindestens jährlich).[139]
	APO 01.11	2. Identifizieren geschäftskritischer IT-Prozesse auf der Grundlage von Leistungs- und Konformitätstreibern und den damit verbundenen Risiken. Bewertung der Leistungsfähigkeit und Identifizierung von Verbesserungszielen. Analysieren von Lücken und Identifizieren von Optionen zur Verbesserung oder Neugestaltung des Prozesses.[140]
	APO 10.05	3. Überwachen und Reviewen der Leistungserbringung durch IT-Lieferanten, um sicherzustellen, dass diese eine akzeptable Servicequalität erbringen, die Anforderungen erfüllen und die Vertragsbedingungen einhalten.[141]
	BAI 05.05	5. Durchführung von Compliance-Audits, um die Ursachen für geringe Akzeptanz zu identifizieren. Empfehlung von Korrekturmaßnahmen.[142]
	BAI 06.01	6. Strukturierte Planung und Bewertung aller Change Requests unter Berücksichtigung der Auswirkungen u. a. auf Sicherheit, Datenschutz, Recht, Verträge und Compliance.[143]
	BAI 07.08	4. Berücksichtigung von Anforderungen an ein Post-Implementation-Review, die sich z. B. aus der Compliance ergeben.[144]
	BAI 09.05	3. Vergleichen der Anzahl der installierten Softwareinstanzen mit der Anzahl der vorhandenen Lizenzen. Sicherstellung, dass die Methode zur Messung der Lizenz-Compliance mit den Lizenz- und Vertragsanforderungen übereinstimmt.[145]
5	APO 03.05	5. Etablieren eines Technologieforums, um Architektur-Richtlinien zu erstellen, Projekte zu unterstützen und die Technologieauswahl zu steuern sowie zum Messen der Compliance mit Standards und Richtlinien, einschließlich externer Anforderungen.[146]
F = Fähigkeitsstufe		

[139] Nach *ebd.*, S. 59.
[140] Nach *ebd.*, S. 60.
[141] Nach *ebd.*, S. 121.
[142] Nach *ebd.*, S. 189.
[143] Nach *ebd.*, S. 193.
[144] Nach *ebd.*, S. 201.
[145] Nach *ebd.*, S. 212.
[146] Nach *ebd.*, S. 75.

Quellenangaben

Andenmatten 2018: Andenmatten, Martin: COBIT 2019 – Das neue Enterprise Governance Modell für Informationen und Technologien, 26.11.2018; online verfügbar unter: Andenmatten https://blog.itil.org/2018/11/kategorie-liste-home/itil/cobit-2019-das-neue-enterprise-governance-modell-fuer-informationen-und-technologien/ (letzter Zugriff am 19.09.2019).

Asprion/Burda 2019: Asprion, Petra M.; Burda, Daniel: COBIT. In: Enzyklopädie der Wirtschaftsinformatik, GITO Verlag, Bearbeitungsstand: 27.02.2019; online verfügbar unter: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Grundlagen-der-Informationsversorgung/COBIT (letzter Zugriff am 19.09.2019).

Gaulke 2014: Gaulke, Markus: Praxiswissen COBIT – Grundlagen und praktische Anwendung in der Unternehmens-IT, 2. Aufl., Heidelberg: dpunkt, 2014.

Gaulke 2019: Gaulke, Markus: COBIT® 2019 – das neue IT-Governance-Modell für die Unternehmens-IT. In: IT-Governance, Jg.13 (2019), Nr. 29, S. 3-9.

ISACA 2012a: Information Systems Audit and Control Association (ISACA): COBIT 5® – Rahmenwerk für Governance und Management der Unternehmens-IT, Rolling Meadows: ISACA 2012.

ISACA 2012b: Information Systems Audit and Control Association (ISACA): COBIT® 5 – Enabling Processes, Rolling Meadows: ISACA 2012.

ISACA 2013: Information Systems Audit and Control Association (ISACA): COBIT® 5 – Enabling Information, Rolling Meadows: ISACA 2013.

ISACA 2018a: Information Systems Audit and Control Association (ISACA): COBIT 2019® – Framework: Introduction and Methodology, Schaumburg: ISACA 2018.

ISACA 2018b: Information Systems Audit and Control Association (ISACA): COBIT 2019® – Framework: Governance and Management Objectives, Schaumburg: ISACA 2018.

ISACA 2018c: Information Systems Audit and Control Association (ISACA): COBIT 2019® – Design Guide, Schaumburg: ISACA 2018.

ISACA 2018d: Information Systems Audit and Control Association (ISACA): COBIT 2019® – Implementation Guide, Schaumburg: ISACA 2018.

Johannsen/Goeken 2011: Johannsen, Wolfgang; Goeken, Matthias: Referenzmodelle für IT-Governance – Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co, 2. Aufl., Heidelberg: dpunkt, 2011.

ISO/IEC 38500: International Organization for Standardization (Hg.): International Standard ISO/IEC 38500:2015, Information technology – Governance of IT for the organization, Second Edition 2015-02-15.

Klotz 2008: Klotz, Michael: IT-Governance genormt – die neue ISO/IEC 38500. In: IT-Governance, Jg. 2 (2008), Nr. 4, S. 21-22; online verfügbar unter: https://www.researchgate.net/publication/333428759_IT-Governance_genormt_-_die_neue_ISOIEC_38500 (letzter Zugriff am 19.09.2019).

Klotz 2013: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: Fachhochschule Stralsund, SIMAT Stralsund Information Management Team, Jg. 5 (2013), Nr. 24; online verfügbar unter:

https://www.researchgate.net/publication/279190512_Regelwerke_der_IT-Compliance_-_Klassifikation_und_Ubersicht_Teil_2_Normen (letzter Zugriff am 19.09.2019).

Klotz 2014: Klotz, Michael: IT-Compliance nach COBIT – Gegenüberstellung zwischen COBIT 4.0 und COBIT 5. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: Fachhochschule Stralsund, SIMAT Stralsund Information Management Team, Jg. 6 (2014), Nr. 25; online verfügbar unter: https://www.researchgate.net/publication/279190647_IT-Compliance_nach_COBITR_-_Gegenuberstellung_zwischen_COBITR_40_und_COBITR_5 (letzter Zugriff am 19.09.2019).

Klotz 2016 a: Klotz, Michael: IT-Governance genormt – die neue ISO/IEC 38500 (reloaded). In: IT-Governance, Jg.10 (2016), Nr. 4, S. 25-27; online verfügbar unter: https://www.researchgate.net/publication/333479998_IT-Governance_genormt_-_die_neue_ISOIEC_38500_reloaded (letzter Zugriff am 19.09.2019).

Klotz 2016b: Klotz, Michael: IT-Governance nach dem Modell der „Three Lines of Defense“. In: Lang, Michael (Hg.): CIO-Handbuch – Strategien für die digitale Transformation, Band 4, Symposion, Düsseldorf 2016, S. 145-160.

Klotz 2017: Klotz, Michael: IT-Compliance. In: Ernst Tiemeyer (Hrsg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 6. Aufl., München: Hanser, S. 857-902.

SFIA 2018: SFIA Foundation Ltd. (Hg.): SFIA 7 – Skills Framework for the Information Age, The complete reference, London, SFIA 2018.

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop-Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Karminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informations-managements
03-11-013	08.2011	H. Auerbach/ N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesund-heitswirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutsch-sprachiger Museums-Apps
03-11-016	11.2011	S. J. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Meck-lenburg-Vorpommern – Strom als Wettbewerbs-faktor und Gegenstand der Standortvermarktung
04-12-017	02.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagement-software – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements

04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.
04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	02.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen
06-14-025	01.2014	M. Klotz	IT-Compliance nach COBIT® – Gegenüberstellung von COBIT® 4.0 und COBIT® 5
06-14-026	04.2014	L. von Blumröder	Projektpriorisierung im Rahmen eines ganzheitlichen Projektportfoliomanagements
06-14-027	06.2014	S. Press	Automatisierte Kontrollen in der Beschaffung – Exemplarische Konzeption und Umsetzung
06-14-028	07.2014	M. Klotz	IT-Compliance – Begrifflichkeit und Grundlagen
07-15-029	09.2015	M. Klotz	Projektmanagement-Normen und -Standards
08-16-030	08.2016	M. Klotz	ISO/IEC 3850x – Die Normenreihe zur IT-Governance
09-17-031	09.2017	S. Marx	Project Management Practice in Interreg Projects – Reflective Analysis and Recommendations
09-17-032	11.2017	S. Marx	Knowledge Management in Interreg Cross-Border Cooperation – a Project Perspective
10-18-033	11.2018	M. Klotz / S. Marx	Projektmanagement-Normen und -Standards, 2. Auflage
11-19-034	08.2019	M. Klotz	IT-Compliance nach COBIT® 2019