Eine Veröffentlichung des ISACA Germany Chapter e.V.

Leitfaden IT-Compliance

Grundlagen, Regelwerke, Umsetzung

ISACA Germany Chapter

BCM Berufsverband der Compliance Manager

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e.V.
Storkower Straße 158
10407 Berlin

www.isaca.de
info@isaca.de

Autorenteam:
- Andreas H. Schmidt, LL.M., CISA, CIPP/A
  (Collegium Auditores GmbH) – Fachgruppenleiter BCM
- Axel Dors, CISA (Dors Impuls Deutschland GmbH)
- Christine Kretschmann
- Diana Nestler, CISA
- Dirk Meissner (Allevio AG)
- RA Günter Untucht († 2018)
- Ioannis Karamitros
  (compliance-net GmbH) – Fachgruppenleiter ISACA
- Jutta E. Zilian, CGEIT, CISA, CISM, PMP, CAPM
- Prof. Dr. Michael Klotz (Hochschule Stralsund)
- Michael Kunzewitsch
- Oliver Dax
  (Genossenschaftsverband – Verband der Regionen e.V.)
- Peter Loos (NTT Group, NTT Security (Germany) GmbH)
- Stefan Purder

Die Inhalte dieses Leitfadens wurden von Mitgliedern des ISACA Germany Chapter e.V. erarbeitet und sind sorgfältig recherchiert. Trotz größtmöglicher Sorgfalt erhebt die vorliegende Publikation keinen Anspruch auf Vollständigkeit. Sie spiegelt die Auffassung des ISACA Germany Chapter wider. ISACA Germany Chapter e.V. übernimmt keine Haftung für den Inhalt.

Der jeweils aktuelle Leitfaden kann unter *https://www.isaca.de* kostenlos bezogen werden. Alle Rechte, auch das der auszugsweisen Vervielfältigung, liegen beim ISACA Germany Chapter e.V.

Stand: Januar 2021 (Final nach Review und Überarbeitung durch die ISACA-Fachgruppe IT-Compliance)

Leitfaden IT-Compliance

Grundlagen, Regelwerke, Umsetzung

ISACA®
Germany Chapter

Vorwort

Wie viele andere Technologien bietet die Informationstechnologie Menschen und Unternehmen mannigfache Vorzüge und verspricht Effizienzsteigerungen in vielen Lebens- und Arbeitsbereichen. Aber neue Technologien bergen auch immer das Potenzial für Gefährdungen und bieten Anreiz zum Missbrauch. Der Vergleich von Vorteilen und Nutzen einerseits mit Nachteilen und Gefahren der IT andererseits ist Bestandteil einer Risikoabwägung, deren Ergebnis wesentlich vom Risikoappetit des IT-Anwenders abhängt. Trifft das Risiko bei Eintritt nur den Anwender, dann ist er für den Schaden selbst verantwortlich und hat diesen zu tragen. Aber trägt er auch die Verantwortung, wenn die von ihm genutzte IT andere schädigt? Hier kommen der Gesetzgeber und Aufsichtsorganisationen ins Spiel. Diese haben Leitplanken in Form von Gesetzen und Vorgaben einzuziehen, um auf der einen Seite die Entwicklung und den Markteintritt neuer, nutzbringender IT-Lösungen nicht zu behindern bzw. zu verhindern, auf der anderen Seite aber auch Nutzer auf ihre gesellschaftliche Verantwortung hinzuweisen und möglicherweise von schädigenden Handlungen abzuhalten. Sollte es dennoch zum Schadensfall kommen, sollten die Betroffenen – soweit möglich – Ansprüche gegen den Schädiger geltend machen können. Wegen ihrer mittlerweile gegebenen Durchdringung aller Lebens- und Arbeitsbereiche muss dies für die Informationstechnologie heute erst recht gelten. Insofern ist es nicht verwunderlich, dass nunmehr seit einigen Jahren sowohl auf nationaler als auch internationaler Ebene wesentliche Modifikationen gesetzlicher Vorgaben, insbesondere zur Rechtssicherheit im elektronischen Geschäftsverkehr, zur Informationssicherheit, zum Datenschutz und im Bereich kritischer Infrastrukturen, in Kraft gesetzt wurden.

In gleicher Weise, wie sich die IT in Zukunft weiterentwickelt, werden sich Gesetzgebung und Rechtsprechung entwickeln. Für Unternehmen bedeutet dies eine ständig zunehmende Zahl an Vorgaben aus Gesetzen, Verordnungen und Urteilen, aber auch aus Normen und Standards. Hinzu kommen Verpflichtungen aus vertraglichen Vereinbarungen, die entweder die Informationsnutzung als wesentlichen Leistungsgegenstand regeln oder Nebenpflichten beinhalten, die sich auf die Informationsverarbeitung beziehen. Für Unternehmen aller Größenordnungen bedeutet dies wachsende Risiken aus potenziellen Regelverstößen der Informationsverarbeitung – die sich schon deswegen ergeben können, weil es eben mittlerweile kaum noch möglich ist, den Überblick zu behalten. Die Vermeidung derartiger Risiken durch Sicherstellung der Befolgung von Vorgaben ist Zielsetzung der Corporate Compliance, im IT-Bereich speziell der IT-Compliance. So stellt sich die Frage: Was ist zu tun, um IT-Compliance zu erreichen und zu erhalten? Die Antwort muss jedes Unternehmen selbst finden. Dieser Leitfaden soll dabei helfen, ein klares Verständnis für IT-Compliance zu erlangen und das Thema hinsichtlich anderer Handlungsfelder (z. B. IT-Governance, IT-Sicherheits- und IT-Risikomanagement) zu verorten. Dies ist die notwendige Grundlage, um Ziele, Umfang und Nutzen von IT-Compliance zu diskutieren, an IT-Compliance Beteiligte zu identifizieren und zu motivieren, Maßnahmen für IT-Compliance zu ergreifen und insbesondere Governance- und Managementstrukturen sowie entsprechende Prozesse für IT-Compliance einzurichten.

Die Autorinnen und Autoren

Die Fachgruppe »IT-Compliance«

Die Fachgruppe »IT-Compliance« wird von folgendem Selbstverständnis geprägt: Die Informationstechnologie in den Unternehmen muss sich permanent mit neuen Gesetzen, Standards und internen Regelungen auseinandersetzen. Für Führungskräfte und Mitarbeiter ist es schwierig, hier up to date zu bleiben. Noch viel schwieriger ist es für Informatiker und Techniker, diese Normen angemessen umzusetzen. Auf der anderen Seite stehen Juristen meist vor dem Problem, zu wenig technisches Grundwissen zu besitzen, um aus den Anforderungen Empfehlungen für die technische Umsetzung zu erarbeiten bzw. als Compliance-Verantwortliche den regelkonformen IT-Betrieb prüfen zu können. Die Fachgruppe »IT-Compliance« möchte hier eine Brücke schlagen. Durch die Kooperation der beiden Verbände ISACA Germany Chapter und dem Berufsverband der Compliance Manager (BCM) zu Beginn des Jahres 2017 kommen in Deutschland verbandsübergreifend technische Spezialisten aus den Bereichen IT-Audit, Informationssicherheit und IT-Governance mit Juristen in einer gemeinsamen Fachgruppe zusammen.

Die Fachgruppe »IT-Compliance« beschäftigt sich mit dem Berufsbild des IT-Compliance-Managers, der Ausgestaltung der IT-Compliance-Funktion und deren Schnittstellen in Unternehmen und bezieht Stellung zu aktuellen Entwicklungen der IT-Compliance. Sie verfolgt das Ziel, die Compliance-Landschaft nachhaltig zu prägen und wichtige Treiber für Wissen, Innovation und praktische Arbeitshilfen im Bereich der IT-Compliance zu sein. Hierfür erarbeiten die Mitglieder der Fachgruppe Arbeitspapiere und Leitfäden, die als Handlungshilfe den Mitgliedern kostenfrei zur Verfügung gestellt werden.

Sollten Sie Interesse an der Mitarbeit in der Fachgruppe »IT-Compliance« haben, können Sie über die Funktionsmail FG-IT-Compliance@isaca.de mit der Fachgruppe Kontakt aufnehmen.

Ioannis Karamitros
ISACA Germany Chapter e. V.
Leiter Fachgruppe IT-Compliance ISACA

Andreas H. Schmidt
Berufsverband der Compliance Manager e. V.
Leiter Fachgruppe IT-Compliance BCM

Danksagung

Die Grundlage des Leitfadens bildet die bereits im Jahr 2009 erschienene Broschüre »IT-Compliance – Ein Überblick« von Prof. Dr. Michael Klotz. Ein besonderer Dank gilt ihm, der dem ISACA Germany Chapter e.V. seine Broschüre zur Verfügung gestellt hat und maßgeblich an der Koordination und Weiterentwicklung mitgewirkt hat.

Der neue Leitfaden »IT-Compliance« entstand durch die enge Zusammenarbeit zwischen ISACA und der Fachgruppe IT-Compliance. Der Dank gilt den Autorinnen und Autoren des Leitfadens, die diesen umfassenden Leitfaden erst ermöglicht haben:

- Andreas H. Schmidt, LL.M., CISA, CIPP/A (Collegium Auditores GmbH) – Fachgruppenleiter BCM
- Axel Dors, CISA (Dors Impuls Deutschland GmbH)
- Christine Kretschmann
- Diana Nestler, CISA
- Dirk Meissner (Allevio AG)
- RA Günter Untucht († 2018)
- Ioannis Karamitros (compliance-net GmbH) – Fachgruppenleiter ISACA
- Jutta E. Zilian, CGEIT, CISA, CISM, PMP, CAPM
- Prof. Dr. Michael Klotz (Hochschule Stralsund)
- Michael Kunzewitsch
- Oliver Dax (Genossenschaftsverband – Verband der Regionen e.V.)
- Peter Loos (NTT Group, NTT Security (Germany) GmbH)
- Stefan Purder

Für das Korrekturlesen, die Qualitätssicherung und die Bereitstellung von Vorlagen geht der Dank an:

- Dr. Martin Fröhlich, CISA, CGEIT (IT Compliance Solutions)
- Marc Friedrich, CISA (BMW AG)
- Prof. Dr. Matthias Goeken (Hochschule der Deutschen Bundesbank und ISACA Germany Chapter)
- Levke Knaack (compliance-net GmbH)
- dpunkt.team

Inhaltsverzeichnis

1 Einleitung 7

2 IT-Compliance im Unternehmen 9

2.1 Aktualität von IT-Compliance ... 9
2.2 Begriff der IT-Compliance ... 11
2.3 IT-Compliance vs. IT-gestützte Compliance ... 12
2.4 Das IT-Compliance-Risiko ... 15
2.5 Integrationsbedarf von IT-Compliance ... 16
2.6 Handlungsfelder von IT-Compliance ... 18

3 Der Nutzen von IT-Compliance 21

3.1 Nutzen von IT-Compliance aus Sicht des Unternehmens ... 21
3.2 Nutzen von IT-Compliance aus Sicht der Unternehmensleitung ... 23
3.3 Nutzen von IT-Compliance aus Sicht der Fachabteilungen ... 24

4 Stakeholder und Interessenlagen 26

4.1 Struktur der Stakeholder ... 26
4.2 Unternehmensexterne Stakeholder ... 27
4.3 Unternehmensinterne Stakeholder ... 29

5 Für IT-Compliance relevante Regelwerke 33

5.1 Klassifikation der Regelwerke ... 33
5.2 Rechtliche Vorgaben ... 34
5.3 Verträge ... 38
5.4 Unternehmensexterne Regelwerke ... 38
5.5 Unternehmensinterne Regelwerke ... 40

6 Organisation der IT-Compliance 42

6.1 Ebenenmodell der IT-Compliance-Organisation ... 42
6.2 Die IT-Compliance im Rahmen des Drei-Linien-Modells ... 45
6.3 Der IT-Compliance-Manager ... 47

7 Compliance-Management-System in der IT (IT-CMS) 50

7.1 Das IT-CMS im Rahmen unternehmensweiter Compliance 50
7.2 Compliance-Kultur und Awareness 51
7.3 Identifizierung von Anforderungen für die IT und Ableitung von konkreten Handlungsanweisungen 53
7.4 Steuerung von IT-Compliance-Risiken 55
7.5 Monitoring und Messung des IT-Compliance-Levels 55
7.6 Kontinuierliche Verbesserungen des IT-CMS 56
7.7 Der Umgang mit Non-Compliance und der Einsatz von Korrekturmaßnahmen im IT-CMS 57

8 Ausblick 59

Abkürzungsverzeichnis 60

Quellenverzeichnis 63

1 Einleitung

Spätestens seit im April 2016 das Gesetzgebungsverfahren für die Datenschutz-Grundverordnung (DSGVO) mit Unterzeichnung durch die Präsidenten des Europäischen Parlaments und des Rates abgeschlossen war, musste den allermeisten, insbesondere den größeren Unternehmen klar sein, dass einer effektiven und effizienten IT-Compliance eine kritische Bedeutung zukommt. Wesentlicher Grund hierfür sind die immensen Bußgelder, die bei Verstoß drohen – im Maximalfall 20 Mio. Euro oder 4 % des weltweit erzielten Umsatzes (nach [DSGVO 2018, Art 83 Abs. 5]). Dass Forderungen in dieser Höhe keine Drohkulisse sind, zeigen die drei größten im Jahr 2019 verhängten Bußgelder gegen British Airways (über 204 Mio. Euro), Marriott International (über 110 Mio. Euro) und Google (50 Mio. Euro) [GDPR ET].

Die DSGVO und die Neufassung des Bundesdatenschutzgesetzes (BDSG) vom Juni 2017 fordern viele Maßnahmen, die heute auch als State of the Art für IT-Compliance anzusehen sind:

- Grundsätze regeln das Handeln der Nutzer in Bezug auf personenbezogene Daten.
- Verhaltensregeln sollen den Akteuren eine Orientierung bieten.
- Umfassende Informations- und Dokumentationspflichten gewährleisten Transparenz und damit Nachvollziehbarkeit.
- Bei hohen Risiken hat eine Folgenabschätzung zu erfolgen.
- Geeignete technische und organisatorische Maßnahmen sind risikobasiert auf Basis der beiden Prinzipien »Privacy by Design« und »Privacy by Default« umzusetzen.
- Verantwortlichkeiten sind sowohl für unternehmensinterne als auch -externe Akteure festzulegen – intern betrifft dies die Position des Datenschutzbeauftragten.
- Bei Verstoß gegen Datenschutzvorgaben bestehen Meldepflichten.
- Und nicht zuletzt soll eine Zertifizierung die Einhaltung der Datenschutzvorgaben bestätigen.

Der Umfang dieser Anforderungen erfordert die Einrichtung eines Datenschutz-Management-Systems. Um Synergien zu realisieren, sollte dieses Teil eines Compliance-Management-Systems für die IT sein, das wiederum Teil des unternehmensweiten Compliance-Management-Systems sein muss. Hierbei stellen sich Fragen nach dem Umfang und dem Anwendungsbereich von IT-Compliance, nach Beteiligten, erforderlichen Verantwortungs- und Prozessstrukturen, Instrumenten und Verfahren, nach Integration mit anderen IT-Managementsystemen und nicht zuletzt nach Zielen und Nutzen von IT-Compliance. Viele dieser Aspekte sollen in diesem Leitfaden behandelt werden. Die Handlungsorientierung steht hierbei im Vordergrund – der Leitfaden soll anleiten. Erfolgreiches Managementhandeln erfordert klare Begriffe, ein Wissen um Anforderungen und Ressourcen einerseits sowie um Risiken und Potenziale andererseits. Dies soll dieser Leitfaden leisten – im Rahmen seines Umfangs und der konzeptionellen und praktischen Erfahrungen seiner Autorinnen und Autoren. Hierbei wird eine interdisziplinäre Sicht eingenommen, d. h., die bei Compliance unentbehrliche juristische Perspektive[1] wird durch fachliche Sichtweisen (v. a. der Disziplinen Management, Prüfung, Organisation, Personal, Wirtschaftsinformatik) ergänzt. Weiterhin wird eine weitgehende Branchenneutralität gewahrt. Gleichwohl sind einzelne Branchen, wie z. B. Finanzdienstleistungen, durch ein anspruchsvolles regulatives Umfeld geprägt, sodass sie gute Beispiele für die Diskussion von Compliance-Herausforderungen bieten und deswegen in diesem Leitfaden angeführt werden.

Im zweiten Kapitel erfolgt eine begriffliche Grundlegung, die deshalb besonders wichtig ist, da Umfang und Anwendungsbereich der real praktizierten IT-Compliance direkt vom Begriffsverständnis von IT-Compliance abhängen. Weiterhin werden Bezüge der IT-Compliance zu anderen Bereichen der IT-Governance und des IT-Managements aufgezeigt, z. B. zum IT-Sicherheitsmanagement oder zum IT-Risikomanagement. Eine Übersicht über aktuelle Handlungsfelder der IT-Compliance komplettiert das Kapitel. Im dritten Kapitel werden die an IT-Compliance beteiligten Akteure und ihre Interessenlagen dargestellt. Der Nutzen von IT-Compliance ist Inhalt des vierten Kapitels. Das fünfte Kapitel gibt einen Überblick über die für IT-Compliance relevanten Regelwerke, deren Vorgaben Quellen von IT-Compliance-Anforderungen darstellen, klassifiziert diese und stellt wesentliche Regelwerke beispielhaft dar. Im sechsten Kapitel wird die Organisation der IT-Compliance mit einem Ebenenmodell, der Positionierung der IT-Compliance im Rahmen der »Three Lines of Defense« und mit Ausführungen zur Position des IT-Compliance-Managers behandelt. Das siebte Kapitel beinhaltet Überlegungen zum IT-Compliance-Management-System (IT-CMS), wobei der

[1] Für eine Darstellung von IT-Compliance aus juristischer Sicht siehe [Stögmöller 2019].

Fokus auf Fragen der Implementierung eines IT-CMS liegt. Der Leitfaden endet mit einem Ausblick.

Auch wenn dies ein Leitfaden des ISACA Germany Chapter ist, wird IT-Compliance nicht nur aus Sicht von COBIT[2] betrachtet.[3] Gleichwohl finden sich an vielen Stellen Referenzierungen auf COBIT. Hierfür wird die aktuelle Version COBIT 2019 zugrunde gelegt. Dadurch, dass im Rahmen der Gesamtsicht des Leitfadens immer wieder auf COBIT 2019 Bezug genommen wird, wird die Compliance-Thematik in COBIT 2019 im Zusammenhang verdeutlicht.

Der Leitfaden basiert auf der 2009 im dpunkt.verlag erschienenen Broschüre »IT-Compliance« [Klotz 2009]. Die Darstellung wurde von den Autorinnen und Autoren überarbeitet, in vielen Einzelpunkten aktualisiert und in Bezug auf neue Entwicklungen der IT-Compliance, Best Practices, neue Vorgaben und vor allem auch zwischenzeitlich gemachte Erfahrungen erweitert.

[2] Ursprünglich stand »COBIT« als Akronym für »Control Objectives for Information and Related Technology«. Seit der Version »COBIT 5« wird »COBIT« nur noch als eigenständiger Terminus verwendet, um die erweiterte Governance- und Managementperspektive zu signalisieren; vgl. [ISACA 2012, S. 90].

[3] Wer hieran interessiert ist, sei verwiesen auf [Klotz 2014] und [Klotz 2019].

2 IT-Compliance im Unternehmen

2.1 Aktualität von IT-Compliance

Die Treiber für einen höheren Stellenwert, einen größeren Aufgabenumfang und demgemäß auch einen Verantwortungszuwachs der IT-Compliance sind zahlreich (vgl. Abbildung 2–1). Die grundlegende Ursache ist die Digitalisierung der Geschäftsprozesse, verbunden mit der Dynamik der gesetzlichen und regulatorischen Entwicklung.

Ein offensichtlicher Treiber für IT-Compliance sind die von Unternehmen kontinuierlich neu zu berücksichtigenden Anforderungen, insbesondere in Form von Gesetzen und regulatorischen Vorgaben durch Aufsichtsbehörden. In der Einleitung wurde die DSGVO bereits beispielhaft erwähnt. Sie ist seit dem 25. Mai 2018 anzuwenden (vgl. [DSGVO 2018, Art. 99]). Lange Zeit waren die deutschen Aufsichtsbehörden bei der Verhängung von Bußgeldern wegen Verstößen gegen die DSGVO im Vergleich zu den Datenschutzbehörden in anderen europäischen Ländern zurückhaltend. Zuletzt jedoch wurde im Oktober 2020 vom Hamburgischen Beauftragten *für Datenschutz und Informationsfreiheit* gegen die H&M Hennes & Mauritz Online Shop A.B. & Co. KG ein Bußgeld in Höhe von über 35 Mio. Euro verhängt (vgl. [GDPR ET]). Vor allem mit Blick auf das Bußgeldkonzept der deutschen Datenschutzkonferenz (DSK) kann als sicher gelten, dass die Zeit der nachsichtigen Bemessung von Bußgeldern vorbei ist. Danach sehen sich Unternehmen mit einem Umsatz ab 45 Mio. Euro Bußgeldern in sechsstelliger Höhe gegenüber, die je nach Schwere des Vergehens mit einem Faktor von 1 bis 6 multipliziert werden. Ab einem Umsatz über 500 Mio. Euro soll der prozentuale Bußgeldrahmen der DSGVO angewendet werden (nach [DSK 2019, S. 6 ff.]).

Neben dem Datenschutz ist es vor allem die Gewährleistung der Informationssicherheit, die durch Gesetze und regulative Vorgaben verstärkt gefordert wird. Aufgrund der exponentiell zunehmenden Bedrohungslage hinsichtlich Cybercrime und der hieraus erheblichen Gefahr für die Versorgungssicherheit der Bevölkerung wurde am 24. Juni 2015 das Gesetz zur Erhöhung der Sicherheit in der Informationstechnik (IT-Sicherheitsgesetz) als Artikelgesetz erlassen. Sein primäres Ziel ist es, die Sicherheit von kritischen Dienstleistungen (kDL) derjenigen Wirtschaftssektoren, deren Versorgungssicherheit essenziell für die Bevölkerung ist, auf ein gemeinsames hohes Niveau zu heben. Infolge des Gesetzes wurde ein Meldewesen aufgebaut, in dem das Bundesamt für die Sicherheit in der Informationstechnik (BSI) bei Sicherheitsvorfällen als zentrale Meldestelle für die betroffenen Betreiber kritischer Infrastrukturen (KRITIS) dient. KRITIS-Betreiber wiederum erhalten vom BSI aktuelle sicherheitsrelevante Informationen (vgl. § 8b BSIG).

Ähnliche Strukturen existieren auf europäischer Ebene. Grundlage hierfür ist die EU-Richtlinie zur Netz- und Informationssicherheit (NIS), die im August 2016 in Kraft getreten ist und deren deutsches Umsetzungsgesetz am 29.06.2017

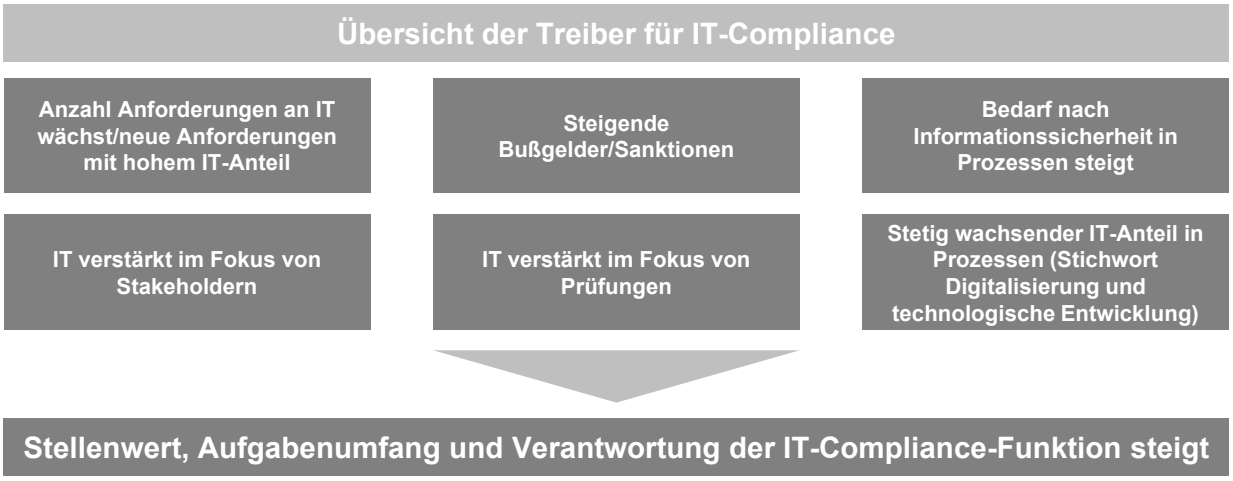


Abb. 2–1: Treiber für IT-Compliance

verkündet wurde[1]. Für die Versorgungssicherheit in Deutschland ist die Richtlinie von hoher Bedeutung, da durch die starke Vernetzung der Infrastrukturen in der EU IT-Systemstörungen oder -ausfälle zu erheblichen Domino-Effekten in den gegenseitig abhängigen Wirtschaftssektoren führen können. Aufgrund dieser Gesetzeslage in Deutschland sind Betreiber kritischer Infrastrukturen nunmehr gehalten, alle zwei Jahre durch ein Audit die Ausfallsicherheit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind, gegenüber dem BSI nachzuweisen. Dieses Audit kann auf Basis von branchenspezifischen Sicherheitsstandards, die durch das BSI zu genehmigen sind, erfolgen. Darüber hinaus kann das BSI selbst Audits durchführen bzw. durchführen lassen (vgl. § 8a Abs. 4 BSIG).

Diese Gesetzgebung hinsichtlich Informationssicherheit ist ein gutes Beispiel dafür, wie zusehends weitere Stakeholder am Compliance-Horizont der Unternehmen in Erscheinung treten. Nicht nur die Zahl von Aufsichtsinstitutionen nimmt zu, sondern auch ihre Informations- und Überwachungsbefugnisse sowie ihre Eingriffsmöglichkeiten. Unternehmen sind damit sowohl quantitativ als auch qualitativ mit mehr bzw. anspruchsvolleren Compliance-Anforderungen konfrontiert.

Ein weiteres Beispiel dafür, dass sich das IT-Compliance-Management in Unternehmen – in diesem Fall in Kreditinstituten und Finanzdienstleistungsunternehmen – aktuell weiterentwickeln muss, bieten die Vorgaben der Bundeanstalt für das Finanzwesen (BaFin). Diese veröffentlichte am 6. November 2017 die »Bankaufsichtlichen Anforderungen an die IT« (BAIT), eine Konkretisierung der ebenfalls novellierten Mindestanforderungen an das Risikomanagement (MaRisk). In den BAIT erläutert die BaFin, »was sie unter einer angemessenen technisch-organisatorischen Ausstattung der IT-Systeme, unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit sowie eines angemessenen Notfallkonzepts, versteht« [BaFin 2017b]. Dies hat zur Folge, dass sich Prüfungen durch die BaFin – neben der bisherigen Konzentration auf betriebswirtschaftliche Kennzahlen und Risikoindikatoren der Finanzinstitute –vermehrt auf den ordnungsmäßigen IT-Betrieb fokussieren werden. Hierbei stehen gemäß der Digitalisierungsstrategie der BaFin u. a. sowohl die Sicherstellung der laufenden Überwachung der IT-Sicherheit als auch die Weiterentwicklung der Aufsichtspraxis, z. B. hinsichtlich der Umsetzung der BAIT und der »Versicherungsaufsichtlichen Anforderungen an die IT« (VAIT) sowie der Cloud-Dienstleistungen, im Vordergrund (vgl. [BaFin 2018a, S. 3]).

Im Tagesgeschäft sind es neben den zu erfüllenden neuen Compliance-Anforderungen die Fälle von verfehlter Compliance, also der Verstoß gegen Vorgaben, die Maßnahmen in Bezug auf IT-Compliance nach sich ziehen. Folgende aus den Erfahrungen der am Leitfaden beteiligten Autorinnen und Autoren stammende Beispiele zeigen die Vielfalt mangelnder Konformität mit Vorgaben:

- Verstöße gegen Telemediengesetz (TMG) und Urheberrechtsgesetz (UrhG) im Rahmen der Nutzung dienstlicher E-Mail-Accounts
- Verstöße gegen §§ 202ff. StGB (Strafgesetzbuch) im Rahmen von Administratoraufgaben
- Verstöße gegen § 257 HGB (Handelsgesetzbuch) respektive § 140ff. AO (Abgabenordnung) bzw. § 14b UStG (Umsatzsteuergesetz) hinsichtlich der Aufbewahrung bzw. Archivierung von Geschäftsbriefen und Rechnungen
- Verstöße gegen DSGVO/BDSG hinsichtlich der Löschung von personenbezogenen Daten, wenn die Voraussetzungen nach Art. 6 Abs. 1 DSGVO nicht mehr gegeben sind
- Verstöße gegen die Meldepflichten nach § 8b Abs. 4 BSIG (BSI-Gesetz)
- Verstöße gegen interne Anforderungen bzgl. der Trennung von Entwicklungs-, Test- und Produktionsumgebung
- Verstöße gegen die Grundsätze des Vier-Augen-Prinzips bei der Gewährung von Berechtigungen in Buchhaltungssystemen
- Verstöße gegen § 289 Abs. 1 Satz 4 HGB wegen mangelnder Transparenz im Lagebericht des Jahresabschlusses hinsichtlich der Risiken aufgrund der Non-Compliance der technisch-organisatorischen Maßnahmen (TOM) in der IT
- Verstöße gegen die unternehmensspezifische Clean Desk Policy durch nicht sachgerechten und verantwortungsbewussten Umgang mit Informationen und Vorgaben bzgl. Sicherheit am Arbeitsplatz
- Verstöße gegen die ISO/IEC-27000-Reihe aufgrund der Nichteinhaltung von internen Regelungen zur Sicherheit, wie z. B. Umgang mit mobilen Geräten, Umgang mit Datenträgern, Vergabe, Protokollierung und Auswertung von (kritischen) Berechtigungen oder Kryptografie

Die Auflistung zeigt beispielhaft, dass die Frage nach Regelkonformität bei der Nutzung von IT nicht nur Datenschutz und IT-Sicherheit fokussiert, sondern alle IT-gestützten Prozesse eines Unternehmens betrifft. Die Beispiele beinhalten neben den Verstößen gegen gesetzliche Vorgaben auch solche gegen interne Regelungen sowie gegen Normen und Standards. Auch die Situationen, in denen die jeweilige Non-Compliance festgestellt wurde, sind unterschiedlich. Im Worst Case wird ein Verstoß zu spät erkannt und das Unternehmen erhält erst Kenntnis darüber, wenn der Fall in den Medien präsent ist oder zur Anzeige gelangt. Um dies zu vermeiden, sind in der IT effektive Überwachungsmechanismen im Rahmen einer Struktur nach dem sogenannten Drei-Linien-Modell (Three Lines Model, TLM) zu instal-

[1] Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

lieren.[2] Daneben ist durch Awareness-Maßnahmen sicherzustellen, dass die Mitarbeiter proaktiv sicherheitsbewusst und compliant agieren.

Neben Einheiten der zweiten Linie, wie dem Datenschutzbeauftragten (DSB) oder dem IT Security Officer, ist es insbesondere die Interne Revision als dritte Linie, die Compliance-Verstöße aufdeckt. Zudem werden Verstöße auch über vom Unternehmen bereitzustellende Hinweisgebersysteme (»Whistleblowing«) angezeigt. Darüber hinaus können technische Hilfsmittel zum Einsatz kommen, wie zum Beispiel im Security Information and Event Management (SIEM), die System- und Protokolldaten systematisch auswerten und in Gefahrsituationen alarmieren. Auch und gerade für IT-Compliance gilt: Potenziellen Verstößen und Fehlern ist vor allem durch automatisierte und präventiv wirkende Überwachungsmaßnahmen zu begegnen. So bietet es sich beispielsweise an, Verstöße und Missbrauch rund um die Vergabe von kritischen Berechtigungen durch ein technisch unterstütztes Privileged Access Management (PAM), das diese kritischen Zugriffe revisionssicher verwaltet, zu vermeiden.

Als Fazit ist die Aussage zu treffen, dass bei Weitem nicht nur die IT-Compliance-Funktion zur Aufdeckung von Non-Compliance beiträgt. Diese ist aber spätestens dann beteiligt, wenn es um IT-bezogene Maßnahmen zur Schadensminderung und vermeidung für die Zukunft geht.

Für COBIT 2019 stellt Compliance ein wichtiges Ziel der Governance dar. Durch Maßnahmen der Governance ist sicherzustellen, dass auch die Compliance im Hinblick auf die Unternehmensziele und die geplante Unternehmensentwicklung überwacht wird (vgl. [ISACA 2018a, S. 13]). Veränderte Compliance-Anforderungen stellen einen wichtigen externen Treiber für IT-Governance dar. Hier führt COBIT 2019 neue Gesetze und regulatorische Vorgaben an, die oft Auswirkungen auf ein bestehendes IT-Governance-System haben. So lösen erweiterte Berichtsanforderungen, z. B. seitens einer Aufsichtsbehörde, angesichts der Durchgängigkeit der IT häufig Veränderungen für das IT-Governance-System aus.[3]

2.2 Begriff der IT-Compliance

In einem allgemeinen, grundlegenden Verständnis ist ein Unternehmen dann »compliant«, wenn es die für seine Geschäftstätigkeit relevanten Vorgaben befolgt. Neben »Befolgung« werden auch die Begriffe »Übereinstimmung«, »Einhaltung«, »Konformität«, »Erfüllung« oder »Entsprechung« verwendet.[4] Welche Vorgaben relevant sind, ist einerseits unternehmensextern vorgegeben, andererseits selbst gewählt. Dementsprechend lässt sich der Compliance-Begriff wie folgt fassen: Compliance liegt vor, wenn alle für das Unternehmen relevanten, d. h. verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden. In dieser Sichtweise stellt Compliance einen Zustand dar – und nicht in erster Linie eine Organisationseinheit oder ein Handeln der Mitarbeiter, auch wenn eine Abteilung oder Stellen mit Compliance-Aufgaben ebenso wie vorgabenkonformes Handeln wichtige Voraussetzungen darstellen, um Compliance als Zustand der Einhaltung von Vorgaben zu erreichen (vgl. [Klotz 2007, S. 14]). Mit dieser Begriffsfassung wird betont, dass es aus Unternehmenssicht entscheidend ist, dass Compliance zum Zeitpunkt einer Prüfung (durch die Interne Revision, den Wirtschaftsprüfer, den Betriebsprüfer, Prüfer von Aufsichtsbehörden oder sonstige Auditoren und Personen[5]) vorliegt.

Compliance in den verschiedenen Funktionen des Unternehmens stellt jeweils eine Spezialisierung dieses allgemeinen Compliance-Begriffs dar (Vertriebs-Compliance, Compliance der Rechnungslegung, Beschaffungs-Compliance, Tax-Compliance etc.). Somit ergibt sich für den Begriff der IT-Compliance als Spezialisierung des oben angeführten allgemeinen Compliance-Begriffs folgende Definition:[6]

IT-Compliance bezeichnet einen Zustand, in dem alle für die IT des Unternehmens relevanten, d. h. verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben eingehalten werden.

Damit stellt IT-Compliance letztlich einen Zielzustand dar, der mal mehr und mal weniger erreicht sein mag. IT-Compliance ist damit als »moving target« charakterisiert – was gleichzeitig vermittelt, dass ein hinreichendes Ausmaß an IT-Compliance als Zustand nicht durch vereinzelte Maßnahmen zu erreichen ist. Zudem ist das ökonomische Prinzip zu beachten, d. h., die Kosten für Maßnahmen der IT-Compliance sind den Risiken für Non-Compliance der IT gegenüberzustellen. Was zu unternehmen ist, um IT-Compliance zu erreichen, muss also jedes Unternehmen in seinem spezifischen Umfeld situationsabhängig entscheiden.[7]

[2] Vgl. das aktuelle Drei-Linien-Modell des IIA [IIA 2020; Eulerich 2020]. In der Vorversion wurde noch der Begriff »Verteidigungslinien« verwendet.

[3] Nach [ISACA 2018d, S. 28], vgl. [Klotz 2019, S. 12].

[4] Beispielsweise verwendet der Deutsche Corporate Governance Kodex explizit den Begriff »Compliance« und versteht darunter »die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien« [DCGK 2019, Grundsatz 5], vgl. [Hauschka et al. 2016, S. 6].

[5] Eine »Prüfung« ist hier in einem weiten Begriffsumfang zu verstehen. Auch ein (nicht beauftragter) Hacker führt i. d. S. eine »Prüfung« durch, wenn sein Angriff erweist, ob sich das Unternehmen an Vorgaben aus IT-Sicherheitsstandards und -normen gehalten hat.

[6] Nach [Klotz/Dorn 2008, S. 5f.]; im Grundsatz ebenso [Falk 2012, S. 37].

[7] Deswegen macht es auch keinen Sinn, einzelne Maßnahmen in eine allgemeine Definition für IT-Compliance aufzunehmen. Jede Auflistung, und sei sie auch noch so umfangreich, muss notwendig unvollständig bleiben oder für den Einzelfall irrelevante Bestandteile enthalten.

COBIT 2019 bietet keine explizite Definition für IT-Compliance, fordert jedoch durchgängig die Compliance mit verschiedensten Anforderungen (im Folgenden nach [Klotz 2019, S. 12f.]). Diese stammen vor allem aus Gesetzen und regulativen Vorgaben. Die diesbezügliche externe Compliance ist Zielinhalt des IT-bezogenen Ziels AG01 (I&T compliance and support for business compliance with external laws and regulations).[8] Als Rechtsbereiche werden z. B. Datenschutz, Finanzberichterstattung, Urheberrecht, Gesundheit und Arbeitssicherheit ausdrücklich genannt.[9] Zur externen Compliance zählen weiterhin vertragliche Vereinbarungen. 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 aufgeführt wird (vgl. z. B. [ISACA 2018a, S. 30]). Als Verträge werden zudem explizit Lizenzvereinbarungen genannt.[10] Auch zur externen Compliance gehörig, aber seltener genannt, ist die Compliance mit Normen und Standards[11]. So fordert COBIT 2019 beispielsweise für das Enterprise Architecture Management (EAM) die Compliance mit entsprechenden Normen und Richtlinien.[12]

Die Compliance mit internen IT-Richtlinien stellt das IT-bezogene Ziel AG11 (I&T compliance with internal policies) dar. Hierunter ist das Befolgen aller Formen interner Vorgaben zu verstehen, z. B. Unternehmensrichtlinien, Hausstandards oder interne Verfahren und Methoden, die in den verschiedenen Unter nehmensfunktionen zum Einsatz gelangen.[13]

Da COBIT 2019 auf die Einhaltung all dieser Compliance-Anforderungen abstellt und diese insbesondere an Fällen von Non-Compliance und damit verbundenen monetären und nicht monetären Schadensfolgen misst, entspricht das Compliance-Verständnis von COBIT 2019 durchaus dem oben beschriebenen zustandsorientierten Compliance-Begriff.

Neben der Bestimmung als Zustand sind weitere Elemente der Definition von praktischer Bedeutung:

- Compliance liegt in der Verantwortung der Unternehmensleitung und damit grundsätzlich auch die IT-Compliance. Dies gilt umso mehr, wenn die IT-Leitung als Chief Information Officer (CIO) Mitglied der Unternehmensleitung ist. Unternehmens- und IT-Leitung dürfen IT-Compliance nicht nur als Pflichtübung begreifen, sondern müssen sichtbar als treibende Kraft agieren. Dies zeigt sich vor allem in einem deutlichen Bekenntnis zu IT-Compliance, verbunden mit einer konsequenten und sichtbaren Sanktionierung von Compliance-Verstößen (vgl. [Klotz 2020, S. 844]).
- Es sind nicht nur extern verbindliche Vorgaben, v. a. aus Gesetzen und Verordnungen, in den Geltungsbereich von IT-Compliance einzubeziehen. Das Unternehmen kann sich entscheiden, z. B. aus Gründen der Effizienz oder der Qualität, darüber hinaus weitere Regelwerke für sich als intern verbindlich zu betrachten.[14] Dies gilt insbesondere für IT-Normen und Standards, die in Fachkreisen entwickelt wurden und häufig den State of the Art abbilden.
- Die Forderung nach Nachweisbarkeit verweist darauf, dass Compliance in seiner Wirksamkeit auch dokumentiert werden muss. Die faktische Nachweisbarkeit ist gegenüber Aufsichtsorganen und Prüfungsinstitutionen (z. B. interne Revision, Wirtschaftsprüfer, Prüfer von Aufsichtsbehörden) notwendig, aber vor allem auch, um sich ggf. gegenüber externen Dritten im Verdachts- oder Streitfall exkulpieren zu können.
- Die zu befolgenden Vorgaben für die Unternehmens-IT können aus sehr unterschiedlichen Regelwerken kommen. Es lassen sich drei Gruppen unterscheiden. (1) Rechtliche Vorgaben an die IT, d. h. im Wesentlichen Gesetze und Rechtsverordnungen, Rechtsprechung, Verwaltungsvorschriften sowie Verträge mit Kunden, Lieferanten und sonstigen Vertragspartnern, soweit IT-relevante Vereinbarungen enthalten sind, (2) unternehmensexterne, auf IT-bezogene Regelwerke, wie Normen, Branchen- oder Verbandsstandards, (3) unternehmensinterne Regelwerke, soweit sie IT-relevante Vorgaben beinhalten, z. B. IT-Richtlinien, interne Vereinbarungen oder IT-Hausstandards (nach [Klotz 2020, S. 867f.]).

2.3 IT-Compliance vs. IT-gestützte Compliance

Auch wenn die Compliance der IT neben der Compliance der verschiedenen anderen Unternehmensfunktionen steht, kommt ihr doch eine herausgehobene Rolle zu. Diese resultiert aus den beiden Perspektiven der IT-Compliance als Compliance der IT-Funktion einerseits und der IT-gestützten Compliance, die durch die Fachabteilungen sicherzustellen ist, andererseits (vgl. Abbildung 2–2).

Im ersten Fall ist mit »IT« die entsprechende Organisationseinheit (IT-Funktion, IT-Abteilung, IT-Department etc.) bezeichnet; es liegt – wie bei anderen Unternehmensfunktionen auch – eine funktionsspezifische Spezialisierung der Compliance vor. Hierbei ist es unerheblich, ob die IT-Leistungen unternehmensintern oder durch externe IT-Dienstleister (im Rahmen von Entwicklungs-, Hosting-, Outsourcing-Verträgen o. Ä.) erbracht werden. Diese »Compliance von IT« stellt somit im Wesentlichen eine Verantwortung der IT-Funktion dar. Die Vorgaben richten sich hier direkt an die IT.

8 Vgl. z. B. [ISACA 2018a, S. 30]; COBIT 2019 spricht von Alignment Goals (AG), in COBIT 5 noch als »IT-related Goals« bezeichnet. Mit Verweis auf [Gaulke 2020, S. 145] wird im Folgenden die Bezeichnung »IT-bezogene Ziele« verwendet.

9 Vgl. die Auflistung in MEA03.01, Aktivität 2, s. [ISACA 2018b, S. 285].

10 Vgl. die Beschreibung der Zielsetzung von BAI09, s. [ISACA 2018b, S. 209].

11 Der englische Begriff »Standard« in COBIT 2019 steht für Normen, bspw. von ISO/IEC oder NIST, Standards werden eher mit den Begriffen »framework« und »guidance« belegt.

12 Vgl. APO03.05, Aktivität 5, s. [ISACA 2018b, S. 76].

13 Vgl. MEA03.03, s. [ISACA 2018b, S. 286].

14 Die DIN EN ISO/IEC 27001 sieht dies in ihrer Compliance-Definition ebenso, vgl. [DIN EN ISO/IEC 27002:2017, S. 101].

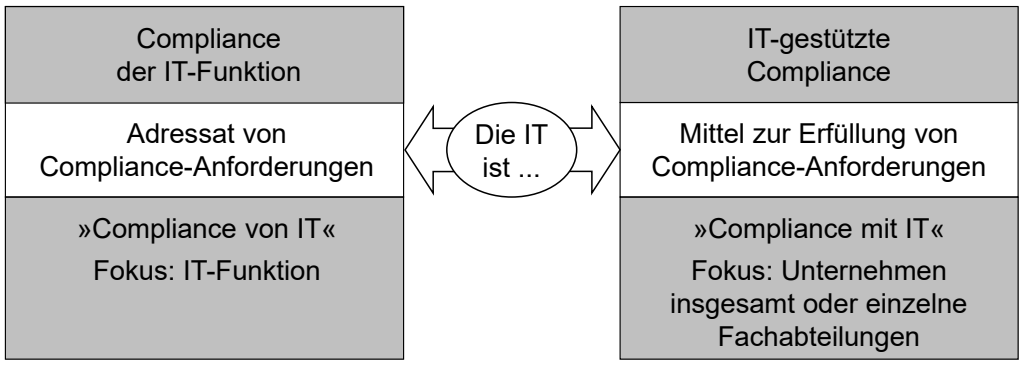


Abb. 2–2: IT-Compliance vs. IT-gestützte Compliance (vgl. [Klotz/Dorn 2008, S. 9])

Beispiele:

Anforderungen zur Vernichtung von Datenträgern sind in verschiedenen Regelwerken enthalten:

- Die DIN EN ISO/IEC 27001:2017 enthält in A.8.3.2 die Forderung, dass nicht mehr benötigte Datenträger sicher und gemäß einem formalen Verfahren entsorgt werden (nach [DIN EN ISO/IEC 27001:2017, S. 20]).
- Die DIN SPEC 66399 fordert für die Datenträgervernichtung durch die verantwortliche Stelle, dass technische und organisatorische Maßnahmen für den Vernichtungsprozess zu definieren sind (nach [DIN SPEC 66399-3:2013, S. 9]).
- Nach Artikel 32 DSGVO hat der für die Verarbeitung personenbezogener Daten (wozu nach Art. 4 Nr. 2 DSGVO explizit auch die Vernichtung von Daten zählt) Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (nach [DSGVO 2018, Art. 32 Abs. 2]).
- Nach der COBIT-Managementpraktik BAI09.03 sind IT-Vermögenswerte entsprechend einem Standard-Lebenszyklus von der Beschaffung bis zur Entsorgung zu managen. Die Entsorgung hat explizit die dauerhafte Löschung von aufgezeichneten Daten auf Datenträgern sicherzustellen (nach [ISACA 2018b, S. 210f.]).
- Der Baustein »CON.6 Löschen und Vernichten« des IT-Grundschutzkompendiums des Bundesamtes für die Sicherheit in der Informationstechnik beinhaltet die Anforderung, dass für das Löschen und Vernichten von Datenträgern geeignete Verfahren ausgewählt werden sollten (nach [BSI 2019]).
- In den EVB-IT Instandhaltungs-AGB ist in Abschnitt 6.4 festgelegt, dass (unter bestimmten Voraussetzungen) die Entsorgung von Datenträgern durch den Auftragnehmer so zu erfolgen hat, dass die gespeicherten Daten weder lesbar noch rekonstruierbar sind (nach [EVB-IT Instandhaltungs-AGB 2016, S. 5]).

Alle Beispiele betreffen die Gestaltung eines formalen, systematischen Prozesses der Daten- bzw. Datenträgervernichtung, prinzipiell unabhängig vom Anwendungsbereich (wenn auch in Abhängigkeit vom Schutzbedarf der betroffenen Daten). Damit richten sich diese Vorgaben an die betreffenden Spezialisten der IT-Abteilung, wobei durchaus eine Zusammenarbeit mit weiteren Stellen, z. B. dem Datenschutzbeauftragten oder der Unternehmenssicherheit, erforderlich sein kann.

Im zweiten Fall wird IT-Compliance als Einsatz von Soft- und Hardwareprodukten verstanden, mit deren Hilfe die Einhaltung von Vorgaben für das Unternehmen insgesamt oder einzelne Fachabteilungen sichergestellt werden kann. In diesem Sinne handelt es sich um »IT-gestützte Corporate Compliance« [Teubner/Feller 2008, S. 401]. Diese Interpretation wird vor allem von Herstellern vertreten, die Lösungen für Security- oder Content-Management, Archivierung, Verschlüsselung, Nutzer-, Zugangs- und Lizenzverwaltung u. a. m. anbieten. Im Unternehmen sind es die Anwender der IT-Systeme, d. h. die Fachabteilungen, die sich »compliant« gegenüber Vorgaben verhalten müssen. Daneben stehen vor allem auch diverse IT-Governance-Funktionen in der Pflicht, aus der »2nd Line« heraus Vorgaben zu erstellen und ihre Einhaltung zu überwachen. Für die Umsetzung dieser Vorgaben bzw. für eine »ganzheitliche Compliance« müssen auch Fachbereiche außerhalb der IT mitwirken, z. B. bei der Vergabe oder dem Entziehen von Berechtigungen im Rahmen eines Access & Identity Management (AIM). Die IT-Funktion stellt hierbei als interner Dienstleister IT-Services zur Verfügung, die von den Fachabteilungen genutzt werden können, um nicht gegen relevante Vorgaben zu verstoßen. Compliance kann hier als Teil von IT-Services aufgefasst werden, ohne dass die Einhaltung von Vorgaben den Nutzern in der Fachabteilung ständig bewusst sein muss.

Beispiele:

- Die IT-Funktion betreibt ein IT-System für das Customer Relationship Management (CRM). Die Nutzung desselben erfolgt durch die Marketingabteilung auf Basis eines Service Level Agreement (SLA). Im SLA ist unter anderem geregelt, dass mit Bereitstellung des Service sichergestellt ist, dass u. a. auch gesetzliche Vorgaben zur Identifizierung der Kunden (»know your customer«) erfüllt werden.
- Im Rahmen einer anstehenden Betriebsprüfung muss die Abteilung »Rechnungswesen« dem Betriebsprüfer nach Vorgaben der Abgabenordnung Einsicht in die Buchhal-

tungsdaten ermöglichen. Daraufhin beauftragt sie die IT-Funktion, im Berechtigungssystem eine Prüfer-Rolle mit Lesezugriff einzurichten.
- Vor dem Hintergrund der Produkthaftung soll in der F&E-Abteilung eine lückenlose Dokumentation aller Qualitätssicherungsmaßnahmen während der Produktentwicklung erfolgen. Die IT-Abteilung unterstützt diese Zielsetzung mit der Einrichtung eines Dokumentenmanagementsystems.
- Das Access & Identity Management regelt den grundsätzlichen Umgang mit Berechtigungen und privilegierten Zugriffen. Die Fachabteilungen stehen hier primär in der Verantwortung, für die eigenen Systeme (kritische) Berechtigungen zu identifizieren, zu dokumentieren und nach AIM-Prinzipien, wie z. B. »need to know«, zu vergeben. Die tagtägliche Zugriffsverwaltung erfolgt dann automatisiert.
- Im Rahmen der Umsetzung von Anforderungen an eine ordnungsmäßige Protokollierung von sicherheitsrelevanten Ereignissen, kritischen Zugriffen und sonstigen Aktivitäten ist es an der Fachabteilung, festzulegen, in welchem Umfang die Protokollierung erfolgen soll. Die Protokollierung selbst geschieht durch die jeweiligen IT-Systeme.

Die Entwicklung gesetzlicher Vorgaben zeigt, dass eine klare Trennung der Verantwortlichkeiten nur schwer umzusetzen ist, da der »IT-Anteil« in den Vorgaben stark zugenommen hat. Konnte man in der Vergangenheit deutlich unterscheiden, ob ein Fachbereich oder die IT-Funktion angesprochen wird, ist dies heutzutage nur bedingt möglich. Als Folge dieser Entwicklung kann die IT heute in der Rolle des Dienstleisters für das Unternehmen nicht jede informationstechnische Anforderung hinsichtlich ihres fachlichen Risikos bewerten und damit ihre Erfüllung verantworten. Umgekehrt sind häufig die Fachabteilungen nicht in der Lage, informationstechnische Aspekte in fachlichen Anforderungen korrekt zu identifizieren und an die IT zu kommunizieren, was verstärkt in entsprechenden Verstößen resultiert. In der Praxis führt diese Situation im Rahmen von Prüfungen mitunter zu Aussagen wie »Das ist doch Aufgabe der IT« oder umgekehrt »Das ist Angelegenheit des Fachbereichs, d. h.t die IT keinen Einfluss«. Eine vermittelnde Rolle können bei der notwendigen Klärung die 2nd-Line-Funktionen der IT einnehmen. Wenn diese Funktionen themenspezifische Vorgaben erstellen, so stehen sie auch in der Verantwortung, ihre Einhaltung zu überwachen. Die IT-Compliance-Funktion muss dann dafür Sorge tragen, dass die Anforderungen hinsichtlich Steuerung und Überwachung in den 2nd-Line-Funktionen nachhaltig platziert und Ergebnisse an die IT-Compliance-Funktion berichtet werden. So wird sie in die Lage versetzt, Aussagen zum Status sowohl von IT-Compliance als auch von IT-gestützter Compliance zu treffen.

Erforderlich ist somit eine effektive und effiziente Verantwortungsteilung. Um eine solche zu erreichen, ist es wichtig, zu einem klaren Begriffsverständnis zu gelangen und die grundlegenden Unterschiede zwischen den beiden Interpretationsmöglichkeiten zu erkennen.

IT-Compliance als Compliance der IT-Funktion betrachtet die IT als Träger von Compliance-Anforderungen. Bei dieser Sichtweise stellen sich beispielsweise folgende Fragen (nach [Klotz/Dorn 2008, S. 9f.]):

- Welche Rechtsnormen und ggf. sonstigen Regelwerke sind für die IT-Funktion des Unternehmens relevant?
- Welche IT-Prozesse sind konkret betroffen?
- Welche Compliance-Anforderungen haben die einzelnen Bereiche der IT (Infrastruktur, Datenhaltung, Betrieb, Prozesse etc.) zu erfüllen?
- Welche Risiken resultieren in welcher Höhe aus fehlender oder mangelhafter Compliance der IT?
- Welche technischen, organisatorischen und personellen Maßnahmen sind für die Gewährleistung von IT-Compliance zu ergreifen?

IT-Compliance als IT-gestützte Corporate Compliance bedeutet, dass IT als Mittel zum Erreichen von Compliance genutzt wird. Bei dieser Sichtweise stellen sich beispielsweise folgende Fragen:

- Welche Rechtsnormen mit »IT-Anteil« und ggf. sonstigen Regelwerke sind für das Unternehmen und einzelne Unternehmensbereiche grundsätzlich relevant?
- Welche Geschäftsprozesse sind von Compliance-Anforderungen mit IT-Anteil betroffen?
- Welche Compliance-Anforderungen haben die Geschäftsprozesse konkret zu erfüllen?
- Welche Risiken resultieren in welcher Höhe aus fehlender oder mangelhafter Compliance der Geschäftsprozesse?
- Welche Anforderungen ergeben sich an die IT, damit diese die Erfüllung der Compliance-Anforderungen unterstützen kann?
- Welche technischen, organisatorischen und personellen Maßnahmen sind für die Gewährleistung von Compliance zu ergreifen?

Auch COBIT 2019 unterscheidet zwischen den beiden Sichtweisen. Dies ist zum einen aus der Formulierung des IT-bezogenen Ziels AG01 zu entnehmen, wo zwischen »I&T compliance« und »business compliance« differenziert wird (nach [ISACA 2018a, S. 30]). Zum anderen wird in der Zielbeschreibung von MEA03 die Compliance sowohl von »I&T processes« als auch von »I&T-supported business processes« mit Gesetzen, regulativen Vorgaben und vertraglichen Anforderungen gefordert (nach [ISACA 2018b, S. 285]). Dazu passend wird die Verantwortung für die Identifizierung von Compliance-Anforderungen sowohl der IT (hier dem CIO) als auch den Fachabteilungen (hier den Prozesseignern) zugeordnet (vgl. [ISACA 2018b, S, 287]).

Es ist offensichtlich, dass die verschiedenen Sichtweisen in der Praxis ineinandergreifen und insofern insgesamt notwendig sind, um Compliance im Allgemeinen und IT-Compliance im Speziellen zu erreichen. Teilweise wird diese Integration von den Regelwerken selbst adressiert. Ein gutes Beispiel hierfür sind die vom Bundesministerium für Finanzen (BMF) publizierten »Grundsätze zur ordnungsmäßigen Führung

und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff« (GoBD). Diese konkretisieren die steuerlichen Buchführungs- und Aufzeichnungspflichten aus dem HGB, der AO, dem Einkommenssteuergesetz (EStG) und dem UStG. All diese gesetzlichen Regelwerke richten sich an das betriebliche Steuer- und Rechnungswesen und insofern an eine Fachabteilung »Rechnungswesen/Finanzen«. In den GoBD finden sich jedoch umfangreiche Vorgaben an die IT, die von den Spezialisten der IT-Funktion umzusetzen bzw. mittels Anweisungen an die Anwender vorzugegeben sind. Diese Vorgaben betreffen bzgl. der steuerrelevanten Daten z. B. die Datensicherheit und aufbewahrung, die Datenauslagerung sowie die Gewährleistung der Unveränderbarkeit, der Nachvollziehbarkeit und Nachprüfbarkeit der Daten und Datenflüsse (vgl. [BMF 2019, S. 26ff.]). Die IT hat hierzu viele einzelne Maßnahmen zu ergreifen, die sich z. B. auf Speicher- und Backup-Systeme, das Management von Berechtigungen und Zugriffen, die Historienverwaltung, Verschlüsselungen und Protokollierungen, Archivierung und Wiedergabe u. v. a. m. beziehen. Aus Sicht der GoBD ergreift die IT-Funktion diese Maßnahmen nicht als Selbstzweck, sondern um die Compliance der Fachabteilung mit den informationstechnischen Vorgaben der o. g. Fachgesetze zu Buchhaltung und Steuern zu gewährleisten. Unabhängig von den GoBD wird die IT-Funktion die Maßnahmen durchaus auch aus eigenem Interesse ergreifen, z. B. um damit Vorgaben zur IT-Sicherheit aus der Normenreihe ISO/IEC 27000ff. zu erfüllen. Gerade diese Interdependenzen machen in der Praxis das Verständnis für IT-Compliance schwierig. Hieraus ergeben sich dann schnell auch Unsicherheiten, wo die Verantwortung für IT-Compliance anzusiedeln ist, welche Aufgaben in Zusammenhang mit IT-Compliance auszuführen sind und wer diese sicherzustellen und zu überwachen hat.

2.4 Das IT-Compliance-Risiko

Allgemeine gesetzliche Regelungen, aber vor allem auch branchenspezifische Vorgaben führen in den betroffenen Unternehmen zur Einrichtung von Risikomanagementsystemen, mit deren Hilfe Risiken effektiv und effizient identifiziert, bewertet, gesteuert und überwacht werden sollen. Dies gilt auch für die IT. Ein IT-Risikomanagement richtet sich speziell auf die IT-Risiken des Unternehmens. Diese sind eine Teilmenge der allgemeinen Risiken eines Unternehmens (vgl. [Knoll 2019, S. 14]), zu denen auch das Risiko der Verstöße gegen Vorgaben, also der Non-Compliance, zählt. IT-Compliance-Risiken ergeben sich als Schnittmenge von IT-Risiken einerseits und Risiken aus Non-Compliance andererseits (vgl. Abbildung 2–3).

Wie andere Risiken auch lassen sich IT-Compliance-Risiken formal durch das Produkt aus Eintrittswahrscheinlichkeit und Schadensauswirkung quantifizieren. In Übertragung des allgemeinen Risikobegriffs ergibt sich folgende Definition für das IT-Compliance-Risiko:

Das IT-Compliance-Risiko ist ein Maß für die Möglichkeit, dass aus einem Verstoß gegen an die IT des Unternehmens gerichtete Vorgaben (Non-Compliance) ein Schaden resultiert.

Der zukünftige Verstoß gegen Vorgaben stellt ein Ereignis dar, das einen Tatbestand der Non-Compliance umfasst. Dieser besteht beispielsweise darin, dass die IT nicht wie geplant funktioniert, schlecht organisiert ist, nicht wie erforderlich betrieben und genutzt wird, unzureichend verfügbar oder ungenügend gesichert ist, manipuliert oder missbraucht werden kann. Damit sich das IT-Compliance-Risiko realisiert, muss der Tatbestand der Non-Compliance zudem durch einen Akteur nachweislich festgestellt werden.

COBIT 2019 richtet sich auf IT-bezogene Geschäftsrisiken (und betrachtet damit IT-Risiken in erster Linie aus der Sicht der IT-gestützten Corporate Compliance). Diese bestehen aus IT-bezogenen Ereignissen, die das Geschäft potenziell beeinträchtigen. Das Management von IT-bezogenen Risiken sollte in den Risikomanagementansatz des Unternehmens integriert werden (vgl. [ISACA 2018a, S. 12]).[15] Insbesondere die Risikoanalyse soll auf Risikoszenarien basieren (vgl. [ISACA 2018b, S. 132]), die sich insgesamt 19 Risikokategorien zuordnen lassen. Eine dieser Risikokategorien wird mit »Noncompliance« bezeichnet. Als beispielhafte Risikoszenarien werden genannt (nach [ISACA 2018c, S. 25]):

- 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

[15] Trotzdem verwendet COBIT 2019 auch den Begriff »I&T risk«.

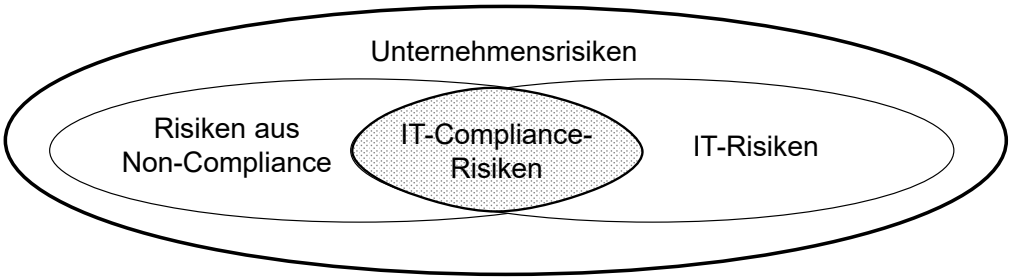


Abb. 2–3: IT-Compliance-Risiken als Schnittmenge (nach [Klotz/Dorn 2008, S. 7])

In der Praxis erweist sich die Frage nach der Verantwortung für IT-Compliance-Risiken als nicht trivial, da die Einhaltung von Einzelanforderungen aus einem Regelwerk im Allgemeinen in dezentraler Verantwortung liegt. Hier kann das Handeln auf der operativen Ebene der Fachabteilungen zu Compliance-Verstößen führen, andererseits kann die IT-Compliance-Funktion durch eine ungenügende Durchführung ihrer Aufgaben, wie z. B. eine ungenügende Einführung und Pflege von Verfahren zur Identifikation und Analyse neuer Gesetze mit IT-Bezug oder die mangelnde Überwachung, IT-Compliance-Risiken verursachen oder beeinflussen. Wird darüber hinaus die IT-gestützte Compliance mitberücksichtigt, so führt dies zu dem Ergebnis, dass die Verantwortung für IT-Compliance-Risiken eine Aufgabe des Gesamtunternehmens darstellt und die betroffenen Organisationseinheiten diejenigen IT-Compliance-Risiken identifizieren sollten, die aus Anforderungen resultieren, für die sie die Verantwortung tragen. Eine pauschale Zuordnung des »einen« IT-Compliance-Risikos (im ganzheitlichen Sinne) wäre kein empfehlenswerter Ansatz.

Die dezentrale Verantwortung für IT-Compliance-Risiken erschwert im Rahmen des Risikomanagements darüber hinaus eine valide Bewertung des Schadensausmaßes. Dennoch muss z. B. die Frage »Wie hoch ist der Schaden, wenn wir gegen die DSGVO verstoßen?« realistisch beantwortet werden können. Dabei auf die in Gesetzen aufgeführten Bußgelder und Strafen oder auf Urteile zu verweisen, kann höchstens einen Pauschalansatz darstellen, der sich jedoch nicht für eine Risikosteuerung, z. B. eine Risikokapitalhinterlegung, eignet. Diese Werte können lediglich als Bewertungsgrundlage dienen. Die in der Praxis bei mittleren und großen Unternehmen bewährte Methodik der Szenarioanalyse stellt einen praktikableren Lösungsansatz dar.[16] Üblicherweise führen die Organisationseinheiten (IT und Fachabteilungen) Risikoanalysen und -bewertungen für die von ihnen identifizierten Risiken durch, wobei auch Compliance-relevante Sachverhalte berücksichtigt werden sollten. Aus diesen Einzelrisiken könnten eine IT-Compliance-Funktion und/oder die Corporate-Compliance-Funktion Risikoszenarien mit dem höchsten Schadensausmaß identifizieren und gemeinsam mit den jeweiligen Fachbereichen, die über eine genaue Kenntnis des Kontrollstatus verfügen, die Szenarien unter Nettorisikobetrachtung, d. h. unter Berücksichtigung von Risikosteuerungsmaßnahmen, bewerten.

Unabhängig von der gewählten Bewertungsmethodik empfiehlt es sich, dass Compliance-Funktionen sowie Fachbereiche die Risikobewertung gemeinsam durchführen, da den Compliance-Funktionen oft die erforderliche Information in Bezug auf den Kontrollstatus fehlt und die Fachbereiche in der Regel nicht das erforderliche Wissen besitzen, um z. B. Rechtsverstöße zu bewerten. Bei IT-gestützten Compliance-Themen ist die Zusammenarbeit ohnehin erforderlich, da im Regelfall weder IT-Compliance-Funktion noch die Corporate-Compliance-Funktion selbstständig Aussagen treffen können.

Die Identifizierung der externen Compliance-Anforderungen ist in COBIT 2019 Inhalt der Managementpraktik MEA03.01. Diese umfasst mit der Bewertung der Folgen von Non-Compliance auch die Abschätzung von IT-Compliance-Risiken. Verantwortlich hierfür sind die IT (hier der CIO) und die Fachabteilungen (hier die Prozesseigner) sowie überwachende Einheiten (Datenschutz, Rechtsabteilung und Revision). Die Gesamtverantwortung liegt bei der Compliance-Funktion (vgl. [ISACA 2018b, S. 285ff.]).

2.5 Integrationsbedarf von IT-Compliance

IT-Compliance ist im Rahmen der Steuerung und Überwachung seit ca. zwölf Jahren im Bewusstsein der IT-Verantwortlichen – und damit in der IT immer noch ein eher junges Handlungsfeld. Für die praktische Ausgestaltung von IT-Compliance wirkt sich dies dahingehend aus, dass es keine gefestigten Standards speziell für IT-Compliance gibt[17], sodass in der Praxis immer noch in hohem Maße unternehmensindividuelle Maßnahmen ergriffen und situative Lösungen für IT-Compliance implementiert werden. Hierbei stellen sich Fragen der notwendigen Integration von Zielen, Prozessen und Verantwortlichkeiten der IT-Compliance.

IT-Compliance und IT-Governance

Auf der Ebene des Gesamtunternehmens ist Compliance im Deutschen Corporate Governance Kodex (DCGK) als Teilverantwortung im Rahmen der Festlegungen zur Corporate Governance ausdrücklich der Unternehmensleitung (Vorstand) zugewiesen [DCGK 2019, Grundsatz 5]. Dies gilt ebenso für IT-Governance als funktionsspezifischer Spezialisierung der Corporate Governance, insbesondere dann, wenn ein Mitglied der Unternehmensleitung als CIO die Verantwortung für die Unternehmens-IT trägt – ggf. sogar verstärkt durch einen Chief Digital Officer (CDO), der für die digitale Transformation zuständig zeichnet (vgl. [Boeselager 2018]). Die Corporate Governance fokussiert vor allem auf wesentliche Stakeholder (nationale und internationale Kapitalgeber, Aufsicht, Öffentlichkeit) und muss insofern die Ordnungsmäßigkeit der Finanzberichterstattung sicherstellen. Hieraus folgt für die IT-Governance bzw. für die IT-Compliance der entsprechende Nachweis hinsichtlich der Entwicklung als auch des Betriebs von rechnungslegungsrelevanten IT-Anwendungen (vgl. [Johannsen/Goeken 2011, S. 17f.]). Dies lässt sich als originäre Aufgabe der IT-Compliance im Rahmen der Corporate Governance bezeichnen. Allgemein richtet sich IT-Governance »auf die Regelung von Verantwortlichkeiten und Entscheidungsrechten sowie von entsprechenden Prozessen und Verfahren mit dem Ziel, aus der IT-Nutzung einen maximalen Wertbeitrag für das Unternehmen zu ziehen. Hierzu gehört auch die Einrichtung eines IT-Kontrollsystems

[16] Für eine Beschreibung der Anwendung der Szenariomethode im Rahmen des IT-Risikomanagements s. [Knoll 2019, S. 209ff.].

[17] Dies zeigt sich z. B. bei einem Vergleich der Aussagen zu IT-Compliance in den drei letzten COBIT-Versionen 4.1, 5 und 2019, der divergierende Prozesspraktiken, -aktivitäten und -verantwortlichkeiten aufzeigt, vgl. [Klotz 2013], [Klotz 2019].

als Bestandteil des unternehmensweiten internen Kontrollsystems (IKS), mit dem die Steuerung und Überwachung der IT im Unternehmen sichergestellt werden soll« [Klotz 2020, S. 854f.]. Dieses IT-Kontrollsystem hat auch die Aufgabe, die Compliance des IT-Einsatzes sicherzustellen.

Für COBIT 2019 als Framework für IT-Governance und IT-Management ist IT-Compliance in den Unternehmens-, den IT-bezogenen Zielen sowie den Governance- und Managementzielen verankert. Und nicht zuletzt bildet COBIT nach wie vor die Blaupause für ein IT-Kontrollsystem.

IT-Compliance und IT-Risikomanagement

Der Zusammenhang zwischen IT-Compliance und IT-Risikomanagement fand in den Publikationen der ISACA bzw. des IT Governance Institute (ITGI) schon früh Berücksichtigung. So steht bereits im ersten Board Briefing zu IT-Governance das Compliance-Risiko neben den Risiken der Sicherheit und Zuverlässigkeit [ITGI 2001, S. 11].

Eine wesentliche Aufgabe im Rahmen des IT-Risikomanagements ist es, den identifizierten IT-Risiken mittels geeigneter Kontrollen zu begegnen. Es gilt, sowohl übergreifende als auch prozess- und transaktionsorientierte Kontrollen in Bezug auf das Umfeld, die Struktur- und Prozessorganisation der IT, die IT-Infrastruktur sowie Daten und Anwendungen (vgl. [IDW RS FAIT 1, Pkt. 9ff.]) zu implementieren. Hierzu sind u. a. als notwendige Maßnahmen IT-Sicherheitskonzepte, Verfahrensanweisungen für IT-Betrieb, (Out-)Sourcing, zum Schutz und zur Sicherung von Datenbeständen, Zugangs- und Zugriffskonzepte, Konzepte für Change- und Notfallmanagement sowie Richtlinien zur Entwicklung und Änderung von Anwendungssoftware zu erstellen (nach [Heese/Fröhlich 2013, S. 558]). Für all diese Regelungen kann auf Normen und Standards zurückgegriffen werden. Welche Regelwerke existieren und inwieweit diese verfügbar und sinnvoll anwendbar sind, ist durch die IT-Compliance zu klären.

Der enge Zusammenhang zwischen IT-Compliance und IT-Risikomanagement zeigt sich in COBIT 2019 darin, dass diejenigen Governance- und Managementziele, die die Erreichung der beiden Compliance-bezogenen IT-Ziele unterstützen, auch beim Erreichen des IT-bezogenen Ziels AG02 »Managed IT-related risk« helfen. Umgekehrt trifft dies auch für die Mehrzahl der Governance- und Managementziele zu, die die Erreichung des IT-bezogenen Ziels AG02 unterstützen (vgl. [ISACA 2018b, S. 298]).

IT-GRC

Governance, Risikomanagement und Compliance verweisen somit aufeinander. Aufgrund der inhaltlichen Zusammenhänge wird häufig von der Trias »Governance–Risk–Compliance« (GRC) gesprochen, die eine integrierte Strategie und ein gemeinsames Management erfordert. Im Ergebnis erfährt die GRC-Trias eine Spezialisierung im IT-Bereich, was zu vielfältigen Koordinationsnotwendigkeiten führt. So muss jede Spezialisierung sich in den jeweiligen generellen Bereich eingliedern, also z. B. die IT-Compliance in die generellen Compliance-Aktivitäten des Unternehmens, sie muss aber auch mit den anderen Spezialisierungen abgestimmt werden, beispielsweise IT-Compliance mit IT-Governance und IT-Risikomanagement (s. Abbildung 2–4).

Für COBIT 2019 greift der GRC-Ansatz zu kurz, da der Eindruck entstehen könnte, dass IT-Governance nur IT-Compliance und IT-Risikomanagement umfasst (vgl. [ISACA 2018a, S. 12]).

IT-Compliance und IT-Sicherheitsmanagement

Eine in der Praxis höchst relevante enge Verbindung besteht zwischen IT-Compliance und IT-Sicherheitsmanagement. Dies liegt daran, dass in der IT-Sicherheit der Nachweis eines etablierten IT-Sicherheitsmanagementsystems eine wichtige Rolle spielt. Ein Beispiel hierfür sind die von der BaFin publizierten MaRisk (Mindestanforderungen an das Risikomanagement). Die zugehörige Erläuterung verweist sowohl auf die vom BSI herausgegebenen IT-Grundschutzkataloge als auch auf die ISO/IEC-27000-Reihe (vgl. [BaFin 2017a, S. 28)]. Auch in der Umsetzung der Anforderungen des IT-Sicherheitsgesetzes spielen Normen, wie die DIN EN ISO/IEC 27001, oder Standards, wie die BSI-Standards zum Informa-

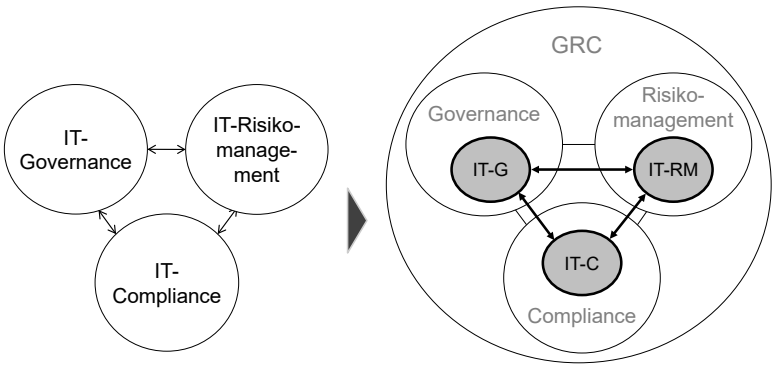


Abb. 2–4: Abstimmungsbedarf von IT-GRC (nach [Klotz 2009, S. 11])

tionssicherheitsmanagementsystem, als Basis der Entwicklung branchenspezifischer Sicherheitsstandards eine zentrale Rolle. Dies zeigt sich beispielsweise am »Branchenspezifischen Sicherheitsstandard zur IT-Sicherheit – UP KRITIS - BAK Datacenter & Hosting mit CDN«. Dieser orientiert sich ausdrücklich an der Normenreihe ISO/IEC 2700x (speziell 27001, 27002, 27005, 27006, 27007, 27032, 27035) und der Norm ISO/IEC 22310 zum Business Continuity Management (BCM). Weiterhin werden die BSI-Standards 100-4 und 200-1 bis -3, die ISO 55000 und die ISO/IEC 38500 referenziert [UP KRITIS 2018, S. 40f.]. Zudem ist die Compliance mit Normen und Standards des IT-Sicherheitsmanagements häufig ein wichtiges Vertriebsargument für IT-Dienstleister bzw. wird von deren Kunden als Voraussetzung einer Geschäftsbeziehung gefordert.

Der enge Zusammenhang zwischen IT-Compliance und IT-Sicherheitsmanagement zeigt sich in COBIT 2019 ebenfalls darin, dass diejenigen Governance- und Managementziele, die die Erreichung der beiden Compliance-bezogenen IT-Ziele unterstützen, auch die Erreichung des IT-bezogenen Ziels AG07 »Security of information processing, infrastructure and applications, and privacy« unterstützen. Umgekehrt trifft dies auch für die Mehrzahl der Governance- und Managementziele zu, die die Erreichung des IT-bezogenen Ziels AG07 unterstützen (vgl. [ISACA 2018b, S. 298]).

2.6 Handlungsfelder von IT-Compliance

IT-Compliance ist kein Zustand, der einmal erreicht und dann über längere Zeit hin oder gar unbegrenzt gegeben ist. Wesentlicher Treiber für Anpassungsmaßnahmen in Bezug auf IT-Compliance ist neben der Gesetzgebung, dem räumlichen Ausmaß der Geschäftstätigkeit und dem Marktdruck vor allem die technologische Entwicklung. Neue Informationstechnologien haben immer auch eine Compliance-Dimension, die es zu identifizieren und zu analysieren gilt und die ggf. Compliance-Maßnahmen erfordert. Die IT-Compliance-Funktion steht hierbei vor der Herausforderung alle diese Neuerungen und Anforderungen in ihr Scoping aufzunehmen und Transparenz bzw. Übersicht zu schaffen, um Compliance je Themengebiet bzw. Handlungsfeld zu fördern. Zur Verdeutlichung dieser Herausforderung sollen folgende Beispiele dienen:

- **Lizenzmanagement:** Auswahl und Beschaffung von Software erfolgt häufig bedarfsgerecht und mitunter auch dezentral, sodass es für Unternehmen schwer ist, den Überblick über die erworbenen Lizenzen zu behalten. *Überlizenzierung* bedeutet einen Kostennachteil, Unterlizenzierung führt zu rechtlichen Problemen. Ein effektives Lizenzmanagements hat also sicherzustellen, dass Software einerseits entsprechend dem realen Bedarf beschafft, andererseits gemäß der abgeschlossenen Lizenzverträge genutzt wird, um Lizenzverstöße sowie daraus resultierende Unterlassungs- oder Schadensersatzansprüche nach UrhG zu vermeiden (vgl. [Jacobs 2017, S. 696f.]). Hierzu ist es z. B. erforderlich, Lizenzrisiken zu identifizieren und entsprechende Maßnahmen aufzusetzen, den Bestand an Lizenzen zu pflegen und den Einsatz der lizenzierten Software zu überwachen. Typische Lizenzrisiken sind beispielsweise der Erwerb falscher Lizenzen (d. h. eines falschen Lizenztyps), die fehlerhafte Nutzung von Open-Source-Komponenten oder die ungeprüfte Einbindung von fremdem Programmcode.
- **GoBD-Anforderungen:** Die bereits erwähnten GoBD stellen zwar grundsätzlich kein »Gesetz« dar, das verpflichtend einzuhalten ist. Da es aber die Grundlage der Auslegung der Ordnungsmäßigkeitsanforderungen bei IT-gestützter Rechnungslegung beinhaltet, die die Finanzverwaltung bei der Beurteilung heranzieht, ist die Kenntnis und Einhaltung anzuraten. Für die IT stehen beispielsweise die folgenden Themen im Fokus: Identifikation der relevanten Haupt-, Vor- und Nebensysteme, Anforderungen an Verfahrensdokumentation, internes Kontrollsystem (u. a. Kontrollen der Applikationen), Aufbewahrung, Anforderungen an das Scannen, Datensicherheit, Protokollierung von Änderungen, Nachvollziehbarkeit von Geschäftsvorfällen bzw. Buchungen, Anforderungen an die Auslagerung von Systemen sowie Datenzugriff für die Finanzverwaltung. Die GoBD werden kontinuierlich im Rahmen von Urteilen ausgelegt. Unternehmen sind damit gut beraten, dementsprechende Entwicklungen zu verfolgen.
- **Bring your own device (BYOD) im Rahmen der Informationssicherheit:** Hinter dem Konzept »BYOD« verbirgt sich die Strategie von Unternehmen, den Mitarbeitern die Nutzung privater Geräte für dienstliche Zwecke zu erlauben (z. B. für das Lesen oder Bearbeiten dienstlicher E-Mails). Bei all den Vorteilen von BYOD – vor allem Motivationssteigerung und Kosteneinsparung – sind die Risiken der Informationssicherheit und des Datenschutzes nicht zu vernachlässigen. Das betrifft vor allem Risiken in Verbindung mit der ordnungsmäßigen Absicherung und dem Update der Geräte. Es bedarf klarer Rahmenbedingungen, durch die vorgegeben wird, welche Gerätetypen und Apps eingesetzt werden dürfen bzw. müssen, um Informationen und sensible Daten zu schützen. Hinsichtlich der Nutzung sind verbindliche Regelungen zu treffen, z. B. zu Nutzungszeiten und umgebung. Darüber hinaus sind Mindestkonfigurationen festzulegen und es ist sicherzustellen, dass die Mitarbeiter wissen, wie bei Sicherheitsvorfällen zu reagieren ist. Aus Compliance-Sicht ist es wichtig, bereits bei der Planungsphase zu berücksichtigen, welche rechtlichen Anforderungen und Sorgfaltspflichten mit BYOD verknüpft sind, z. B. hinsichtlich Urheberrechten, Datenschutz, steuerlichen Fragen, Aufbewahrungspflichten und Beteiligungsrechten der Arbeitsnehmervertretung.[18] Im Ergebnis werden eine Betriebsvereinbarung und eine Richtlinie die BYOD-Nutzung regeln müssen – und auch wieder Gegenstand von IT-Compliance sein.

[18] Vgl. die Regelungsbereiche in [Gruber et al. 2013, S. 16].

- **3D-Druck:** Der 3D-Druck ist eine Technologie, mit deren Hilfe Gegenstände im Schichtverfahren dreidimensional gedruckt werden können. Sie ermöglicht eine effiziente Kleinserien-Produktion, bis hin zur Losgröße 1. Zudem kann das *für den Druck erforderliche* CAD-Modell als Datei an jeden Ort gesendet werden, an dem ein adäquater 3D-Drucker zur Verfügung steht. Hieraus resultieren Anwendungspotenziale für das Customizing von Produkten, für Service und Wartung sowie für die Teilelogistik. Diese Potenziale sind verbunden mit vielfältigen rechtlichen Fragen zu Patenten, Gebrauchs- und Geschmacksmustern, zu Design-, Urheber- und Wettbewerbsrechten. Unternehmen müssen einerseits die Durchsetzung ihrer eigenen Rechte sicherstellen, andererseits als Anwender des 3D-Drucks aber auch Rechte Dritter nachweislich beachten.
- **IT-Outsourcing:** Die vertraglich vereinbarte Verlagerung von IT-Aufgaben oder IT-Prozessen an externe Dienstleister entbindet Unternehmen nicht von der Verantwortung, sicherzustellen, dass gesetzliche und aufsichtsrechtliche Vorgaben oder interne Standards eingehalten werden. Unzureichende Vorgaben hinsichtlich Vertragsgestaltung und Dienstleistersteuerung im Rahmen von IT-Outsourcing erhöhen das Compliance-Risiko. Eine enge Verzahnung zwischen dem externen IT-Dienstleister und der internen IT-Compliance sollte sicherstellen, dass nicht nur eine Überwachung der Einhaltung der vertraglichen Verpflichtungen stattfindet, sondern auch aus gesetzlichen oder regulatorischen Änderungen sowie aktueller Rechtsprechung resultierende Anforderungen vom Dienstleister umgesetzt und eingehalten werden.
- **Cloud Computing:** So sehr Cloud-Dienste die Flexibilität eines Unternehmens im Hinblick auf die Rechenzentrumsinfrastruktur vergrößern, so sehr bietet diese Flexibilität auch Risiken. Wenn persönliche Daten bei einem Cloud-Anbieter gespeichert werden, ist mit diesem eine Vereinbarung zur Auftragsdatenverarbeitung abzuschließen. Die Beauftragung von Unterauftragnehmern wird in Art. 28 DSGVO an strenge Vorgaben geknüpft. Viele Vereinbarungen haben bereits derartige Regelungen vorgesehen; eine Prüfung im Detail ist jedoch gerade auch in diesen Fällen erforderlich. Der Auftragnehmer hat den Auftraggeber bei der Erfüllung seiner Rechte zu unterstützen. Dieser gesetzlichen Anforderung ist durch die Vertragsgestaltung Rechnung zu tragen. So muss beispielsweise sichergestellt sein, dass personenbezogene Daten die EU nicht verlassen. Einige Anbieter garantieren dies; andere Anbieter betreiben ihre Rechenzentren ohnehin nur auf dem Gebiet der EU. Dass sich dies ändern kann, zeigt der Brexit, der aktuell dazu Anlass gibt, bestehende Verträge hinsichtlich ihrer Brexit-Folgen zu hinterfragen. Die Vertragsgestaltung ist auch aus Sicht der Aufsicht wesentlich, müssen in den Verträgen doch die aufsichtsrechtlich relevanten Vorgaben berücksichtigt werden. Um dies z. B. für Finanzdienstleistungsinstitute sicherzustellen, hat die BaFin eine »Orientierungshilfe zu Auslagerungen an Cloud-Anbieter« publiziert. Deren Ziel ist es insbesondere, »für die beaufsichtigten Unternehmen ein Problembewusstsein im Umgang mit Cloud-Diensten und den damit verbundenen aufsichtsrechtlichen Anforderungen zu schaffen« [BaFin 2018b, S. 3].

Während die eben aufgezählten Handlungsfelder bereits in den meisten Unternehmen im Fokus stehen, sollen die folgenden Beispiele aufzeigen, mit welchen Themenfeldern sich die IT-Compliance zukünftig befassen muss:

- **Blockchain:** Der Anwendungsbereich der Blockchain-Technologie[19] reicht weit über die sogenannten Kryptowährungen hinaus. Dieses Potenzial liegt vor allem in der Verifizierung der Echtheit von Daten und kann damit überall dort sinnvoll eingesetzt werden, wo es gilt, Transaktionen von Daten richtig und regelkonform sicherzustellen bzw. eine dezentrale Datenhaltung lückenlos und nachvollziehbar zu protokollieren. Blockchain kann also dem Zweck dienen, Datenhaltung und transfer sicherer zu machen, um dolose Handlungen bzw. Fraud zu verhindern bzw. zu erschweren. Auf IT-Compliance bezogen bedeutet dies, dass zukünftig die Technologie »Blockchain« Gegenstand von IT-Compliance sein wird, z. B. wenn unterschiedliche Akteure (Hersteller, Lieferanten, Nutzer etc.) die Blockchain-Technologie für Transaktionen oder Tracking-Prozesse entlang einer gemeinsamen Wertschöpfungskette nutzen. Hierfür wäre eine vertragliche Grundlage zu schaffen, bei der auch Datenschutz- oder Kartellrecht zu berücksichtigen wären (nach [Süme/Sens 2001, S. 23ff.]).
- **Künstliche Intelligenz (KI):** Die von der Europäischen Kommission eingesetzte »Unabhängige hochrangige Expertengruppe für Künstliche Intelligenz« hat bereits 2018 Anforderungen an eine vertrauenswürdige KI formuliert. Danach muss sich eine vertrauenswürdige KI durch drei Komponenten auszeichnen. Erstens soll sie robust sein, sowohl in technischer als auch in sozialer Hinsicht, damit kein unbeabsichtigter Schaden verursacht wird. Zweitens soll sie die Einhaltung ethischer Grundsätze und Werte garantieren und drittens rechtmäßig sein, also geltendes Recht und alle gesetzlichen Bestimmungen einhalten (nach [HEG-KI 2018, S. 6]). Anders ausgedrückt soll die Technologie compliant sein und Ergebnisse generieren, die compliant sind. Dies dürfte jedoch nicht so leicht umzusetzen sein. Nicht zuletzt stellt sich gerade bei autonomen Systemen die Frage der Zuordnung von Haftung zwischen Hersteller, Anbieter und Nutzer. Es ist absehbar, dass bei verstärktem KI-Einsatz im Unternehmensumfeld zukünftig immer mehr Entscheidungen, aber auch Kontrollen von autonomen KI-Systemen getroffen werden. Für die IT-Compliance ergibt sich hierbei das Potenzial für eine Effizienzsteigerung durch eine qualitativ hochwertige Automatisierung von Überwachungsmaßnahmen, z. B. bei einer vorgelagerten, KI-basierten Verbesserung von Detection-Modellen. Die erhoffte Wirkung besteht in einer Erhöhung der Aufdeckungsrate von Betrugsfäl-

[19] Einen umfassenden Einblick in Governance- und Compliance-Aspekte der Blockchain-Technologie bietet die Ausgabe Nr. 30 der Zeitschrift »IT-Governance« vom Dezember 2019.

len bzw. einer aktiven Verhinderung von Verstößen gegen rechtliche Vorgaben (nach [Deloitte 2019, S. 17]).

Die Bandbreite der Beispiele zeigt deutlich, dass das Bemühen um Compliance eine kontinuierliche und umfangreiche Herausforderung darstellt. Um diese zu bestehen, hat sich in der Praxis die Identifizierung und Priorisierung von Handlungsfeldern bewährt. Die IT-Compliance-Funktion hat hierbei sicherzustellen, dass für die identifizierten Handlungsfelder die spezifischen Vorgaben aus Gesetzen, Regulatorik, Standards und Normen Berücksichtigung finden und effektive und effiziente Prozesse des Compliance-Managements etabliert werden, die die Implementierung von Maßnahmen und die damit verbundene Berichterstattung gewährleisten.

Für die Identifizierung der Handlungsfelder (die Summe der Handlungsfelder bildet das »IT Compliance Universe«) gibt es verschiedene Verfahren:

- Ein Unternehmen analysiert sein Normenregister und bildet thematisch zusammenhängende Cluster, aus denen es Handlungsfelder identifiziert.
- Aus den Anforderungen der Stakeholder lassen sich Handlungsfelder ableiten und priorisieren, sodass die IT-Compliance-Funktion ihre Maßnahmen fokussieren kann.
- Die Handlungsfelder werden systematisch aus IT-Trends und neuen Technologien abgeleitet (diesen Weg sieht COBIT 2019 in APO04 vor).

Sind die Handlungsfelder definiert, gilt es auch die Akteure zu identifizieren, die im jeweiligen Handlungsfeld verantwortlich zeichnen.

In COBIT 2019 beinhaltet das IT-Managementziel APO04 (Managed Innovation) Praktiken für eine systematische Suche nach IT-Innovationen. In APO04.03 (Monitor and scan the technology environment) wird ein Prozess zur systematischen Analyse der externen Umgebung des Unternehmens gefordert, um neue Technologien mit Wertschöpfungspotenzial zu identifizieren. Für die identifizierten Technologien ist eine Potenzialanalyse durchzuführen. Diese ist Inhalt der Managementpraktik APO04.04 (Assess the potential of emerging technologies and innovative ideas). Gleich die erste Aktivität dieser Praktik richtet sich auf die Bewertung der identifizierten innovativen Technologien, wobei u. a. potenzielle rechtliche Auswirkungen als inhärentes Risiko zu berücksichtigen sind (vgl. [ISACA 2018b, S. 82]).

Handlungsempfehlungen

- Klären Sie, welche Treiber von IT-Compliance für Ihr Unternehmen relevant sind.
- Verdeutlichen Sie den Handlungsbedarf für IT-Compliance anhand bekannt gewordener Fälle von Non-Compliance.
- Klären Sie, was IT-Compliance für Ihr Unternehmen bedeutet. Der Zusammenhang zwischen IT-Compliance und IT-gestützter Compliance kann dazu dienen, unterschiedliche Auffassungen und kritische Schnittstellen zu identifizieren.
- Betrachten Sie IT-Compliance-Risiken als spezifische IT-Risiken.
- Ergreifen Sie vor allem automatisierte und präventive Überwachungsmaßnahmen, um Non-Compliance zu vermeiden.
- Klären Sie den Zusammenhang zwischen IT-Compliance und Corporate Compliance.
- Klären Sie den Zusammenhang zwischen IT-Compliance und IT-Governance und IT-Risikomanagement.
- Identifizieren Sie die prioritären aktuellen und künftigen Handlungsfelder der IT-Compliance.

3 Der Nutzen von IT-Compliance

3.1 Nutzen von IT-Compliance aus Sicht des Unternehmens

Neben der Pflicht zur Erfüllung gesetzlicher Vorschriften soll IT-Compliance ein Unternehmen vor allem vor rechtlichen und wirtschaftlichen Nachteilen als Folge von Verstößen gegen gesetzliche oder regulatorische Vorgaben bewahren. Hierdurch sollen insbesondere behördliche Eingriffe in den Geschäftsbetrieb (bis hin zum Verbot der Gewerbeausübung), mögliche Zwangsmaßnahmen, Schadensersatzpflichten, Strafen, Buß- und Zwangsgelder oder auch erhöhte Steuerzahlungen aufgrund von Schätzungen des Finanzamts vermieden werden. Verstöße gegen Datenschutz oder IT-Sicherheit sind durch die Gesetzgebung mit massiven Strafandrohungen bewehrt, die über den Rahmen einfacher operationeller Zusatzkosten hinausgehen und ggf. Bilanzrisiken für das Unternehmen darstellen können. In stark regulierten Branchen ist die Compliance mit Vorgaben der Aufsichtsbehörden von essenzieller Bedeutung, da bei schweren Verstößen in letzter Konsequenz sogar die Fortführung des Geschäftsbetriebs auf dem Spiel steht, z. B. für Kreditinstitute und Versicherungen nach §§ 32, 33 Kreditwesengesetz (KWG) in Verbindung mit Artikel 4 Abs. 1 der SSM-Verordnung[1] bzw. § 11 VAG. Branchenunabhängig resultieren künftig aus dem »Gesetz zur Sanktionierung von verbandsbezogenen Straftaten« (Verbandssanktionengesetz – VerSanG) ggf. hohe Bußgelder. Eine Verstärkung der Compliance-Maßnahmen in Unternehmen ist ein ausdrückliches Ziel dieser Gesetzgebung zum Unternehmensstrafrecht. Die Regelung, dass Compliance-Maßnahmen Auswirkungen auf die Höhe der Sanktion haben, wird die adäquate Ausgestaltung von Compliance-Management-Systemen wesentlich vorantreiben.

Ein Schaden kann aber auch dann entstehen, wenn ein Unternehmen im Rahmen einer gerichtlichen Auseinandersetzung beweiserhebliche Daten und Dokumente aufgrund eines unzureichenden Daten- und Dokumentenmanagements nicht vorlegen und damit seiner Beweispflicht nicht nachkommen kann. Dies kann viele Bereiche des Unternehmens betreffen, z. B. F&E, Produktion, Umweltmanagement oder Arbeitsschutz. Wird z. B. im Zusammenhang mit steuerrelevanten Unterlagen gegen Archivierungspflichten verstoßen, drohen steuerliche Nachteile. Die Pflicht zur Archivierung besteht insbesondere auch für die Verfahrensdokumentation nach GoBD, die den Inhalt, Aufbau, Ablauf und die Ergebnisse steuerrelevanter DV-Verfahren umfasst (siehe [BMF 2019, Rz. 151ff.]). Weitere monetäre Nachteile von Non-Compliance können ggf. der Verlust von Schadenersatzansprüchen oder eines Versicherungsschutzes sein (vgl. [Stögmöller 2019, S. 28]).

Zusätzlich zu monetären Schäden ist ein potenzieller Imageschaden von Bedeutung, der wiederum häufig zu einem monetären Schaden führt. Dies ist in der IT beispielsweise der Fall, wenn gegen Datenschutznormen verstoßen wird oder Kundendaten abhandenkommen oder missbraucht werden. Folgen sind neben einer negativen Publizität ggf. auch Nachteile bei der Vergabe öffentlicher Aufträge oder gar Kunden-

[1] Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank.

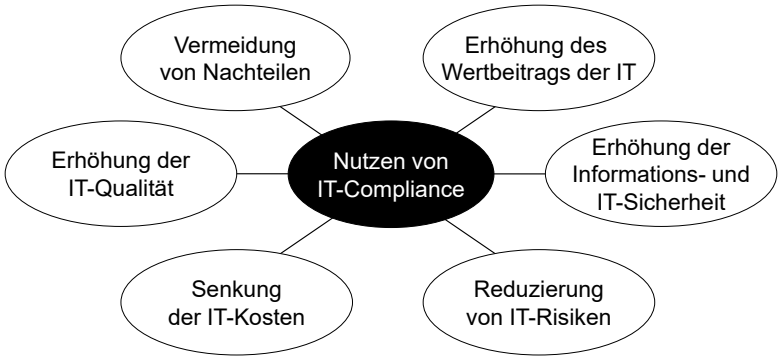


Abb. 3–1: Nutzendimensionen von IT-Compliance

abwanderungen, was in beiden Fällen zu Umsatzverlusten oder im schlimmsten Fall zur Geschäftsaufgabe führen kann. Im Falle von Unternehmen, die ihren Kapitalbedarf über den Kapitalmarkt decken, können sich zudem monetäre Rückwirkungen ergeben, wenn der Aktienkurs oder das Kreditrating negativ beeinflusst werden.

Neben der Schutzfunktion, die auf die Vermeidung von Nachteilen zielt, ist IT-Compliance mit Vorteilen verbunden (vgl. Abbildung 3–1) (vgl. [Böhm 2008, S. 26f.]).

- **Wertbeitrag:** Wenn die IT eines Unternehmens ihre Compliance nachweisen kann, führt dies auf vielfältigen Wegen zu einer Erhöhung des Unternehmenswertes. Erweisen sich bestimmte Standards (z. B. IT-Sicherheitszertifikate) als Markteintrittsbarrieren, ist der Wertbeitrag offensichtlich. Ohne die Konformität zu derartigen externen Vorgaben könnten Umsatzchancen nicht genutzt werden. Dies spielt vor allem bei IT-Dienstleistungsverhältnissen eine große Rolle. Hier geht es bei Prüfungen nach IDW PS 951 oder ISA 3401 um Compliance-Reporte, mit denen die Einhaltung regulatorischer und IKS-Anforderungen nachgewiesen werden soll und ohne deren Vorliegen eine Geschäftsbeziehung nicht zustande kommt. Auch die Realisierung von Wertbeiträgen aus der Nutzung moderner Technologien ist ohne den Nachweis der Einhaltung von Compliance-Anforderungen nicht denkbar. Dies gilt z. B. auch für die Nutzung der Blockchain-Technologie als Gegenstand der Jahresabschlussprüfung bzw. bei Prüfungen, die das Vertrauen der Blockchain-Teilnehmer fördern sollen (vgl. und vertiefend hierzu [Fröhlich 2019]). Andererseits kann mangelnde IT-Compliance zu Abschlägen bei der Bestimmung des Unternehmenswertes im Falle von Unternehmenstransaktionen führen, wenn sich während einer Compliance Due Diligence (CDD) Risiken in Bezug auf IT-Compliance offenbaren. Gerade der Datenschutz rückt immer mehr in das Blickfeld von CDD-Prüfungen. Entdeckte Compliance-Risiken führen neben Kaufpreisreduzierungen häufig zu Freistellungspflichten oder zur Verpflichtung zu einer Durchführung zusätzlicher Compliance-Maßnahmen, die wiederum entsprechende Kosten verursachen (nach [Langenbucher et al. 2019, S. 6ff.]). Allgemein ergibt sich der Wertbetrag der IT-Compliance dadurch, dass kein nicht qualifiziertes IT-Compliance-Risiko besteht und somit keine negativen Auswirkungen auf den Wert des Unternehmens zu erwarten sind.
- **IT-Qualität:** Viele Maßnahmen zur Herstellung von IT-Compliance tragen zu einer höheren Qualität von IT-Services und IT-Prozessen bei. Dies ist insbesondere dann der Fall, wenn IT-Compliance-Anforderungen und Kontrollen als Elemente des IKS systematisch aufeinander abgestimmt werden. Hieraus resultiert eine höhere Transparenz, die die gesamte IT-Architektur umfasst und letztlich ein effektives Enterprise Architecture Management unterstützt. Eine in diesem Sinne verbesserte Qualität führt zu einer verbesserten Steuerungsfähigkeit, aber auch Auditierbarkeit der IT.
- **Informations- und IT-Sicherheit:** Methoden und Verfahren der IT-Compliance adressieren zu einem hohen Anteil die Informationssicherheitsziele der Vertraulichkeit, Verfügbarkeit und Integrität (vgl. [BSI 2017, S. 14]). Hieraus resultieren Synergiepotenziale, die bei einer abgestimmten Vorgehensweise realisiert werden können. Auf diese Weise entfaltet IT-Compliance zusätzliche Nutzenpotenziale für die operationelle IT-Sicherheit. Dies zeigt sich beispielsweise in der DIN EN ISO/IEC 27002, in der rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen eine der Hauptquellen von Anforderungen an die Informationssicherheit darstellen (vgl. [DIN EN ISO/IEC 27002:2017, S. 9]) und demgemäß Maßnahmen der IT-Compliance in einem Unterkapitel behandelt werden (vgl. [DIN EN ISO/IEC 27002:2017, S. 101ff.]).
- **IT-Risiken:** Wie bereits erwähnt, stellen IT-Compliance-Risiken eine Teilmenge der IT-Risiken dar. Hieraus ergeben sich Synergiepotenziale für das Management von IT-Risiken und IT-Compliance. Einerseits beeinflusst das IT-Risikobewusstsein auch das Bewusstsein für IT-Compliance. Ein gutes Beispiel hierfür ist das Wissen um die hohen Bußgelder der DSGVO, das in vielen Unternehmen der Compliance mit datenschutzrechtlichen Vorgaben einen wesentlich höheren Stellenwert verschafft hat. Die Bewertung von IT-Risiken im Rahmen des IT-Risikomanagements hilft der IT-Compliance, sich auf wesentliche und hohe IT-Compliance-Risiken zu konzentrieren. Andererseits schützt »gute« IT-Compliance auch vor IT-Risiken (nach [Knoll 2019, S. 240]). Dies ist überall dort gegeben, wo durch die Konformität mit IT-Standards und -Normen das Management von IT-Risiken unterstützt wird. Bei COBIT 2019 wird dieser Nutzen deutlich.

COBIT 2019 stellt ein IT-Governance-Modell zur Verfügung, das auch das Management von IT-Risiken unterstützt. Konkret erfolgt dies durch die beiden expliziten IT-Governance- und IT-Managementzielsetzungen EDM03 »Risikooptimierung ist sichergestellt« und APO12 »Risiko ist gemanagt« mit insgesamt neun Praktiken und 36 Aktivitäten. IT-Risiken werden aber noch von weiteren Prozesspraktiken adressiert: IT-Projekt- und IT-Programmrisiken von BAI01.08 und BAI11.06, Risiken aus der Zusammenarbeit mit IT-Lieferanten von APO10.04 und Anforderungsrisiken bei der Softwareentwicklung und -auswahl von BAI02.03. Zudem ist es mittels des Designfaktors (»Design Factor«) »Risikoprofil« möglich, für IT-Risikomanagement relevante IT-Governance- und IT-Managementzielsetzungen anhand von IT-Risikokategorien und IT-Risikoszenarien zu identifizieren und damit entsprechende Handlungsoptionen für das IT-Risikomanagement zu erhalten (vgl. [Gaulke 2020, S. 224ff.] und [ISACA 2018b, S, 41f, 131-134]).

- **IT-Kosten:** Die verschiedenen Maßnahmen zur Sicherstellung der IT-Compliance verursachen i. d. R. Kosten. Da die Maßnahmen aber auch aus Gründen der Risikoreduzierung (Substanzsicherung) und der Erhöhung der operationellen IT-Sicherheit erfolgen, lassen sich die damit verbundenen Kosten oft nicht eindeutig der IT-Compliance zurechnen. Dies gilt auch umgekehrt für die Kosteneinsparungen, die sich u. a. aus der Automatisierung manueller Arbeitsabläufe (bspw. bei der Überwachung oder im Reporting), geringeren Kosten in der IT-Administration und -Wartung oder bei der Durchführung von Prüfungshandlungen ergeben. Der ROI von Maßnahmen der IT-Compliance kann – wenn überhaupt – nur in einem größeren Zusammenhang ermittelt werden. Trotzdem gilt, dass IT-Compliance zwar Investitionen erfordert, aber auch zur Reduzierung von IT-Kosten beiträgt. Diese Kostenreduktion wird insbesondere dann offensichtlich, wenn der Beweis angetreten werden muss, dass durch eine Schwachstelle kein Schaden entstanden ist. Beispiele hierfür sind der Nachweis der Vollständigkeit von Daten und Dokumentationen oder der Nachweis, dass Zugriffrechte nicht missbräuchlich genutzt wurden.

Die verschiedenen Nutzendimensionen realisieren sich in der Praxis nicht unabhängig voneinander. Werden Compliance-Anforderungen von Beginn an beim Design von IT-Prozessen oder der Entwicklung von IT-Services berücksichtigt, so erhöht dies die Qualität und ggf. auch die Sicherheit der betreffenden Prozesse und Services. Hierdurch können gleichzeitig höhere Kosten vermieden werden, die sich ergeben, wenn bestehende IT-Prozesse und -Services nicht compliant sind und deswegen geändert werden müssten. Gerade dann, wenn derartige Änderungen zu hohen Anpassungskosten führen, steht IT-Compliance häufig in der Kritik. Ein frühzeitig einsetzendes IT-Compliance-Management kann somit Auseinandersetzungen um vermeintlich »zu teure« Compliance vermeiden und seinen Nutzen entfalten.

Für COBIT 2019 besteht der Nutzen von IT-Compliance ganz überwiegend in der Vermeidung von Nachteilen. Diese kommen in den verschiedenen Zielmetriken zum Ausdruck. Danach zeigt sich der Nutzen von IT-Compliance in der Vermeidung von Kosten, z. B. in Form von Bußgeldern oder Vergleichszahlungen. Nicht monetäre Nachteile sind Reputationsverluste in der Öffentlichkeit infolge bekannt gewordener Non-Compliance, aber auch bei Regulierungs- oder Aufsichtsbehörden, wenn diese Verstöße festgestellt haben. Wenn das Unternehmen gegen vertragliche Vereinbarungen verstoßen hat, können sich auf der Seite der Geschäftspartner sowohl Reputationsverluste als auch ein monetärer Schaden ergeben (vgl. [ISACA 2018a, S. 30ff.]).

3.2 Nutzen von IT-Compliance aus Sicht der Unternehmensleitung

Die Unternehmensleitung trägt die Verantwortung für die Sicherstellung von Compliance (vgl. [DCGK 2019, Grundsatz 5]). Wird sie dieser Verantwortung gerecht, bewahrt sie das Unternehmen vor Schäden. Werden jedoch, z. B. im Bereich der Informationssicherheit, keine ausreichenden Maßnahmen zum Schutz der Informationswerte ergriffen und dadurch Dritte geschädigt, so können aus einem Organisationsverschulden heraus Unterlassungs- und Schadensersatzansprüche gegen das Unternehmen geltend gemacht werden (nach [Stögmöller 2019, S. 27]). Aus Sicht des einzelnen Mitglieds der Unternehmensleitung kann sich hieraus eine persönliche Haftung ergeben, wenn den Organen des Unternehmens eine schuldhafte Verletzung von Sorgfaltspflichten nachgewiesen werden kann. Weitere Folgen können die Verweigerung der Entlastung, eine Abberufung bzw. eine außerordentliche fristlose Kündigung sein.

Im Falle von Non-Compliance kommt es nicht darauf an, ob die Pflichtverletzung einem einzelnen Mitglied der Unternehmensleitung zugerechnet werden kann. Aufgrund der gesamtheitlichen Verantwortlichkeit nach § 93, Absatz 2 AktG und § 43 Absatz 2 GmbHG haftet jedes Mitglied eines Vorstands oder einer Geschäftsführung gesamtschuldnerisch und damit auch für Pflichtverletzungen der jeweils anderen Mitglieder des Leitungsgremiums. Es ist möglich, dass sich Mitglieder der Unternehmensleitung mittels einer D&O-Versicherung gegen persönliche Haftungsrisiken versichern. Es stellt sich jedoch immer die Frage, ob die Grenzen zur Fährlässigkeit überschritten und der Versicherungsschutz damit hinfällig ist. Ein bewusster Verstoß gegen Gesetze oder ein nachweisbares Versäumnis hinsichtlich üblicher interner Kontroll- und Überwachungsmaßnahmen dürfte mit recht hoher Wahrscheinlichkeit als grob fahrlässig angesehen werden, sodass eine Haftbarkeit gegeben sein kann.

Verschärft wird die Haftungssituation für Mitglieder der Unternehmensleitung durch die Regelungen des Gesetzes über Ordnungswidrigkeiten (OWiG) und des Verbandssanktionengesetzes. Nach dem OWiG hat der Betriebsinhaber bzw. haben die ihm gleichgestellten Geschäftsführungs- und Vorstandsmitglieder sicherzustellen, dass die mit Aufgaben Betrauten keine Pflichtverletzungen (Straftaten oder Ordnungswidrigkeiten) begehen. Hierzu müssen sie durch Maßnahmen der Steuerung und Überwachung dafür sorgen, dass einerseits Zuwiderhandlungen erschwert, andererseits Verstöße festgestellt und korrigiert werden. Ein Verstoß, der aus einer Verletzung von Aufsichtspflichten resultiert, begründet eine persönliche Haftung der Mitglieder der Unternehmensleitung. Ähnlich sieht das künftige Verbandssanktionengesetz Geldsanktionen in Höhe von bis zu 10 Mio. Euro oder bis zu 10 % des durchschnittlichen Jahresumsatzes vor, wenn Leitungspersonen eine Straf-

tat selbst begehen oder »durch angemessene Vorkehrungen zur Vermeidung von Verbandstaten wie insbesondere Organisation, Auswahl, Anleitung und Aufsicht hätten verhindern oder wesentlich erschweren können«[2]. Der Unternehmensleitung kommt somit die Organisationspflicht zu, geeignete Compliance-Maßnahmen zu ergreifen.

Die Steuerungsverantwortung der Unternehmensleitung für IT-Compliance richtet sich grundlegend auf die Zielfestlegung und die Bereitstellung ausreichender finanzieller Ressourcen (i. S. sowohl von CAPEX als auch OPEX). Letztere sind erforderlich, um die personellen, aufbau- und ablauforganisatorischen sowie technisch-instrumentellen Voraussetzungen zur Erreichung und Aufrechterhaltung eines hinsichtlich der IT-Compliance-Risiken angemessenen Compliance-Levels zu schaffen. Zudem wird die Compliance- und Risikokultur eines Unternehmens wesentlich durch das Verhalten der Unternehmensleitung beeinflusst. Letztlich ist ein IT-Compliance-Management-System (IT-CMS) zu etablieren. Ein effektives IT-CMS ist ein deutliches Indiz dafür, dass die Unternehmensleitung ihre Sorgfaltspflichten hinsichtlich IT-Compliance erfüllt.

Weiterhin muss die Unternehmensleitung die Erfüllung externer und interner Vorgaben durch angemessene und wirksame Kontrollmaßnahmen sicherstellen. Der wesentliche Beitrag von IT-Compliance besteht aus einer systematischen Identifizierung von IT-Compliance-Anforderungen und der Bewertung ihrer Relevanz für das Unternehmen. Hierauf beruhend stellt die Ableitung von internen Kontrollen zur Sicherstellung der ordnungsmäßigen Prozessausführung innerhalb der IT einen wesentlichen Nutzen von IT-Compliance für das Unternehmen und die Unternehmensleitung dar. Hierbei sollte über das IT-Kontrollsystem ein IT-Compliance-Status ermittelt werden können. Mittels dieses Status wird die notwendige Transparenz erzeugt, damit die Unternehmensleitung IT-Compliance-Risiken bewerten und priorisieren sowie ggf. erforderliche Maßnahmen zur Risikosteuerung ergreifen kann.

Auch für IT-Compliance-Risiken muss die Unternehmensleitung gemäß der IT-Governance-Zielsetzung EDM03 den Risikoappetit sowie Toleranzgrenzen festlegen. Explizit ist das Potenzial für Compliance-Fehler zu minimieren (vgl. [ISACA 2018b, S. 41]). Dementsprechend richten sich die für das IT-bezogene Ziel AG01 (IT-Compliance und Unterstützung der Unternehmens-Compliance mit externen Gesetzen und Bestimmungen) angegebenen Metriken auf die Anzahl der Fälle von Non-Compliance, die zu Vergleichszahlungen, Bußgeldern und Reputationsverlusten führen, die vertragliche Vereinbarungen betreffen, einem internen Aufsichtsgremium berichtet werden müssen oder zu – für die Mitglieder der Unternehmensleitung ggf. auch persönlicher – negativer Publicity führen (vgl. [ISACA 2018b, S. 29]).

3.3 Nutzen von IT-Compliance aus Sicht der Fachabteilungen

In den Fachabteilungen (Rechnungswesen/Finanzen, Marketing, Einkauf etc.) zeigt sich der Nutzen von IT-Compliance vor allem darin, dass eine regelkonforme IT nicht nur die IT-bezogenen Ziele, sondern letztlich die Geschäftsziele der Fachabteilungen unterstützt. Dieses gilt insbesondere dadurch, dass ein Geschäftsprozess ohne IT nicht mehr vorstellbar ist und immer mehr Aufgaben dieses Geschäftsprozesses innerhalb von Anwendungen implementiert wird. Im Rahmen der Automatisierungs- und Digitalisierungsstrategien sind die Fachbereiche und das Unternehmen auf IT-Prozesse und IT-Services angewiesen. In dem Falle, dass Compliance-Anforderungen schon bei Anforderungsanalyse und Entwicklung von IT-Services berücksichtigt werden, können sich das Management und die Mitarbeiter der Fachabteilungen hinreichend sicher sein, in Übereinstimmung mit Compliance-Anforderungen zu agieren. Die oben bereits angesprochene Sicherstellung der ordnungsmäßigen Prozessausführung innerhalb der IT wirkt sich damit auch auf die operative Geschäftsprozessausführung aus.

Aufgrund des hohen Veränderungstempos im geschäftlichen Umfeld, bei gesetzlichen/regulatorischen Anforderungen und IT-Lösungen sind Compliance-Abweichungen nicht selten. Insofern generiert IT-Compliance für die Fachabteilungen dann einen Nutzen, wenn

- das erreichte Ausmaß an IT-Compliance messbar ist und als Management-Information vorliegt;
- durch aufbau- und ablauforganisatorische Maßnahmen ein Regelkreis etabliert wird, der veränderte IT-Compliance-Anforderungen erkennt und adressiert, aber auch unwirksame oder in ihrer Wirksamkeit mangelhafte Maßnahmen identifiziert und dem kontinuierlichen Verbesserungsprozess zuführt.

Für COBIT 2019 zeigt sich der Nutzen aus Sicht der Fachabteilungen in der Zufriedenheit mit den IT-Services. Diese hängt wesentlich von der Erfüllung vereinbarter Service Level ab. Hierbei haben IT-Services nach der Managementpraktik APO09.03 auch Compliance- und regulatorische Anforderungen zu berücksichtigen. Diese sind somit in Zusammenarbeit von Fachabteilungen und IT-Funktion in die Servicevereinbarungen aufzunehmen (vgl. [ISACA 2018b, S. 30, 113f.]). Dies gilt auch in Bezug auf Verträge mit IT-Anbietern, deren Leistungen die Fachabteilungen in der operativen Prozessausführung in Anspruch nehmen (vgl. [ISACA 2018b, S. 120]).

[2] So die Regelungen im derzeitigen Gesetzesentwurf vom 16.06.2020, s. § 3 Abs. 1 sowie § 9 Abs. 1 und 2 VerSanG-E.

Handlungsempfehlungen

- Sorgen Sie dafür, dass sich alle Unternehmensebenen mit der Bedeutung und dem Nutzen der IT-Compliance für die Geschäftstätigkeit auseinandersetzen.
- Die Nutzendiskussion von IT-Compliance sollte sich nicht nur auf die Vermeidung von Nachteilen (Bußgeldern, Strafen, Reputationsverlust etc.) konzentrieren, sondern auch die positiven Auswirkungen von IT-Compliance umfassen.
- Der Nutzen von IT-Compliance ist nicht nur allgemein, sondern auch für einzelne Regelwerke (ISO/IEC 2700x, PCI DSS, DSGVO, CSA STAR etc.) zu konkretisieren.
- Stellen Sie die Festlegung von Nutzendimensionen und it-git-zirmetriken sicher.
- Für jeden Prozess muss ein Prozesseigner (Owner) benannt sein, der die Prozess-Performance hinsichtlich IT-Compliance verantwortet (dies gilt auch für ausgelagerte IT-Compliance-Funktionen).
- Kommunizieren Sie den (auch individuellen) Nutzen von IT-Compliance an die Stakeholder. Dies ist die Voraussetzung dafür, dass ausreichend Ressourcen für IT-Compliance zur Verfügung gestellt werden.1

4 Stakeholder und Interessenlagen

4.1 Struktur der Stakeholder

Der Kreis der grundsätzlich an IT-Compliance beteiligten und von IT-Compliance betroffenen Personen und Gruppen (Stakeholder) erweist sich als durchaus umfangreich. In der Innensicht steht oft ein »IT-Compliance-Manager« im Mittelpunkt der fachlichen Diskussion. Gleichwohl gibt es eine ganze Reihe von beteiligten Stellen und Rollen, die in die aufbauorganisatorische Gestaltung von IT-Compliance einzubeziehen sind. In der Außensicht können unterschiedliche Personen, Gruppen oder Institutionen von IT-Compliance betroffen sein (vgl. Abbildung 4-1). Während in Bezug auf die unternehmensinternen Stakeholder in erster Linie ihre Aufgaben- und Verantwortungsteilung für IT-Compliance zu regeln sind, stehen bei den externen Stakeholdern Transparenz- und Informationspflichten im Vordergrund.

Die generellen Interessenlagen in Bezug auf IT-Compliance sind unterschiedlich. Zudem haben Stakeholder i. d. R. mehrere Interessen an der Sicherstellung von IT-Compliance durch Unternehmen.

- So können Stakeholder Quellen von Vorgaben an die Unternehmens-IT sein. In diesem Falle erwarten die Stakeholder die Einhaltung der Vorgaben bzw. stellen diese aktiv sicher.
- Stakeholder können Verantwortung i. S. von Haftbarkeit tragen. Sie erwarten die Compliance der IT, um persönliche Nachteile zu vermeiden.
- Stakeholder können aber auch insofern Betroffene sein, als ihre persönlichen Daten durch das Unternehmen verarbeitet werden. In diesem Fall haben sie im Wesentlichen ein Schutzinteresse.
- Verschiedenste Stakeholder haben ein Informationsinteresse, das sich auf den Status der IT-Compliance bezieht. Dieses Interesse umfasst nicht nur die Regelkonformität, sondern insbesondere auch eine unmittelbare Information im Falle von Non-Compliance.
- Weiterhin haben verschiedene Stakeholder ein fachliches Interesse an IT-Compliance, da sie diesbezügliche oder angrenzende Aufgaben ausführen oder verantworten. Gegebenenfalls nehmen diese Stakeholder in Bezug auf IT-Compliance Überwachungsaufgaben wahr.

Eine eingehende Stakeholder-Analyse und -Kommunikation ist heute eine notwendige Governance-Aufgabe und damit auch für Corporate Compliance bzw. IT-Compliance durchzuführen. Gerade Compliance benötigt eine intensive Kommunikation, um eine hinreichende Motivation für die Wahrnehmung von Compliance-Aufgaben zu schaffen – umso mehr, als Compliance häufig in der Kritik steht, teuer und

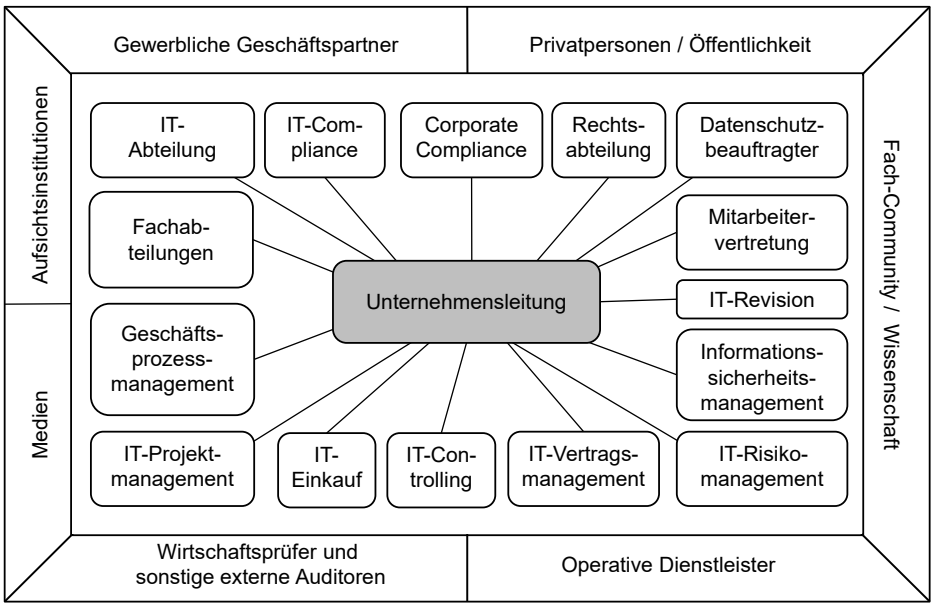


Abb. 4–1: Unternehmensinterne und -externe Stakeholder der IT-Compliance

überflüssig zu sein oder bremsend auf den Geschäftsalltag zu wirken. Nicht anders stellt sich dies für die IT-Compliance dar; »so wenig wie absolut notwendig« ist häufig das Motto. Insofern ist eine effektive Compliance-Kommunikation in Richtung der relevanten Stakeholder eine zentrale Aufgabe der IT-Compliance und wichtiges Element eines Compliance-Management-Systems.

In COBIT 2019 stellt die Sicherstellung der Stakeholder-Beteiligung eines der IT-Governance-Ziele (EDM05 – Ensured Stakeholder Engagement) dar. Die einzelnen Prozesspraktiken richten sich auf die Identifizierung und Gruppierung interner und externer Stakeholder, die Gestaltung des Berichtswesens und der sonstigen Kommunikation in Bezug auf die Informationsbedarfe der Stakeholder sowie die Überwachung der Effektivität der Stakeholder-Beteiligung. Diese Praktiken sollen nach COBIT 2019 explizit einen Beitrag dafür leisten, dass die Kosten von Non-Compliance minimiert werden (vgl. [ISACA 2018b, S. 49f.]). Auf das operative Management der Stakeholder-Beziehungen richtet sich das IT-Managementziel »APO08 – Managed Relationships«. Hinsichtlich Compliance steht hier das Verständnis für die regulatorischen Einflussfaktoren im Vordergrund (vgl. [ISACA 2018b, S. 108]). Im Rahmen des Risikomanagements (APO12 – Managed Risk) sind die IT-Risiken – und damit auch die IT-Compliance-Risiken – den Stakeholdern rechtzeitig zu kommunizieren (vgl. [ISACA 2018b, S. 133]). Beim Management von (Compliance-bezogenen) Prüfungen (MEA04 – Managed Assurance) sind die Prüfziele und Inhalte der Prüfinitiativen an den Interessen der Stakeholder auszurichten und mit diesen abzustimmen (vgl. [ISACA 2018b, S. 290f.]).

4.2 Unternehmensexterne Stakeholder

Bei den unternehmensexternen Stakeholdern kommt den Aufsichtsinstitutionen und denjenigen Stakeholdern, mit denen das Unternehmen in einer vertraglich geregelten Geschäftsbeziehung steht, eine besondere Bedeutung zu.

- **Aufsichtsinstitutionen**
  Aufsichtsinstitutionen stellen spezifische Anforderungen an die Ausgestaltung der Unternehmens-IT und erwarten die Einhaltung ihrer Vorgaben. Hierzu sind sie berechtigt, Informationen einzuholen, Nachweise zu verlangen oder die Compliance ggf. auch vor Ort zu prüfen. Bei Non-Compliance können sie – in unterschiedlichem Ausmaß – Sanktionen verhängen. Dadurch sind sie in der Lage, ihre Vorgaben bei den betroffenen Unternehmen durchzusetzen. Beispiele sind die BaFin, das BSI, die Datenschutzbehörden der Bundesländer und die Behörden der Finanzverwaltung.
- **Gewerbliche Geschäftspartner**
  Gewerbliche Geschäftspartner sind Wirtschaftssubjekte, mit denen das Unternehmen als Kunde oder Lieferant verkehrt. Diese Geschäftsbeziehungen sind vertraglich geregelt, sodass sich aus den Verträgen i. d. R. Verpflichtungen ergeben, die vom Unternehmen einzuhalten sind. IT-bezogene Verpflichtungen betreffen vor allem den Austausch vertraulicher Daten und Dokumente und eine damit oftmals verbundene Geheimhaltung. Gewöhnlich werden Fälle von Non-Compliance über Vertragsstrafen sanktioniert. Hinzu kommen Nachteile, die sich im B2B-Geschäftsverkehr bei Verstößen gegen gesetzliche Regelungen zum E-Commerce ergeben. Weiterhin spielen Anforderungen der IT-Compliance eine wichtige Rolle, wenn das Unternehmen mit strategischen Partnern – vor allem in der Supply Chain – so eng zusammenarbeitet, dass die IT-Systeme der Partner direkt miteinander interagieren. Eine derartige überbetriebliche Integration von IT-Systemen kann nur auf der Basis vereinbarter organisatorischer und technischer Standards funktionieren.
- **Operative IT-Dienstleister**
  Dienstleister zählen auch zu den gewerblichen Geschäftspartnern, nehmen aber in der IT eine besondere Rolle ein. Zum einen werden IT-Dienstleister heute im Rahmen des IT-Outsourcings[1] damit beauftragt, umfangreiche IT-Aufgaben oder ganze IT-Prozesse auszuführen. Aber auch das Outsourcing IT-gestützter Geschäftsprozesse ist hier zu berücksichtigen. Gerade im Bereich des Betriebs von IT-Infrastrukturen in der Cloud sind IT-Dienstleister heute unverzichtbare Partner. Damit stellen sich in der Zusammenarbeit mit ihnen besondere Anforderungen an Sicherheit, Verfügbarkeit, Nachhaltigkeit und nicht zuletzt Rechtskonformität und Compliance mit relevanten Normen und Standards. Hinsichtlich der IT-gestützten Geschäftsprozesse sind Anforderungen der Vollständigkeit, Richtigkeit, Nachvollziehbarkeit, Dokumentation etc. zu erfüllen. Hier hat ein Dienstleister jeweils mindestens die gleichen Anforderungsniveaus zu erfüllen wie der Auftraggeber selbst. Die Verantwortung für die Angemessenheit und Compliance der vom Dienstleister erbrachten IT-Services liegt weiterhin beim beauftragenden Unternehmen und ist demgemäß bei der Auftragsvergabe klar zu regeln und in der Durchführung kontinuierlich zu überwachen. Der IT-Dienstleister wird danach trachten (müssen), die Qualität seines internen Kontrollsystems und die Compliance seiner Leistungserbringung durch geeignete Zertifikate nachzuweisen, z. B. durch eine Zertifizierung des Informationssicherheitsmanagementsystems nach ISO/IEC 27001 oder eine Prüfung des IKS nach IDW PS 951 bzw. ISAE 3402.
- **Wirtschaftsprüfer und sonstige Auditoren**
  Vom Unternehmen beauftragte Wirtschaftsprüfer prüfen im Rahmen der Jahresabschlussprüfung die Ordnungsmäßigkeit und Sicherheit der IT-gestützten Rechnungslegung und damit die rechnungslegungsbezogene Compliance gegenüber den einschlägigen Vorschriften (HGB, AO, EStG, GoBD etc.). Darüber hinaus nehmen sie spezielle Zertifizierungen vor, insbesondere die eben angesprochene Prüfung des IKS nach IDW PS 951 bzw. ISAE 3402. Sonstige Auditoren führen institutionelle Zertifizierungen in verschiedenen Themen durch, z. B. des Informationssicherheitsmanagementsystems nach ISO/IEC 27001 oder des Datenschutzes mittels eines Datenschutzaudits.

[1] In einem weiten Begriffsverständnis, d. h. inkl. IT-Fremdbezug bzw. Outtasking.

- **Öffentlichkeit**
  Die Öffentlichkeit ist in Bezug auf IT-Compliance eine wichtige Stakeholder-Gruppe, wenn Non-Compliance, vor allem in Bezug auf datenschutzrechtliche Verstöße, durch die öffentlichen Medien kommuniziert wird. Reputationsverluste und ggf. auch Umsatzeinbußen können – wenn i. d. R.auch nur kurzfristig – einen beträchtlichen Schaden verursachen. Dieser kann für Unternehmen noch größer werden, wenn durch öffentlichen Druck die Politik oder Aufsichtsinstitutionen zu reglementierenden Maßnahmen gedrängt werden.
- **Privatpersonen**
  Auch mit Kunden als Privatpersonen verkehrt ein Unternehmen im Rahmen einer vertraglich geregelten Geschäftsbeziehung. Die Kunden haben zum einen ein Interesse am Schutz ihrer personenbezogenen Daten, die im Rahmen der Geschäftsabwicklung verarbeitet werden. Die Verarbeitung der personenbezogenen Daten ist vertraglich zwischen Kunde und Unternehmen zu regeln, die Grundlage hierfür stellen die datenschutzrechtlichen Vorgaben der DSGVO, des BDSG und ggf. weiterer gesetzlicher Regelwerke dar. Insbesondere ergeben sich aus den gesetzlichen Regelungen die Sanktionsandrohungen bei Non-Compliance. Zum anderen müssen Kunden auf die Verfügbarkeit und den sicheren IT-Betrieb der IT-Systeme, über die sie mit dem Unternehmen interagieren, vertrauen dürfen. Dies gilt vor allem für E-Commerce-Systeme und für IT-Systeme im Rahmen von kritischen Infrastrukturen, z. B. im Gesundheitswesen. Die diesbezügliche Verpflichtung für die Unternehmen entsteht aus den Vorgaben des IT-Sicherheitsgesetzes.

Als externe Stakeholder nennt COBIT 2019 explizit Regulierungsinstitutionen, Geschäftspartner, IT-Lieferanten und Assurance-Provider. Für die Zusammenarbeit mit diesen Gruppen bietet ein IT-Governance-System nach COBIT 2019 jeweils spezifische Compliance-Vorteile:

- Im Hinblick auf die Regulierungsinstitutionen wird gewährleistet, dass sich das Unternehmen auch aus Sicht der jeweiligen Regulierungsinstitution an die geltenden Regeln und Vorschriften hält und über das richtige Governance-System verfügt, um Compliance zu steuern und aufrechtzuerhalten.
- In der Zusammenarbeit mit Geschäftspartnern und IT-Lieferanten wird sichergestellt, dass der IT-Betrieb des jeweiligen Geschäftspartners oder Lieferanten sicher, zuverlässig und in Übereinstimmung mit den geltenden Regeln und Vorschriften erfolgt. Hierzu sind Compliance-Anforderungen bereits bei der Lieferantenauswahl (APO10.02) zu berücksichtigen. Die Überwachung der Compliance des Lieferanten mit den vertraglichen Anforderungen hat regelmäßig zu erfolgen (APO10.05) (vgl. [ISACA 2018b, S. 120f.]).
- Assurance Provider unterstützen das Unternehmen darin, die Abhängigkeit von externen Dienstleistern zu steuern, Zusicherungen in Bezug auf die IT zu erhalten und die Existenz eines effektiven und effizienten internen Kontrollsystems sicherzustellen (vgl. [ISACA 2018a, S. 15]).

→

Die Öffentlichkeit als Stakeholder findet sich in COBIT 2019 im Rahmen der Unternehmens- und IT-bezogenen Ziele wieder. Das Unternehmensziel Nr. 3 (Compliance with external laws and regulations) bezieht sich auf die Compliance mit gesetzlichen und regulatorischen Vorgaben. Eine der Metriken zur Messung der Zielerreichung ist die Anzahl der Fälle von Non-Compliance, die das Unternehmen zu einer öffentlichen Stellungnahme zwingen oder negative Publicity nach sich ziehen. Ähnlich verhält es sich mit den IT-bezogenen Zielen Nr. 1 (I&T compliance and support for business compliance with external laws and regulations) und Nr. 7 (Security of information, processing infrastructure and applications, and privacy). Auch hier richten sich jeweils Metriken auf die Anzahl der IT-bezogenen Fälle von Non-Compliance, die eine öffentliche Stellungnahme erfordern und das Ansehen des Unternehmens in der Öffentlichkeit schädigen (vgl. [ISACA 2018a, S. 29ff.]).

Die Wissenschaft und die Fach-Community sowie die Medien sind im Einzelfall bedeutende Stakeholder.

- **Wissenschaft / Fach-Community**
  Wissenschaft und Fach-Community können wichtige Impulse für die Gestaltung der IT-Compliance im Unternehmen geben. In erster Linie erfolgt dies über wissenschaftliche Publikationen und Vorträge bzw. über Best Practices, Leitfäden (wie die ISACA-Leitfäden) oder Fach- und Branchenstandards. Letztere bilden dann wieder einen Teil der Regelwerke, gegenüber denen ein Unternehmen ggf. compliant agieren muss. Auch der Austausch in Fachgremien bildet eine Möglichkeit, erforderliches Wissen zu erlangen. Im Bereich der Weiterbildung sind es Seminare und umfangreichere Formate bis hin zu Studienabschlüssen, die einen Know-how-Aufbau der Compliance-Beteiligten im Unternehmen bewirken. Ein Engagement in diesen Fachstrukturen ermöglicht es Unternehmen aber auch, auf den State of the Art der Compliance Einfluss zu nehmen.
- **Medien**
  Die Medien sind dann ein wichtiger Stakeholder, wenn sie in Fällen von Non-Compliance über derartige Vorfälle berichten. Je nach Umfang kann die Berichterstattung geringer oder umfangreicher ausfallen. In letzterem Fall nimmt die Compliance-Kommunikation die Form einer Krisenkommunikation an. Auf der anderen Seite werden über die Medien aber auch Fachinhalte kommuniziert, die für die Gestaltung eines IT-Compliance-Management-Systems, beispielsweise für die Gestaltung von Compliance-Prozessen und die Nutzung von Compliance-Tools, in vielfältiger Weise genutzt werden können. Durch die Berichterstattung der Medien, z. B. zu neuen Gesetzen, mit Reportagen über Bedrohungen oder Dokumentationen zu aktuellen IT-Entwicklungen, wirken die Medien aber auch an der Bewusstseinsbildung in Bezug auf IT und IT-Compliance mit.

Fachexperten und Social Media werden von COBIT 2019 im Rahmen der Managementpraktik BAI08.01 (Identify and classify sources of information for governance and management of I&T) angesprochen. In dieser Praktik geht es um die Identifizierung, Validierung und Klassifizierung verschiedener Quellen interner und externer Informationen, die für die Steuerung und das Management der IT – und damit auch für Themen der IT-Compliance – benötigt werden (vgl. [ISACA 2018b, S. 206]).

4.3 Unternehmensinterne Stakeholder

Mit der Position in der Mitte der Abbildung 4-1 soll betont werden, dass die Hauptverantwortung für IT-Compliance der Unternehmensleitung zukommt. Damit diese Verantwortung wahrgenommen werden kann, sollte die IT im Verantwortungsfokus der Unternehmensleitung und eventueller Aufsichtsorgane einen wesentlich größeren Anteil erhalten, als dies bisher in vielen Unternehmen der Fall ist. Dies erfordert jedoch nicht nur quantitative personelle Ressourcen (z. B. in Form der Positionen CIO oder CDO), sondern auch qualitative Verbesserungen in Form der Erhöhung der IT-Kompetenz in Vorstands- und Geschäftsführungsgremien. Dieses muss Hand in Hand gehen mit einem Compliance-Berichtswesen, das die spezifischen Informationsbedarfe der verschiedenen Chief-Positionen adressiert. Zum Beispiel erfordern die multidisziplinären Anforderungen der DSGVO eine unterschiedliche Information für die verschiedenen Mitglieder der C-Ebene (CEO, CFO, CIO, COO etc.) (nach [Pearce 2019, S. 32f.]).

Vor dem Hintergrund der Allgegenwart von IT in der heutigen Wirtschaftswelt und der Entwicklung, dass Geschäftsmodelle zunehmend IT-Anteile beinhalten oder gar gänzlich auf IT basieren, muss IT auch zum Thema in Aufsichtsorganen, insbesondere Aufsichtsräten, werden. Mitglieder von Aufsichtsorganen besitzen aber gewöhnlich keine ausgeprägte IT-Kompetenz. Auch ist die Vermittlung von IT- und Digitalisierungswissen im Rahmen der Weiterbildung für Mitglieder von Aufsichtsorganen derzeit eher die Ausnahme.

Die Unternehmensleitung muss zur Wahrnehmung ihrer Compliance-Verantwortung strategisch-konzeptionelle und operative Aufgaben übernehmen und die hierfür erforderlichen Befugnisse delegieren. Der Kreis der hierfür zur Verfügung stehenden Funktionsträger hängt vor allem von der Unternehmensgröße, der Gesellschaftsform, der Kapitalherkunft und der Branchenzugehörigkeit ab. In jedem Falle sind aber die IT-Abteilung und die Fachabteilungen als Hauptbeteiligte einzubeziehen.

- **IT-Abteilung**
  Die IT-Abteilung und ihre Leitung bzw. der CIO haben den Großteil an Maßnahmen zur Erfüllung der Compliance-Anforderungen zu planen und durchzuführen, zumindest soweit es die informations- und kommunikationstechnischen Mittel anbelangt. Hierbei sind die Entwicklung und der Betrieb von IT-Systemen selbst an Standards, wie der Information Technology Infrastructure Library (ITIL®[2]) oder der ISO/IEC-27000-Reihe bzgl. der Informationssicherheit, auszurichten. Hinsichtlich der IT-gestützten Compliance ist auch die Anwendungsentwicklung und -pflege betroffen. Da rechtliche Anforderungen oft tief in die Prozesse und die Architektur einer Software hineinwirken, sind diese bereits bei der Anforderungsspezifikation zu berücksichtigen. Dieser Ansatz wird als »Compliance by Design« bezeichnet. Er stellt die softwaretechnische Umsetzung der Forderung aus der DSGVO nach »Data Protection by Design« dar, wonach das Recht auf Datenschutz bei der Entwicklung, Gestaltung und Auswahl von IT-Anwendungen und Diensten durch geeignete technische und organisatorische Maßnahmen zu berücksichtigen ist (vgl. [DSGVO 2018, Rz. 78]).
- **Fachabteilungen**
  Auch das Management der Fachabteilungen trägt eine Verantwortung für die Erfüllung von Compliance-Anforderungen. Im Idealfall sollten sich die Fachabteilungen im Rahmen der Ausführung ihrer Geschäftsprozesse auf regelkonforme IT-Systeme stützen können, sodass die mit den Geschäftsprozessen verbundenen Risiken durch die IT-Anwendungen und die darin automatisierten Kontrollen per se sicher sind. Trotzdem muss IT-Compliance durch die Fachabteilungen aktiv sichergestellt werden, und zwar immer dann, wenn organisatorische oder personelle Maßnahmen ergriffen und entsprechende Kontrollen eingeführt werden. Vor allem die »Awareness« für IT-Compliance, insbesondere für Datenschutz und Informationssicherheit, muss in den Fachabteilungen entwickelt werden. Damit ist aber nicht nur das Management der Fachabteilungen angesprochen, sondern auch die Mitarbeiter stellen als Nutzer der IT-Systeme einen Stakeholder dar.

Als Unternehmensleitung spricht COBIT 2019 das in der US-amerikanischen Unternehmensverfassung typische monistische (»one tier«) System mit einem »Board« an, das sowohl Mitglieder der Unternehmensleitung als auch externe Mitglieder umfasst. Die »C-Ebene« wird von COBIT 2019 in die einzelnen Positionen untergliedert (CEO, CFO, COO, CRO und CIO). Das Board wird ergänzt durch ein »Executive Management«. Weitere Stakeholder aus dem Management sind Bereichsleitungen und IT-Manager (vgl. [ISACA 2018a, S. 15] und [ISACA 2018b, S. 76]).

Vor allem mit Blick auf die Regulierungsbestrebungen von Gesetzgebung und Aufsichtsinstitutionen ist es unumgänglich, dass nicht nur in größeren, sondern auch in mittelständischen Unternehmen konsequent eine ganze Reihe von Stellen und Funktionen aufgebaut werden, die sich explizit mit IT-Compliance befassen.

[2] ITIL® ist ein eingetragenes Warenzeichen von AXELOS Limited.

- **Corporate Compliance/IT-Compliance**
  Eine »Corporate Compliance« als zentrale, der Unternehmensleitung zugeordnete Compliance-Funktion findet sich derzeit vor allem in großen Unternehmen, insbesondere in börsennotierten Aktiengesellschaften. Derartige Organisationseinheiten können unabhängig die Aufstellung von Regeln und deren Schulung mit der Überwachung der Regeleinhaltung verbinden und alle notwendigen Aspekte von finanziell-steuerlicher, arbeitsgesetzlicher, produkt- und umweltrechtlicher Compliance abdecken (nach [Behringer 2013, S. 376f.]). In einem solch umfassenden Compliance-Verständnis wäre dann auch zumindest ein Teil der Verantwortung für IT-Compliance in dieser Funktion anzusiedeln und in der Stellenstruktur bzw. der Aufgabenverteilung abzubilden. In diesem Falle wäre dann auch die Stelle eines IT-Compliance-Managers an der Corporate Compliance anzubinden.
- **Rechtsabteilung**
  Die juristische Beurteilung gesetzlicher, regulatorischer und vertraglicher Anforderungen an die IT bedarf des Know-how-Aufbaus in der Rechtsabteilung, damit diese ihrer Verantwortung – auch für die IT-Compliance – angemessen nachkommen kann.
- **Geschäftsprozessmanagement**
  Eine weitere Schnittstelle ergibt sich zum Geschäftsprozessmanagement hinsichtlich der Compliance von Geschäftsprozessen. Soweit Stellen mit spezialisierter Prozessverantwortung eingerichtet sind (sog. Prozesseigentümer bzw. Process Owner), ist es erforderlich, deren Verantwortungsbereich um Aspekte der IT-Compliance zu erweitern. Hierbei gilt es, prozessuale, IT-bezogene Compliance-Anforderungen in die Geschäftsprozessmodellierung und -gestaltung zu integrieren und die Einhaltung im Rahmen der Prozessüberwachung – ggf. in Zusammenarbeit mit der IT-Abteilung – sicherzustellen.
- **IT-Risikomanagement**
  Der oben beschriebene inhaltliche Zusammenhang zwischen IT-Risikomanagement und IT-Compliance erfordert auch auf institutioneller Ebene eine Zusammenarbeit zwischen den entsprechenden organisatorischen Einheiten. Das Risikomanagement konzentriert sich auf wesentliche Unternehmensrisiken, zu denen IT-Risiken in der Vergangenheit in den wenigsten Unternehmen zählten. Dies hat sich durch die gesetzlichen Entwicklungen grundlegend geändert; IT-Risiken und speziell IT-Compliance-Risiken hinsichtlich des Datenschutzes und der IT-Sicherheit sind zusehends in den Fokus des Risikomanagements gerückt. Die potenziellen Bußgelder der DSGVO führten und führen zu umfangreichen Datenschutzmaßnahmen. In KRITIS-Unternehmen gilt dies vor allem für das Notfall- und Kontinuitätsmanagement. Maßnahmen in all diesen Bereichen können bzw. müssen sich an zahlreichen allgemeinen und branchenbezogenen IT-Normen und -Standards orientieren.
- **Informationssicherheitsmanagement**
  Ähnlich wie für das IT-Risikomanagement ist auch für IT-Compliance und Informationssicherheitsmanagement eine enge inhaltlich-institutionelle Verzahnung gegeben. Gerade die Vielzahl an Sicherheitsvorgaben (z. B. aus der ISO/IEC 27001, den GoBD, den BSI-Standards, der DSGVO, dem IT-Sicherheitsgesetz sowie branchenbezogenen Vorgaben, wie die an die Finanzdienstleistungsinstitute gerichteten MaRisk und BAIT/VAIT) lassen die Konformität mit Gesetzen, Normen und Standards zum IT-Sicherheitsmanagement als Kern der IT-Compliance erscheinen.[3] Auch wenn diese Auffassung vor dem Hintergrund aktueller Herausforderungen als faktisch vertretbar anzusehen ist, geht der Geltungsbereich von IT-Compliance doch weit über den IT-Sicherheitsfokus hinaus. Die zu schaffenden Strukturen, z. B. hinsichtlich IT-Compliance-Prozessen, einem IT-CMS und der Zuordnung von Rollen und Verantwortlichkeiten, sollten die gesamte Bandbreite der an die Unternehmens-IT gerichteten Vorgaben abdecken, um Überschneidungen, Dopplungen, Lücken und daraus resultierende Ineffizienzen zu vermeiden.
- **IT-Vertragsmanagement**
  IT-Vertragsmanagement reicht von der Spezifikation der IT-Leistungen und dem Festlegen der vertraglichen Anforderungen über die Vertragsgestaltung und verhandlung bis hin zum Vertragscontrolling (nach [Klotz/Dorn 2016, S. 71]). Dieser Aufgabenumfang ist in Unternehmen oftmals nicht zentralisiert, sondern auf unterschiedliche Stellen verteilt. Involviert ist in jedem Falle die Rechtsabteilung; spätestens dann, wenn eine mangelnde Vertragseinhaltung moniert werden muss. Auch die Einkaufsabteilung, das IT-Controlling bzw. diejenige Organisationseinheit, der das Management von Auslagerungen obliegt, nehmen Überwachungs- und Steuerungsaufgaben bei der Durchführung von IT-Verträgen wahr. Eine weitere organisatorische Gestaltungsoption besteht darin, dass das IT-Vertragsmanagement in ein umfassenderes IT-Lieferantenmanagement integriert ist. Gerade im Bereich der Auftragsverarbeitung nach Art. 28 DSGVO bildet die Sicherstellung der vertraglichen Compliance eine wichtige Aufgabe, da die Verantwortung für die Ordnungsmäßigkeit des IT-Betriebs beim Auftraggeber verbleibt. Bei umfangreichem IT-Outsourcing sind speziell für geschäftskritische IT-Services Service Level Agreements zur Definition von Leistungsgrenzen zu verwenden. Die SLAs müssen so ausgestaltet sein, dass sie eine messbare Abgrenzung zwischen Leistungserfüllung und Minderleistung ermöglichen – nur dann kann ggf. in der IT das Vorliegen vertraglicher Non-Compliance festgestellt werden (vgl. [Gründer 2016, S. 27]).
- **IT-Projektmanagement**
  IT-Projekt-Compliance in Bezug auf den Leistungsgegenstand richtet sich auf die Frage, welche Regelwerke das Projektergebnis (Software, IT-Service) zu erfüllen hat. Compliance ist hier insofern in die Zukunft gerichtet, als es um die spätere, den Compliance-Vorgaben entsprechende Nutzung des IT-Produkts geht (nach [Klotz

[3] Diesen Fokus wählen Rath/Sponholz in ihrem Werk zu IT-Compliance, wenn sie ihr Wirkungsmodell zur IT-Sicherheit an den Beginn ihrer Ausführungen stellen, vgl. [Rath/Sponholz 2014, S. 45ff.].

2014b, S. 698]). Die Integration von Compliance-Fragen in das Projektmanagement stellt eine organisatorische Umsetzung der Forderung nach »Compliance by Design« dar. Relevant sind auch hier Vorgaben aus Normen, Standards, Gesetzen und Verträgen. Falls vertraglich geregelte Leistungen im Rahmen von IT-Projekten erbracht werden, kann das Vertragscontrolling auch Aufgabe des IT-Projektmanagements sein.

- **IT-Einkauf**
  Der IT-Einkauf muss in enger Zusammenarbeit mit der Rechtsabteilung IT-Leistungen auf der Basis klarer und nachvollziehbarer vertraglicher Vereinbarungen beschaffen. Hierbei gilt es, die Risiken aus vertraglicher Non-Compliance gering zu halten. Beispielsweise ist die Prüfung auf Compliance bzgl. der Vorgaben zur Auftragsverarbeitung i. S. der DSGVO beim Abschluss und der Durchführung von Verträgen für die Inanspruchnahme von IT-Leistungen in der Cloud obligatorisch. Der IT-Einkauf hat Transparenz bzgl. der Leistungen und Pflichten der zu beauftragenden IT-Dienstleister bereits bei Anfragen bzw. Ausschreibungen – z. B. im Rahmen eines Lastenheftes – sicherzustellen.
- **IT-Controlling**
  Mit dem IT-Vertragsmanagement ist in manchen Unternehmen anstelle der Rechtsabteilung das Controlling befasst, sodass diese Stelle mitunter auch Überwachungs- und Steuerungsaufgaben bei der Durchführung von IT-Verträgen wahrnimmt. Von größerer Bedeutung ist allerdings die Aufgabe, das Management von IT-Compliance mit Instrumenten des IT-Controllings zu unterstützen. Diese umfassen vor allem ein System zur Bildung, Erfassung und Berechnung aussagekräftiger Kennzahlen sowie ein Berichtswesen, das die unternehmensinternen Stakeholder mit den relevanten Informationen über den Stand und die Entwicklung der IT-Compliance unterrichtet. Hierbei ist das Reporting bzgl. IT-Compliance in das Reporting der Corporate Compliance zu integrieren.
- **Datenschutzbeauftragter**
  Mit dem durch Art. 37 DSGVO und § 4f BDSG vorgeschriebenen Datenschutzbeauftragten gibt es eine Stelle im Unternehmen, die bezogen auf das Gebiet des Datenschutzes eine Compliance-Funktion wahrnimmt. Der DSB hat nach Art. 39 Abs. 1 DSGVO explizit die Aufgabe, die Einhaltung der DSGVO und anderer Datenschutzvorschriften zu überwachen. Das vielfach propagierte Datenschutz-Management-System sollte jedoch nicht isoliert aufgebaut werden, sondern einen integralen Bestandteil des IT-Compliance-Management-Systems bilden.
- **IT-Revision**
  Da Buchführung und Finanztransaktionen des Unternehmens IT-gestützt erfolgen, ist die Ordnungsmäßigkeit der IT Gegenstand nicht nur der externen Jahresabschlussprüfung, sondern auch der Internen Revision (IR). Diese Prüfungsinstanz stellt aus Sicht der Unternehmensleitung ein unverzichtbares Instrument zur Überwachung der Einhaltung von externen und internen Vorgaben dar. Die IT-Revision als Teil der IR hat unter anderem die Angemessenheit und Wirksamkeit des IT-Kontrollsystems zu beurteilen, indem sie die Durchführung verschiedener IT-Kontrollen prüft. Auch der Datenschutz sollte regelmäßig Gegenstand der IT-Revision sein und z. B. die fristgerechte Veröffentlichung des Verzeichnisses der Verarbeitungstätigkeiten, die Verpflichtung der Mitarbeiter auf das Datengeheimnis, die Durchführung von Folgenabschätzungen und einen Prozess zur Erfassung von erheblichen Datenschutzverstößen zum Inhalt der Prüfung haben (vgl. [Thelemann/Bunzel 2011, S. 166]). In ihrer Prüfungsarbeit orientieren sich IT-Revisoren an entsprechenden Standards, vor allem des IIA und des DIIR, sowie Normen zum Prüfwesen, zur IT-Sicherheit und zum IT-Risikomanagement und bestätigen ggf. die hinreichende Konformität oder treffen Feststellungen zu Abweichungen. Praxisnahe Hinweise und Handlungsempfehlungen für die IT-Revision bietet auch der ISACA-Leitfaden »Grundlagen der IT-Revision«, der demnächst auch in einer neuen Version erscheinen wird.
- **Mitarbeitervertretung**
  Die Mitarbeitervertretung ist ein gesetzlich vorgeschriebener Stakeholder, dem nach Betriebsverfassungsgesetz umfangreiche Informations- und Beteiligungsrechte zukommen. Für die IT wesentlich sind Mitwirkungsrechte in der Planungsphase oder ggf. Mitbestimmungsrechte in der Einführungsphase. So ist der Betriebsrat nach §§ 80 Abs. 2, 90 BetrVG über die geplante Einführung von IT-Systemen, die Erweiterung ihres Einsatzes und die Einführung neuer Programme unverzüglich zu unterrichten. Dem Betriebsrat steht darüber hinaus ein Mitbestimmungsrecht zu (und die Maßnahme bedarf somit seiner Zustimmung in Form einer Betriebsvereinbarung), wenn es sich beim betreffenden IT-System gemäß § 87 Abs. 1 Nr. 6 BetrVG um eine Einrichtung handelt, die dazu bestimmt ist, die Leistung oder das Verhalten von Arbeitnehmern zu überwachen.

Viele der genannten Organisationseinheiten werden auch in COBIT 2019 berücksichtigt (vgl. [ISACA 2018b, S. 300f.]):

- **Compliance:** Funktion im Unternehmen, die für alle Führungsaufgaben im Hinblick auf Compliance verantwortlich ist.
- **Legal Counsel:** Funktion, die für die Beratung in rechtlichen und regulatorischen Fragen zuständig ist.
- **Business Process Owner:** Einzelne Mitarbeiter, die für die Durchführung von Prozessen und/oder die Realisierung von Prozesszielen, die Prozessverbesserung und die Freigabe von Prozessänderungen verantwortlich sind.
- **IT Risk Officer:** Optionale Position zur Überwachung der IT-Risiken.
- **Information Security Officer:** Stelle, die die Informationssicherheit eines Unternehmens managt, gestaltet, überwacht und/oder bewertet.
- **Privacy Officer/Data Protection Officer:** Stelle, die die Risiken und geschäftlichen Auswirkungen von Datenschutzgesetzen beobachtet und abschätzt sowie Richtlinien und Aktivitäten zur Umsetzung von Datenschutzrichtlinien koordiniert und überwacht.
- **Audit:** Funktion, die für die Durchführung von internen Prüfungen zuständig ist.

Diese Abteilungen bzw. Stellen bilden die Governance-Komponente »Organisationsstrukturen« und sind damit Teil der Beschreibungen der IT-Governance- und IT-Managementzielsetzungen. COBIT 2019 nutzt hierzu das bekannte RACI-Modell, wobei nur noch A- und R-Rollen verwendet werden, um die Verantwortlichkeiten für die Durchführung der Praktiken den Abteilungen und Stellen zuzuordnen.

Neben den hier aufgeführten gibt es weitere Stellen und Funktionen, die sich nach Branchenerfordernissen richten. So schreiben z. B. das Wertpapierhandelsgesetz (WpHG) für Wertpapierdienstleistungsunternehmen (dies sind u. a. Kredit- und Finanzdienstleistungsinstitute) in § 33 Abs. 1 WpHG wie auch die Mindestanforderungen für das Risikomanagement (MaRisk AT 4.4.2) die Einrichtung einer Compliance-Funktion vor. Sie hat insbesondere auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen hinzuwirken. Ferner hat die Compliance-Funktion die Geschäftsleitung hinsichtlich der Einhaltung dieser rechtlichen Regelungen und Vorgaben zu unterstützen und zu beraten. Eine IT-gestützte Compliance dürfte hierzu in den meisten Fällen erforderlich sein.

Das Interesse der Stelleninhaber an IT-Compliance wird sich nach dem Inhalt und dem Umfang der an sie delegierten Verantwortung richten. In jedem Falle steht auch eine persönliche Haftung infrage, nicht nur für die Unternehmensleitung. Bei einer nicht regelkonformen Aufgabenausführung können auch Mitarbeiter prinzipiell zur Verantwortung gezogen und haftbar gemacht werden, wenn zumindest mittlere Fahrlässigkeit vorliegt.

In vielen Unternehmen stellt sich derzeit die Herausforderung, IT-Compliance vertikal gegenüber der Corporate Compliance und horizontal gegenüber IT-Risiko- und IT-Sicherheitsmanagement zu verorten. In dieser Konstellation bietet sich für die Beteiligten die Chance, den eigenen Aufgaben- und Verantwortungsbereich zu erweitern. Mitunter können sich so auch neue Karrierepfade eröffnen. Auf der anderen Seite ergeben sich fast automatisch Konkurrenzsituationen bzgl. Ressourcen und Einfluss. Hieraus resultierende Unsicherheiten gilt es bei der institutionellen Verankerung von IT-Compliance im Unternehmen durch eine klare Aufgaben- und Verantwortungsteilung zu beseitigen. Diese Klärung zu initiieren und durchzusetzen ist eine Aufgabe im Rahmen der IT-Governance und liegt damit in der Verantwortung der Unternehmensleitung.

Handlungsempfehlungen

- Identifizieren Sie die Stakeholder und ihre Interessen in Bezug auf Ihre IT-Compliance. Berücksichtigen Sie hierbei interne und externe Stakeholder.
- Je Stakeholder ist das Compliance-Risiko zu ermitteln, sollte es zur Nichteinhaltung von Anforderungen oder Vereinbarungen kommen.
- Etablieren Sie eine effektive Stakeholder-Kommunikation. Dabei sollte sichergestellt werden, dass Berichte auf Basis von zentralen Vorgaben und Datenerhebungen erstellt und geprüft werden. Gegebenenfalls sind Kommunikationswege und -umfang vertraglich zu vereinbaren und zu dokumentieren.
- Die Analyse der IT-Anforderungen seitens der Stakeholder ist in das IT-CMS zu integrieren.
- Klären Sie die Aufgaben und Verantwortlichkeiten der verschiedenen internen Stakeholder in Bezug auf IT-Compliance. Identifizieren Sie organisatorische Schnittstellen und regeln Sie die Zusammenarbeit.

5 Für IT-Compliance relevante Regelwerke

5.1 Klassifikation der Regelwerke

Die Anforderungen, die von der IT-Compliance zu behandeln sind, basieren auf unterschiedlichen Rechtsgrundlagen und stammen aus sehr unterschiedlichen Quellen. Als Sammelbezeichnung hierfür wird der Begriff der »Regelwerke« eingeführt, wobei der alltagssprachliche Gebrauch des Dudens verwendet wird. Hiernach ist eine Regel eine »aus bestimmten Gesetzmäßigkeiten abgeleitete, aus Erfahrungen und Erkenntnissen gewonnene, in Übereinkunft festgelegte, für einen jeweiligen Bereich als verbindlich geltende ... Anweisung für jemandes Verhalten in einem bestimmten Einzelfall, in einer Situation, bei einer Tätigkeit o. Ä.«.[1]

Es lassen sich grundsätzlich vier Gruppen von Regelwerken unterscheiden, die in ihrer Summe ein Grundgerüst (auch bekannt unter »House of IT Compliance«) für eine systematische Analyse von Compliance-Anforderungen darstellen (vgl. Abbildung 5–1):

- Rechtliche Vorgaben, d. h. Rechtsnormen (also vom Gesetzgeber erlassene Gesetze sowie auf deren Grundlage von den Verwaltungen erlassene Rechtsverordnungen), Rechtsprechung sowie Verwaltungsvorschriften und weitere Regelwerke, auf die in Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften verwiesen wird oder die von der Rechtsprechung zur Auslegung herangezogen werden
- Mit Kunden und Lieferanten geschlossene Verträge des Unternehmens, die IT-relevante Vereinbarungen enthalten
- Unternehmensexterne, auf IT-bezogene Regelwerke, wie z. B. Normen oder Standards vielfältiger Institutionen
- Unternehmensinterne Regelwerke, wie IT-Richtlinien, Hausstandards, Verfahrensanweisungen und interne, IT-bezogene Vereinbarungen, soweit sie IT-relevante Vorgaben enthalten

Gesetzliche und regulatorische Compliance-Anforderungen stellen für COBIT 2019 einen externen Informationsinput dar. Eine grobe Klassifikation der Regelwerke wird auch von COBIT 2019 vorgesehen. So unterscheidet die Managementpraktik MEA03.01 (Identify external compliance requirements) zwischen gesetzlichen und regulatorischen, aber auch vertraglichen Anforderungen (vgl. [ISACA 2018b, S. 285ff.]).

[1] [Duden], Stichworte Regel und Richtlinie. Die Definition des Dudens für »Regel« verwendet den Begriff »Richtlinie«. Da dieser im Kontext der Compliance eher als Fachbegriff anzusehen ist, wurde er durch seine Definition »Anweisung für ...« ersetzt.

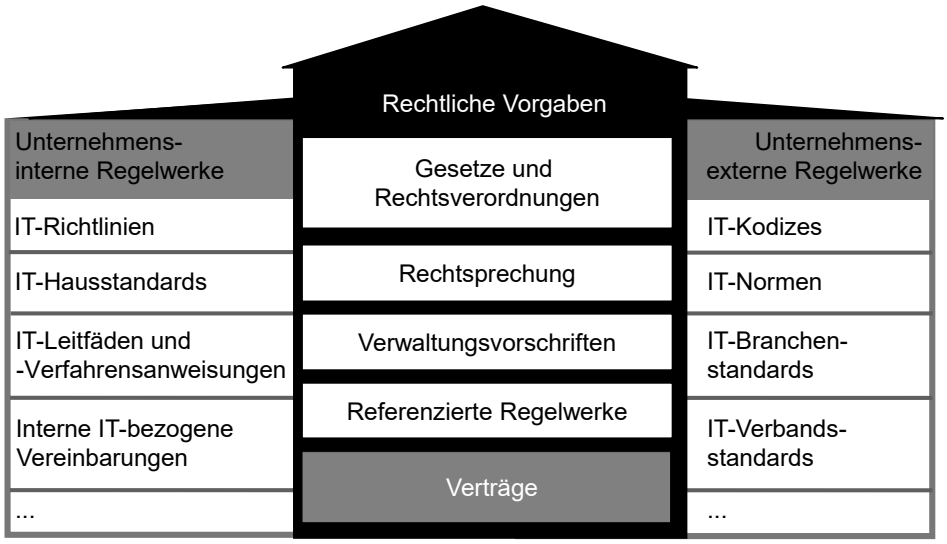


Abb. 5–1: Klassifikation der Regelwerke für IT-Compliance (»House of IT Compliance«) (nach [Klotz 2009, S. 4])

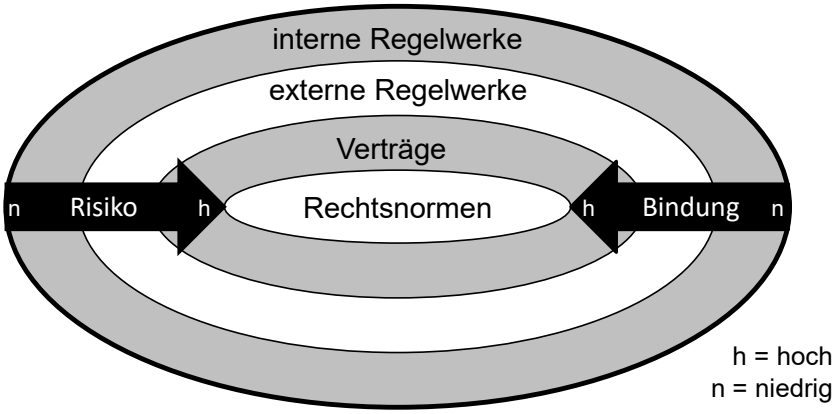


Abb. 5–2: Zwiebelmodell für Compliance-relevante Regelwerke (nach [Klotz 2009, S. 21])

Mit der Überlegung, dass sowohl der Bindungsgrad als auch das Risiko bei einem Verstoß in der genannten Reihenfolge tendenziell abnehmen, ergibt sich das in Abbildung 5–2 dargestellte »Zwiebelmodell«.

Der Bindungsgrad kann von einer freiwilligen Anwendung bis zu einer obligatorischen Verpflichtung reichen. Je weiter ein Regelwerk in der Mitte einzuordnen ist, desto größer sind die Risiken, die mit der Nichtberücksichtigung bzw. Nichteinhaltung dieses Regelwerks verbunden sind. Entsprechend hoch sollte aus Sicht der Compliance die Bindung i. S. einer angestrebten Regelwerktreue und daraus resultierend die Umsetzung der Anforderungen sein.

Bei Rechtsnormen und Verträgen ergeben sich höhere Risiken, weil hier oft ein monetäres Strafmaß entweder gesetzlich oder vertraglich geregelt ist bzw. aus Vertragsverletzungen teilweise bestandsgefährdende Schadensersatzpflichten resultieren können. Außerdem kommen in diesen Fällen häufig ein Vertrauensverlust, Imageschäden und ggf. Störungen im Betrieb hinzu, die das Schadensausmaß zusätzlich erhöhen. Durch strafverfolgende Institutionen (vor allem Aufsichtsinstitutionen, Staatsanwaltschaft) bzw. Vertragspartner, die ihre Interessen wahren wollen, ergibt sich auch eher die Wahrscheinlichkeit, dass ein Verstoß reklamiert und ein Anspruch verfolgt und durchgesetzt wird.

Bei den externen Regelwerken ist zu beachten, dass diese ggf. aufgrund von Verweis oder Heranziehung zur Auslegung der Rechtsnormen letztlich deren Bindungswirkung und das daraus resultierende Risiko teilen. Die Regelwerke dieser Gruppe erlangen somit dann eine höhere Bindungswirkung, wenn ihre Einhaltung von Dritten (z. B. Wirtschaftsprüfern, Kunden, Interessengruppen) eingefordert wird. Gleiches gilt für die internen Regelwerke, wenn sie eine Übersetzung bzw. Umsetzung der externen Regelwerke und vertraglichen Verpflichtungen beinhalten.

Die Einführung eines IT-Governance-Systems hat nach COBIT 2019 verschiedene situative Einflussfaktoren zu berücksichtigen. Hierzu gehören einerseits Gesetze, regulative Vorgaben, Normen und Industriestandards, andererseits unternehmensinterne Leit- und Richtlinien sowie Verfahrensweisen (vgl. [ISACA 2018d, S. 15]). Zudem stellt die Nichteinhaltung von IT-bezogenen regulatorischen oder vertraglichen Anforderungen einen wichtigen internen Anlass für die Etablierung effektiver Praktiken für IT-Governance und -Management dar (vgl. [ISACA 2018d, S. 26]). Dementsprechend bilden neue Gesetze und regulative Vorgaben einen externen Treiber für IT-Compliance (vgl. [ISACA 2018d, S. 28]).

5.2 Rechtliche Vorgaben

Im Zentrum der rechtlichen Vorgaben stehen Rechtsnormen, also Gesetze und Rechtsverordnungen. In der Praxis sind jedoch Verwaltungsvorschriften, die häufig als regulatorische Vorgaben bezeichnet werden, ebenso wie Verträge wichtige Quellen von Compliance-Anforderungen.

(1) Ausländische Gesetze

Ausländische Gesetze sind immer dann einzuhalten, wenn ein Unternehmen Geschäftsaktivitäten oder gar Niederlassungen im Ausland unterhält. Aus Sicht der kontinentaleuropäischen Rechtssysteme (dem sog. Civil Law) werden die auf Präzedenzfällen und richterlicher Auslegung beruhenden Rechtssysteme des Common Law, die z. B. in den USA, England, Südafrika, Indien und Australien anzutreffen sind, eher als unübersichtlich und deswegen als risikobehaftet empfunden.

Beispiel SOX:

Eine der einflussreichsten Gesetze für die IT-Compliance ist der Sarbanes-Oxley Act (SOX). Es handelt sich hierbei um ein im Jahr 2002 erlassenes US-Bundesgesetz, das infolge diverser Unternehmensskandale bzgl. Manipulationen und Bilanzfälschungen[2] Regelungen für die Corporate Governance von Unternehmen trifft. Es ist für diejenigen Unternehmen relevant, die bei der US-Börsenaufsicht SEC (Security and Exchange Commission) registriert sind – inklusive deren Tochtergesellschaften – sowie deren Wirtschaftsprüfer (nach [Rüter et al. 2006, S. 117]). Deutsche Unternehmen sind betroffen, wenn sie selbst an der SEC registriert sind oder wenn sie Tochtergesellschaft eines bei der SEC registrierten US-Unternehmens sind. Section 404 des SOX schreibt die Implementierung und Bewertung eines internen Kontrollsystems für die Rechnungslegung vor. Da dieses gewöhnlich nicht ohne IT-Kontrollen auskommt, ergeben sich aus SOX indirekt Anforderungen an die IT eines Unternehmens, d. h. an das Konzipieren, Entwickeln, Testen und Überwachen rechnungslegungsrelevanter IT-Kontrollen (nach [Klotz 2012, S. 24f.]).

Als Geschäftsaktivität gilt auch – ohne das Unterhalten von eigenen Niederlassungen – ein Geschäftsverhältnis mit ausländischen Personen. Insbesondere Geschäftsbeziehungen mit US-amerikanischen Kunden führen zu Benachrichtigungspflichten, vor allem bei Sicherheitsproblemen, insbesondere Datenverlust, nach dem Recht der jeweiligen US-Bundesstaaten (Security Breach Notification) (vgl. [Stögmöller 2019, S. 22]).

Eine besondere Herausforderung bei internationaler Geschäftstätigkeit ist der Umgang mit Konflikten zwischen EU-, nationalen und ausländischen gesetzlichen Vorgaben.

Beispiel Freedom Act:

Der USA Freedom Act (Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act) hat im Jahr 2015 den USA Patriot Act abgelöst. Nach diesem US-amerikanischem Bundesgesetz unterliegen auch in Europa gespeicherte Kundendaten von Telekommunikationsunternehmen, Internet Service Provider, Webdiensten u. Ä. aus den USA dem Zugriff der US-Sicherheitsbehörden. Diese Verpflichtung trifft ggf. auch Tochtergesellschaften US-amerikanischer Unternehmen – unabhängig von bzw. im Konflikt mit den Vorgaben der DSGVO zur Datenweitergabe (vgl. [Stögmöller 2019, S. 40f.]).

Internationale Gesetze werden in COBIT 2019 als Teilgruppe der Gesetze angesehen. Ausdrücklich erwähnt werden internationale gesetzliche und regulatorische Vorgaben in der Beschreibung der oben bereits angeführten Managementpraktik MEA03.01. Hier wird gefordert, dass diesbezügliche Änderungen kontinuierlich zu überwachen und daraus Compliance-Vorgaben zu ermitteln sind (vgl. [ISACA 2018b, S. 285]). Dies gilt natürlich ebenso für nationale Gesetze.

(2) Anforderungen auf Grundlage des EU-Rechts

Weiterhin zählen zu dieser Gruppe rechtlicher Vorgaben die Rechtsentwicklungen, die sich auf EU-Ebene vollziehen. Hier sind insbesondere die Datenschutz-Grundverordnung (DSGVO) der EU und Vorschriften zur Finanzaufsicht (BASEL I bis IV, CRD, CRR) relevant. Bei Letzteren ist die Unternehmens-IT dann betroffen, wenn sie im Rahmen des Risikomanagements einen Teil der operationellen Risiken – insbesondere in Form von Prozess-, Technologie- und Systemrisiken – darstellt. Ähnlich verhält es sich mit der viel diskutierten 8. EU-Richtlinie (auch kurz »Euro-SOX« genannt), die in Deutschland durch das Bilanzrechtsmodernisierungsgesetz (BilMoG) umgesetzt wurde. Die Regelungen des BilMoG in Bezug auf Risikomanagement sowie internes Kontroll- und Revisionssystem betreffen auch die IT – vor allem dort, wo der Geschäftsbetrieb kritisch vom Funktionieren der IT abhängt.

Beispiel DSGVO:

Die Datenschutz-Grundverordnung ist nach wie vor ein wesentlicher Treiber für IT-Compliance. Dies liegt vor allem an der beträchtlichen Höhe der Bußgelder. Nach Art. 83 DSGVO sind Geldbußen in Höhe von bis zu 10 bzw. 20 Mio. Euro oder 2 bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs möglich. Diese Größenordnung hat potenziell zumindest erhebliche Auswirkungen auf den Jahresgewinn. Für gewinnschwache Unternehmen könnte eine maximale Strafe durchaus existenzbedrohend werden. Non-Compliance in Bezug auf die DSGVO kann sich somit für Unternehmen als wesentliches Risiko darstellen und muss insofern Gegenstand des Risikomanagements sein.

(3) Nationale Gesetze und Rechtsverordnungen

Die Notwendigkeit zur Einhaltung von Anforderungen an die IT ergibt sich nicht nur aus Gesetzen, die sich schon vom Namen her offensichtlich auf die IT beziehen, wie beispielsweise national das Bundesdatenschutzgesetz oder das Telemediengesetz (TMG). Vielmehr regeln zahlreiche weitere Gesetze den IT-Einsatz im Unternehmen, z. B. BetrVG, StGB sowie hinsichtlich der Buchführungs- und steuerlichen Pflichten HGB und AO nebst Teilen der einzelnen Steuergesetze. Vertragliche Anforderungen sind insbesondere im Bürgerlichen Gesetzbuch (BGB) geregelt.

[2] In den USA waren dies vor allem die Betrugsfälle und Bilanzmanipulationen bei den Firmen Worldcom und Enron, in deren Folge es zu Unternehmenszusammenbrüchen, Strafverfolgungen und Verurteilungen, gar zu Selbstmorden der Verantwortlichen kam.

Beispiel BGB:

Die Bezüge des BGB zur IT sind mittlerweile vielfältig. Vor allem gilt das Kauf- und Gewährleistungsrecht des BGB auch für Softwareerstellung und -kauf. So stellt das Gewährleistungsrecht des BGB sowohl im Kauf- als auch im Werkvertragsrecht in erster Linie auf die vereinbarte Sollbeschaffenheit ab (§§ 437 Abs.1, 633 Abs. 2 BGB), was in Verträgen eine möglichst genaue, ggf. funktionale Leistungsbeschreibung erfordert, deren Einhaltung durch Abgleich mit der tatsächlichen Beschaffenheit der jeweiligen Hard- oder Software zu überprüfen ist.

Für Unternehmen, die zur kritischen Infrastruktur zählen, sind das BSI-Gesetz (BSIG) und die BSI-Kritisverordnung (BSI-KritisV) von Bedeutung.

Beispiel BSIG:

Das BSI-Gesetz regelt in erster Linie die Arbeit des Bundesamtes für Sicherheit in der Informationstechnik. In den §§ 8a-8d sind jedoch bußgeldbewehrte Vorgaben für Unternehmen, die kritische Infrastrukturen betreiben, enthalten. § 8a Abs. 1 BSIG enthält die grundlegende Vorschrift, dass KRITIS-Betreiber »angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen« haben.

Beispiel BSI-KritisV:

Die häufig genannte BSI-Kritisverordnung enthält keine ausdrücklichen Vorgaben an die IT. Sie legt jedoch fest, welche Unternehmen der KRITIS-Branchen als Betreiber einer kritischen Infrastruktur i. S. des BSI-Gesetzes gelten und somit die Vorgaben des BSIG an die IT zu erfüllen haben.

Beispiel ArbStättV:

Dass IT-Compliance auch Felder wie den Arbeitsschutz betreffen kann, zeigt die Arbeitsstättenverordnung (ArbStättV). Sie enthält u. a. Vorgaben für die Arbeit an Bildschirmen und dient damit der Sicherheit und dem Gesundheitsschutz der IT-Nutzer. In einem Anhang sind insgesamt 28 verbindliche Anforderungen an Bildschirmarbeitsplätze, z. B. hinsichtlich Geräten und Arbeitsumgebung, aber auch in Bezug auf die softwareergonomische Gestaltung, formuliert.

Die Identifizierung, Berücksichtigung und Erfüllung gesetzlicher Vorgaben sowie ein entsprechender Nachweis ist in allen fünf Governance- und Management-Domänen zu finden, wie folgende Beispiele zeigen:

- Im Rahmen der Governance-Praktik EDM01.01 (Evaluate the governance system) gehören Gesetze zu den externen Umgebungsfaktoren, die sich auf die Konzeption der Governance auswirken und insofern zu berücksichtigen sind (vgl. [ISACA 2018b, S. 29]). Nach EDM01.03 (Monitor the governance system) ist zu überwachen, inwieweit die IT gesetzlichen Verpflichtungen nachkommt (vgl. [ISACA 2018b, S. 30f.]).
- **APO:** In APO07.04 (Assess and recognize/reward employee job performance) wird gefordert, dass personenbezogene Daten im Rahmen der Mitarbeiterbewertung gemäß datenschutz- und arbeitsrechtlichen Vorgaben genutzt und gespeichert werden (vgl. [ISACA 2018b, S. 101]).
- **BAI:** Nach der Managementpraktik BAI02.01 (Define and maintain business functional and technical requirements) sind Informationskontrollanforderungen in die Geschäftsprozesse, automatisierten Prozesse und IT-Umgebungen zu integrieren, um die gesetzliche Compliance sicherzustellen (vgl. [ISACA 2018b, S. 164]). Weiterhin sind gesetzliche Vorgaben im Rahmen von BAI03.01 (Design high-level solutions) in der Grobkonzeption von IT-Lösungen zu berücksichtigen (vgl. [ISACA 2018b, S. 169]).
- **DSS:** Ein weiterer Bereich, in dem Gesetzeskonformität gefordert wird, ist in der Managementpraktik DSS01.05 (Manage facilities) zu finden. Die Praktiken fordern u.a., dass die IT-Standorte und -Einrichtungen gesetzlichen Vorgaben entsprechen, dass das Personal der Standorte hinsichtlich der Gesetzesanforderungen unterwiesen ist und dass gesetzliche Berichtspflichten bei etwaigen Störungen erfüllt werden (vgl. [ISACA 2018b, S. 233]).
- **MEA:** In MEA03 als zentralem Compliance-Managementziel richten sich alle Praktiken auf die Compliance mit externen Anforderungen, insbesondere mit Gesetzen (aber auch behördlichen und vertraglichen Vorgaben). Wie oben bereits angeführt, sollen durch die Managementpraktik MEA03.01 Gesetzesänderungen und entsprechende gesetzliche Vorgaben identifiziert werden, ggf. mit externer Unterstützung. Hierzu gehört auch die Festlegung der Konsequenzen von Non-Compliance. Nach MEA03.02 (Optimize response to external requirements) ist mittels der Überprüfung und Anpassung von grundsätzlichen Regelungen, Richtlinien, Standards, Verfahren und Methoden sicherzustellen, dass gesetzliche Anforderungen erfasst und kommuniziert werden. Die entsprechende Compliance wird im Rahmen von MEA03.03 (Confirm external compliance) bestätigt. Schließlich richtet sich MEA03.04 (Obtain assurance of external compliance) auf die Einforderung von Erklärungen seitens beauftragter IT-Serviceanbieter und sonstiger Geschäftspartner dahingehend, dass diese die relevanten gesetzlichen Vorgaben erfüllen (vgl. [ISACA 2018b, S. 285]).

Soweit einzelne Rechtsbereiche in COBIT 2019 ausdrücklich angesprochen werden, sind dies gesetzliche Vorgaben zur Beachtung geistigen Eigentums, zum Arbeitsrecht, zum Gesundheit- und Arbeitsschutz sowie zum Datenschutz. Wo in den Praktiken derartige Angaben erfolgen, ist dies weniger als systematische Auflistung, sondern eher exemplarisch zu verstehen.

→

(4) Rechtsprechung

Zu den rechtlichen Vorgaben zählt weiterhin die Rechtsprechung, die die Rechtsnormen auslegt und damit wesentlich deren Inhalt bestimmt. Dies betrifft in besonderem Maße sogenannte unbestimmte Rechtsbegriffe bzw. Generalklauseln. Beispiele hierfür sind die »übliche Beschaffenheit« (§ 434 Abs. 1 Nr. 2 BGB), die das Vorliegen eines Mangels im Werkvertragsrecht bestimmt, oder die »im Verkehr erforderliche Sorgfalt« (§ 276 Abs. 2 BGB), deren Missachtung den Vorwurf fahrlässigen Verhaltens begründet.

Beispiel OLG Hamm:

Das Oberlandesgericht Hamm hat eine unterlassene Datensicherung bei Schäden, die durch Datenverluste infolge von Programmfehlern entstehen, als Mitverschulden gewertet. In dem entschiedenen Fall hatte dies zur Folge, dass die Geltendmachung von Schadensersatzansprüchen verhindert wurde. Die Richter gingen davon aus, dass eine Sicherung täglich, eine Vollsicherung mindestens einmal wöchentlich zu erfolgen habe (nach [OLG Hamm 2003]).

Dass die Rechtsprechung in COBIT 2019 nicht explizit als Quelle von Compliance-Vorgaben erwähnt wird, verwundert nicht, da das angloamerikanisch »case law« schon begrifflich beim Bezug auf Gesetze (law) erfasst ist.

(5) Verwaltungsvorschriften

Auch ohne dass es sich um Rechtsnormen im engeren Sinne handelt, sind für IT-Compliance ferner Regelwerke relevant, die von den zuständigen Behörden (insb. Aufsichtsinstitutionen) zur Interpretation und Ausführung der Rechtsnormen aufgestellt oder erklärtermaßen herangezogen werden. Verwaltungsvorschriften werden mit unterschiedlichen Bezeichnungen tituliert, z. B als Report, Leitlinien oder einfach nur (Rund-)Schreiben. Derartige Regelwerke bewirken rechtlich eine Selbstbindung der Verwaltung, indem sie die Anwendung der Rechtsnormen durch die Verwaltung bestimmen.

Beispiel GoBD:

Die »Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff« wurden vom Bundesministerium für Finanzen mittels eines Schreibens an die obersten Finanzbehörden der Länder als Verwaltungsanweisung erlassen. Sie interpretieren die Regelungen der Abgabenordnung zu den Anforderungen an die ordnungsgemäße Buchführung beim Einsatz IT-gestützter Buchhaltungssysteme und bei Verwendung digitaler Unterlagen.

Da Aufsichtsinstitutionen in ihrer Überwachung auf Branchen ausgerichtet sind, zeichnen sich die betroffenen Branchen im Vergleich zu anderen durch eine intensivere Regulierung aus. So sind beispielsweise im Finanzdienstleistungssektor die regulativen Vorgaben äußerst zahlreich. Hier sind auf europäischer Ebene die verschiedenen Guidelines der European Banking Authority (EBA) maßgebend. Beispiele für Guidelines, die sich unmittelbar an die IT richten, sind die »EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)« (EBA/GL/2017/05) und die »EBA Guidelines on ICT and security risk management« (EBA/GL/2019/04).

Beispiel EBA/GL/2017/05:

Die »Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)« (EBA/GL/2017/05) beschreiben, wie Prüfer der Aufsichtsbehörden unter anderem die IT-Strategie und die IT-Governance bei Finanzinstituten prüfen und bewerten sollen und welche IT-Risiken mindestens zu berücksichtigen sind.

National sind vor allem die »Mindestanforderungen an das Risikomanagement« (MaRisk) und die »Bankaufsichtlichen Anforderungen an die IT« (BAIT) sowie die »Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen« (MaGo) und die »Versicherungsaufsichtlichen Anforderungen an die IT« (VAIT) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) von Bedeutung. Hierbei werden die in den jeweiligen Mindestanforderungen genannten Vorgaben an die IT in Finanzdienstleistungsunternehmen durch die wesentlich umfangreicheren Ausführungen der BAIT bzw. VAIT konkretisiert.[3]

Verwaltungsvorschriften werden in COBIT 2019 mit dem Begriff »regulations« adressiert. Sie werden i. d. R. gemeinsam mit Gesetzen angesprochen.

(6) Referenzierte Regelwerke

Regelwerke, die als solche keinen Rechtsnormcharakter haben und sowohl von Verwaltungen wie auch von privatrechtlichen Institutionen (z. B. dem DIN, Deutsches Institut für Normung) stammen können, haben für die IT-Compliance die gleiche Bedeutung wie Rechtsnormen, wenn sie durch ausdrückliche Verweisung in diese einbezogen werden.

Beispiel MaRisk:

Die den »Mindestanforderungen an das Risikomanagement« zugehörige Erläuterung verweist auf die vom BSI herausgegebenen IT-Grundschutzkataloge und die ISO-27000-Reihe (vgl. [BaFin 2017a, S. 28]). Dies hat zur Folge, dass Kreditinstitute, um keinen Beanstandungen der BaFin ausgesetzt zu sein, ein Sicherheitsniveau entsprechend den IT-Grundschutzkatalogen oder der ISO-27000-Reihe realisieren müssen.

[3] Vgl. [BaFin 2018c], S. 28. Für einen Überblick zu den BAIT s. [Terwort/Wilop 2018], zu den VAIT s. [Reffgen 2019].

5.3 Verträge

Vertragsverstöße stellen für ein Unternehmen operationelle Risiken dar, die es mittels einer effektiven und effizienten Vertragssteuerung zu managen gilt. Zwei Gruppen von Verträgen sind hier von Bedeutung:

- Verträge allgemeiner Art, deren Vertragsgegenstand sich nicht auf IT-Belange konzentriert, die aber einzelne IT-relevante Regelungen enthalten (beispielsweise zum Austausch oder zur Aufbewahrung von Informationen) oder die dem Vertragsdokument als IT-Objekt einen schutzwürdigen Status zuerkennen (was gewöhnlich durch eine Geheimhaltungsvereinbarung geschieht);
- spezifische IT-Verträge, deren Vertragsgegenstand sich auf IT-Leistungen bezieht und die dadurch direkt relevant sind für IT-Compliance, z. B. Beschaffungsverträge für Hardware, Lizenzverträge für Software, aber auch IT-System- und IT-Versicherungsverträge.

Bei Verträgen allgemeiner Art stehen aus Compliance-Sicht nur diejenigen vertraglichen Vereinbarungen im Fokus, aus denen sich IT-spezifische Pflichten und Obliegenheiten des Unternehmens als Vertragspartner ergeben. Dagegen hat eine IT-Vertrags-Compliance bei spezifischen IT-Verträgen sicherzustellen, dass alle »Vertragsleistungen den – während der Vertragsdurchführung mitunter auch aktualisierten – Zielsetzungen des Leistungsempfängers entsprechen und dass die im Vertrag vereinbarten Haupt- und Nebenpflichten von beiden Vertragsseiten während der Vertragslaufzeit und ggf. auch danach erfüllt werden« [Klotz/Dorn 2016, S. 110]. Operativ richtet sich die Compliance-Aufgabe bei Verträgen, die vom Vertragspartner im Rahmen eines Projektes im Unternehmen durchgeführt werden, z. B. auf die Einhaltung bestimmter End- und Zwischentermine (Meilensteine), die Erfüllung von Mitwirkungs- und Dokumentationspflichten sowie von Geheimhaltungsabreden (vgl. [Klotz/Dorn 2016, S. 112]). In Bezug auf das Risikomanagement stehen solche Regelungen im Vordergrund, aus denen sich Risiken hinsichtlich potenzieller Fristsetzungen (Inverzugsetzung) sowie hohe Schadensersatzansprüche bei Nicht- oder Schlechtleistung oder sonstigen Sachverhalten mittels vereinbarter Vertragsstrafen ergeben.

IT-Vertrags-Compliance spielt einerseits im IT-Projektmanagement eine wichtige Rolle, vor allem in größeren Projekten, die für das Unternehmen von geschäftskritischer Bedeutung sind. Andererseits bilden Verträge aber auch die formale Grundlage für den IT-Betrieb, wobei das Spektrum von der Beschaffung einzelner Komponenten der IT-Infrastruktur über IT-Beratung und Einzelaufträge, z. B. in der Auftragsentwicklung von Applikationen, bis hin zu komplexen Vertragswerken, wie sie vor allem beim IT-Outsourcing erforderlich sind, reicht.

Auch Verträge werden in COBIT 2019 i. d. R.gemeinsam mit Gesetzen genannt. Aufgrund der Bedeutung von Verträgen finden sich jedoch auch spezielle Managementpraktiken. So soll APO07.06 (Manage contract staff) sicherstellen, dass beauftragtes Personal einerseits die Richtlinien der Organisation kennt und einhält, andererseits die vereinbarten vertraglichen Anforderungen erfüllt (vgl. [ISAC 2018b, S. 101]). Dementsprechend ist im Rahmen des Vertragsmanagements – beschrieben in APO10.03 (Manage vendor relationships and contracts) – zu gewährleisten, dass neue oder geänderte Verträge mit Unternehmensstandards sowie gesetzlichen und behördlichen Anforderungen übereinstimmen (vgl. [ISACA 2018b, S. 120]). Die Überwachung von Verträgen sollte Bestandteil einer IT-Beschaffungsrichtlinie sein (vgl. [ISACA 2018b, S. 123]). Insbesondere das Management kritischer Betriebsmittel (BAI09.02 Manage critical assets) muss auf formalen Dienstleistungsverträgen beruhen, die den Sicherheits-/Datenschutzrichtlinien und -standards der Organisation entsprechen (vgl. [ISACA 2018b, S. 210]). Ähnlich verhält es sich mit DSS01.02 (Manage outsourced I&T services), wo dafür zu sorgen ist, dass die mit Dritten abgeschlossenen Verträge bzgl. Hosting oder Bereitstellung von Services und SLAs eingehalten werden (vgl. [ISACA 2018b, S. 232]). Dementsprechend wird von COBIT 2019 das Scheitern von externen Dienstleistern, Projekte gemäß den vertraglichen Vereinbarungen durchzuführen, als ein exemplarisches Risikoszenario für die Risikokategorie »Lebenszyklusmanagement von Projekten und Programmen« genannt (nach [ISACA 2018c, S. 23]). Hinsichtlich des Lizenzmanagements ist nach COBIT 2019 sicherzustellen, dass die Methode zur Messung der Lizenzeinhaltung mit den Anforderungen des Lizenzvertrags übereinstimmt (nach [ISACA 2018b, S. 212]).

5.4 Unternehmensexterne Regelwerke

Die Spannbreite in der Gruppe der unternehmensexternen Regelwerke reicht von Richtlinien supranationaler Organisationen, wie der OECD (Organisation for Economic Co-operation and Development), über Kodizes, nationale und internationale Normen, Standards internationaler und nationaler Verbandsorganisationen und behördlicher Einrichtungen bis hin zu Empfehlungen oder Konzepten, die sich über die Zeit durch Informations- und Erfahrungsaustausch in der Fachwelt herausgebildet haben.

Beispiel OECD-Richtlinien zum Digital Security Risk Management:

Die OECD-Publikation »Digital Security Risk Management for Economic and Social Prosperity« fordert auch von Unternehmensleitungen, einem Ansatz für das Management digitaler Sicherheitsrisiken zu folgen, der zur Vertrauensbildung beiträgt und die Vorteile eines offenen digitalen Umfelds für wirtschaftlichen und sozialen Wohlstand nutzt. Dieser von der OECD formulierte Ansatz besteht aus acht miteinander verbundenen, voneinander abhängigen und sich ergänzenden Governance- und Managementprinzipien [OECD 2015, S. 3f.].

COBIT 2019 sieht sich als Framework, das sich an den relevanten, wichtigen Normen, Standards und Vorschriften ausrichtet (vgl. [ISACA 2018a, S. 18]). Insofern referenziert COBIT über 30 dieser Regelwerke.[4] Der Verweis erfolgt jeweils am Ende einer Beschreibung der Governance- und Managementzielsetzungen.

IT-Compliance ist Teil der Corporate Compliance, die wiederum einen Verantwortungsbereich der Corporate Governance ausmacht. Insofern sind für IT-Compliance auch immer übergeordnete Regelwerke zu Governance und Unternehmensüberwachung und Risikomanagement relevant. Auf internationaler Ebene sind dies die G20/OECD-Grundsätze der Corporate Governance, auf nationaler Ebene der DCGK.

Hinsichtlich Governance verweist COBIT 2019 auf den hierzulande eher weniger diskutierten südafrikanischen Governance-Kodex »King IV Report on Corporate Governance™«. Bezüglich Unternehmensüberwachung bzw. Risikomanagements wird das COSO ERM Framework berücksichtigt.

Von hoher praktischer Bedeutung sind diejenigen Regelwerke, die in der IT-Praxis als »Framework«, »Referenzmodell« oder »Best-Practice-Modell« bezeichnet werden. Zum einen handelt es sich vor allem um die verbreiteten Standards für IT-Governance und IT-Management, wie vor allem CMMI® (Capability Maturity Model Integration), ITIL® und COBIT.

Beispiel ITIL®:

Der wohl am weitesten verbreitete Standard im Bereich der Unternehmens-IT dürfte die »IT Infrastructure Library®« sein. Sie richtet sich auf die Planung, den Betrieb und die Steuerung von IT-Services und bildet insofern den zentralen Standard für das IT-Servicemanagement (ITSM). Entwickelt wurde ITIL® durch eine IT-Dienstleistungsorganisation der britischen Regierung, die Central Computer and Telecommunications Agency (CCTA). Mittlerweile wurden die Rechte vom Cabinet Office der britischen Regierung auf das Unternehmen »Axelos Limited« übertragen. Mit der dritten Version (ITIL® V3) öffnete sich der Standard auch übergeordneten Fragestellungen der strategischen Ausrichtung von IT-Services, der verstärkten Kundenorientierung, dem Nachfragemanagement und der kontinuierlichen Verbesserung der Leistungserbringung. Insofern werden zumindest Teilbereiche der IT-Governance, der IT-Compliance und des IT-Risikomanagements adressiert.

ITIL® versteht sich als Best-Practice-Sammlung. Eine Zertifizierungsmöglichkeit gibt es auf einer individuellen Ebene bzw. institutionell nach ISO 20000. Heute besteht die ITIL®-»Bewegung« aus allen Ingredienzen eines professionellen Managementkonzeptes: Trainingsangebote inkl. qualifizierter Zertifikatsabschlüsse, Beratung und unabhängiger Erfahrungsaustausch innerhalb spezieller Organisationen, Umsetzungshilfen und Softwaretools.

ITIL® wird in COBIT 2019 recht umfangreich referenziert. Von CMMI® werden dagegen lediglich die Cybersecurity Platform – hier handelt es sich um ein Risk Assessment Framework – und ein Reifemodell für das Datenmanagement berücksichtigt, nicht aber die weitverbreiteten CMMI®-Referenzmodelle für IT-Services, -Beschaffung und -Entwicklung. Weiterhin finden u. a. der Architekturstandard TOGAF®, das Kompetenzmodell SFIA® und der Standard für Informationssicherheit des Information Security Forum (ISF) Verwendung.

Zum anderen sind Normen nationaler und internationaler Normungsorganisationen von Bedeutung. Hierzu gehören sowohl spezialisierte IT-Normen, wie die ISO/IEC 27001 oder die ISO/IEC 38500, als auch generelle Normen, wie die ISO 19600 (Compliance-Management-Systeme) oder die ISO 31000 (Risikomanagement), die auch auf die Unternehmens-IT angewendet werden können. Hierbei ist zwischen »zertifizierbaren« Normen und nicht zertifizierbaren Normen zu unterscheiden.

Beispiel ISO/IEC 27001:

Die ISO/IEC 27001 als wohl bedeutendste Norm für Informationssicherheitsmanagementsysteme (ISMS) beschreibt Anforderungen für eine systematische Erstellung, Umsetzung, Dokumentation, Ausführung, Überwachung und Weiterentwicklung von ISMS. Die Verantwortung des Managements, z. B. für eine grundlegende Verpflichtung auf Informationssicherheit oder für die Bereitstellung von Ressourcen, wird in einem eigenen Kapitel herausgestellt. Die Norm legt Wert auf eine kontinuierliche Verbesserung des ISMS. Hierfür bilden ISMS-Audits und Managementbewertungen des ISMS die Grundlagen. Ein Anhang enthält normative Vorgaben für Maßnahmen zur IT-Sicherheit, die in der Praxis weite Verbreitung gefunden haben (vgl. [Bitkom/DIN 2020].

Beispiel ISO/IEC 38500:

Die ISO/IEC 38500 beinhaltet ein Referenzmodell für die IT-Governance, das auf dem Corporate-Governance-Verständnis des Cadbury-Reports und den Corporate-Governance-Grundsätzen der OECD beruht. Nach der ISO/IEC ist »Corporate Governance of IT« das System, durch das die aktuelle und künftige Nutzung der IT geleitet und bedarfsgerecht gesteuert wird. Im Vordergrund steht der planvolle Einsatz der IT, der an den Unternehmenszielen und der daraus abgeleiteten IT-Strategie ausgerichtet sein soll. Die Norm beschreibt ein grundlegendes Modell der IT-Governance, das im Rahmen von sechs Prinzipien (Verantwortlichkeit, Strategie, Beschaffung, Performanz, Konformität[5], Verhalten) Zielsetzungen guter IT-Governance postuliert.

[4] Die Auflistung der bei der Entwicklung von COBIT 2019 genutzten Regelwerke findet sich in [ISACA 2018a, S. 63f.].

[5] Statt »Compliance« verwendet die ISO/IEC 38500 den Begriff »Conformance«. Eine Übersicht über die Norm, die sich mittlerweile zur Normenreihe weiterentwickelt hat, geben die beiden Aufsätze [Klotz 2008] und [Klotz 2016a].

COBIT 2019 bezieht neben der US-amerikanischen Projektmanagement-Norm »PMBOK® Guide« eine ganze Reihe von Richtlinien des NIST, der US-amerikanischen Normungsorganisation, zu IT-Sicherheits- und -Risikomanagement ein, insbesondere das »Framework for Improving Critical Infrastructure Cybersecurity«.[6] Weiterhin finden die ISO/IEC 20000-1 für IT-Servicemanagement, mehrere IT-Sicherheitsnormen der Normenreihe ISO/IEC 27000ff. sowie die ISO/IEC 38500 Berücksichtigung.

Aus Sicht der IT-Compliance sind zudem Regelwerke von hoher Relevanz, die als Basis für interne Prüfungen[7] sowie externe Testierungen oder Zertifizierungen dienen. Hierzu zählen neben der ISO/IEC 27001 vor allem die Prüfungsstandards zur Internen Revision sowie die Prüfungsstandards des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW PS), z. B. der IDW PS 860.[8] In jüngster Zeit werden die Standards des IDW durch internationale Standards ersetzt, wie z. B. durch den ISAE 3000 (revised) und den ISAE 3402. Aber auch umgekehrt werden internationale Standards an nationale Belange angepasst, wie es z. B. für die ISA [DE] 315 und ISA [DE] 330 der Fall ist.

Beispiel IDW PS 860:

Der Prüfungsstandard IDW PS 860 (IT-Prüfung außerhalb der Abschlussprüfung) richtet sich an Unternehmen, die die Ordnungsmäßigkeit, die Sicherheit, das Risikomanagement oder auch die Compliance ihrer IT-Systeme und -Prozesse außerhalb der Abschlussprüfung sicherstellen wollen. Die Prüfung kann als Angemessenheitsprüfung oder als Wirksamkeitsprüfung erfolgen (nach [IDW PS 860, Tz. 14]). Ein wesentlicher Nutzen besteht darin, die Ergebnisse der Prüfung extern gegenüber Dritten, z. B. Geschäftspartnern, oder intern gegenüber einem Aufsichtsgremium zu dokumentieren.

Prüfungsstandards richten sich in erster Linie an die externen Jahresabschlussprüfer. Allerdings können Unternehmen ihnen damit auch Hinweise entnehmen, über welche Strukturen, Prozesse, Konzepte etc. die Unternehmens-IT verfügen sollte. Gleiches gilt auch die die Stellungnahmen zur Rechnungslegung des IDW-Fachausschusses für Informationstechnologie IDW RS FAIT 1 bis FAIT 5.

Als grundlegende Prinzipien der internen Prüfung berücksichtigt COBIT 2019 die »Core Principles for the Professional Practice of Internal Auditing« des Institute of Internal Auditors® (IIA®).

5.5 Unternehmensinterne Regelwerke

Bei unternehmensinternen Regelungen ist die Bindungswirkung auf dasjenige Unternehmen beschränkt, das die jeweilige Regelung in Kraft setzt. Beispiele für unternehmensinterne Regelungen aus dem IT-Bereich sind interne IT-Richtlinien oder -Verfahrensvorgaben zur IT-Sicherheit (z. B. IT-Sicherheitsvorschriften, E-Mail-Richtlinien, Regelungen zum Umgang mit Passwörtern etc.). Aber auch zwischen der IT-Abteilung und den Fachabteilungen vereinbarte Service Level Agreements zählen zu dieser Gruppe. In diesem Zusammenhang sind auch Betriebsvereinbarungen zu beachten, die neben gesetzlichen Normen ebenfalls rechtliche Wirkung entfalten.

Interne Regelwerke sind in zweierlei Hinsicht für IT-Compliance relevant. Zum einen dienen sie in vielen Fällen dazu, die Beachtung der Anforderungen aller anderen Regelwerke sicherzustellen, indem sie verständliche und konkrete Handlungsanweisungen für die Organisationsmitglieder vorgeben. Zum anderen dokumentieren das Vorliegen interner Regelwerke, ihre Verfügbarkeit an zentraler Stelle und ihre Kommunikation mittels Awareness-Maßnahmen nach außen, dass externen Verpflichtungen, insbesondere rechtlichen Vorgaben, nachgekommen wird. Damit können sie im Streitfall ggf. als Indiz für die Erfüllung von Sorgfaltspflichten dienen.

Häufig angesprochen werden in COBIT 2019 Guidelines. Viele der Vorgaben bzgl. Gesetzen und Verträgen richten sich ebenso an interne Richtlinien. So sind die Mitarbeiter im Rahmen der Governance-Praktik EDM01.02 (Direct the Governance System) anzuweisen, Richtlinien für ethisches und professionelles Verhalten zu befolgen, und es ist sicherzustellen, dass die Folgen mangelnder Compliance mit diesen Richtlinien bekannt sind und durchgesetzt werden (nach [ISACA 2018b, S. 30]). Auch die Überwachung des IT-Governance-Systems hat in EDM01.03 (Monitor the Governance System) die Befolgung interner Richtlinien zum Ziel (vgl. [ISACA 2018b, S. 31]).

Ausdrücklich fordert COBIT 2019 die Einhaltung einer ganzen Reihe interner Richtlinien, die in den Beschreibungen der IT-Governance- und IT-Managementzielsetzungen in der Komponente »Policies and Procedures« aufgeführt werden:

- Richtlinie für Budgetierung und Durchführung des Investitionsprogramms
- IT-Beschaffungsrichtlinie
- Eskalationsrichtlinie für Stakeholder-Kommunikation
- Operative Organisationsrichtlinien
- Richtlinien für Datenmanagement, insbesondere Datenschutz, Datenklassifizierung, Datensicherheit und -kontrolle, Datenbereinigung, Datenqualität
- Richtlinie für Informationssicherheit
- Richtlinie zur Steuerung von Business/IT-Beziehungen
- Richtlinie zum Management externer IT-Services
- Richtlinie zum Verfügbarkeitsmanagement

→

6 Für eine Einführung in dieses Framework s. [Kochanek 2018].
7 Ein Überblick über Standards in der IT-Revision ist zu finden in [ISACA-FG IT-Revision 2015].
8 Eine kompakte Beschreibung der IT-Prüfungen nach IDW findet sich in [Nestler/Modi 2019, S. 54-58].

- Richtlinie zum Asset-Management
- Richtlinie zum geistigen Eigentum (IP)
- Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs
- Richtlinie zum Krisenmanagement

Inhaltlich weiter ausgeführt werden die Richtlinie zum Datenschutz und die Compliance-Richtlinie.

- Die Richtlinie zum Datenschutz definiert, wie ein Unternehmen personenbezogene Daten sammelt, speichert und freigibt; wie und wann der Kunde über bestimmte Daten informiert wird, und ob diese vertraulich behandelt, mit Partnern geteilt oder an andere Firmen oder Unternehmen verkauft werden. Hierbei schreibt die Richtlinie insbesondere die Einhaltung der Gesetzgebung zum Datenschutz vor (nach [ISACA 2018b, S. 149]).
- Die Compliance-Richtlinie beinhaltet Festlegungen zur Identifizierung gesetzlicher, regulatorischer, vertraglicher und interne Compliance-Anforderungen. Sie beschreibt den Prozess zur Bewertung der Compliance mit regulatorischen, vertraglichen und internen Anforderungen und listet Rollen und Zuständigkeiten für verschiedene Aktivitäten im Prozess auf. Sie legt Kennzahlen zur Bewertung der Compliance fest. Weitere Festlegungen betreffen das Compliance-Berichtswesen sowie die Bestätigung von Compliance- oder Korrekturmaßnahmen zur rechtzeitigen Behebung von Compliance-Defiziten [ISACA 2018b, S. 288].

Handlungsempfehlungen

- Klären Sie, wie das »House of IT Compliance« für Ihr Unternehmen aufgebaut ist.
- Analysieren Sie Risiken und Verbindlichkeit der einzelnen Regelwerke.
- Identifizieren Sie die gesetzlichen und regulatorischen Verpflichtungen, denen Ihr Geschäft in allen Aspekten (Produkte, Märkte, Regionen etc.) unterliegt.
- Ziehen Sie Standards und Normen dort her, wo sie – ggf. aufgrund von Zertifizierungen oder Vorgaben des Marktes – verbindlich sind.
- Nutzen Sie Standards und Normen in Ihrem IT-Management weiterhin dort, wo Ihr Unternehmen Nachteile gegenüber dem Wettbewerb hat.
- Sorgen Sie für eine Umsetzung externer Regelwerke, indem Sie wichtige Anforderungen in interne Regelwerke aufnehmen.
- Behalten Sie die Übersicht über die Anforderungen aus internen und externen Regelwerken sowie rechtlichen Vorgaben.
- Führen Sie ein Register der für Ihr Unternehmen relevanten Regelwerke.
- Sorgen Sie für eine Archivierung der nicht mehr aktuellen Versionen.
- Dokumentieren Sie die Compliance mit allen Anforderungen zeitnah und nachvollziehbar.

6 Organisation der IT-Compliance

6.1 Ebenenmodell der IT-Compliance-Organisation

Die Eingliederung der IT-Compliance in die hierarchische Ordnung des Unternehmens richtet sich auf die Übertragung von IT-Compliance-Aufgaben sowie eine entsprechende Zuweisung von Befugnissen und Verantwortung an die Beteiligten. Es geht hierbei nicht nur um die Etablierung einer Abteilung oder einer Stelle mit der Bezeichnung »IT-Compliance« bzw. die Einrichtung einer Position »IT-Compliance-Manager«. Vielmehr ist für die Sicherstellung von IT-Compliance eine umfangreiche Zusammenarbeit zu organisieren, die über unterschiedliche hierarchische Ebenen von der Unternehmensleitung bis auf die operative Ebene zentrale und dezentrale Strukturen verbinden und hierbei auch organisatorische Schnittstellen zwischen IT-Funktion und Fachabteilungen klären muss.

Grundlage für die aufbauorganisatorische Einordnung der IT-Compliance ist die Frage, wie die Corporate Compliance im Unternehmen strukturiert ist, insbesondere wie hier zentrale und dezentrale Strukturen etabliert und zueinander ausgerichtet sind. Vor allem Unternehmen mit einer umfangreichen räumlichen Verteilung ihrer Unternehmenseinheiten werden nicht umhinkommen, eine diesbezüglich ausgewogene Lösung zu etablieren. Das Grundmodell der IT-Compliance-Organisation besteht dann zumindest aus drei Ebenen (vgl. Abbildung 6–1).

- **Ebene 1:** Der Unternehmensleitung obliegt die Letztverantwortung für IT-Compliance als Teil der Gesamtverantwortung für Compliance. Dies umfasst insbesondere die erforderliche, geeignete und angemessene Ausgestaltung der gesamten Compliance-Struktur des Unternehmens (inkl. IT-Compliance).
- **Ebene 2:** Der IT-Compliance im Rahmen der Corporate Compliance kommt eine Schnittstellen- und Steuerungsfunktion für IT-Compliance zu. Sie agiert im Rahmen der zentralen Compliance-Funktion. Wahrgenommen wird diese Funktion von einem IT-Compliance-Manager.
- **Ebene 3:** Die dezentrale IT-Compliance in den Unternehmensfunktionen wird von dezentralen Compliance-Stellen mit bereichsbezogener Verantwortung für IT-Compliance gebildet. Sie müssen im Wesentlichen IT-Compliance-Probleme ihres Verantwortungsbereichs identifizieren, ihre Reaktion dokumentieren und an den IT-Compliance-Manager berichten (in Anlehnung an [Bürkle 2016, S. 1157ff.]).

Die Verantwortung der Unternehmensleitung für IT-Compliance als Teil der Corporate Compliance insgesamt ergibt sich aus den Sorgfaltspflichten der Unternehmensleitung, bei einer AG aus § 93 Abs. 1 AktG bzw. bei einer GmbH aus § 42 Abs. 1 GmbHG. Konkret liegt damit bei der Unternehmensleitung die Gesamtverantwortung für die Sicherstellung von Compliance mittels der Initiierung, Konzeption, Implementierung, Überwachung und Weiterentwicklung des unternehmensweiten Compliance-Management-Systems. Immer mehr

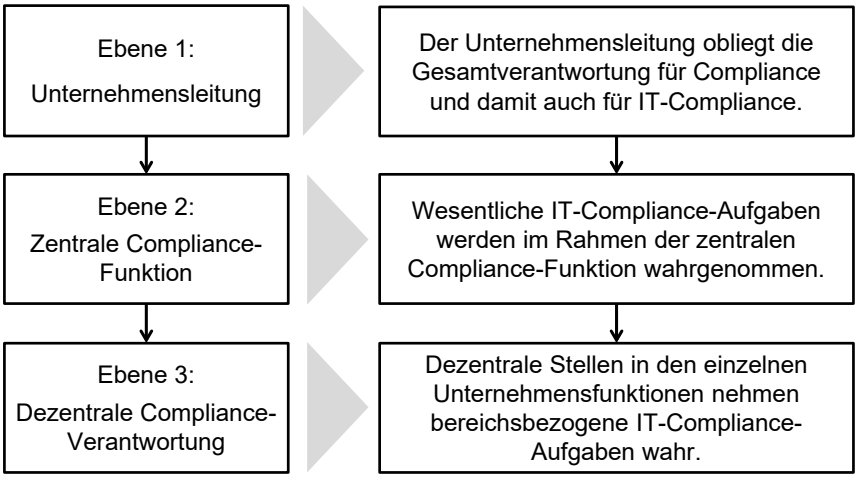


Abb. 6–1: Drei-Ebenen-Modell der IT-Compliance-Organisation (nach [Klotz 2020, S. 876])

Unternehmen gehen dazu über, ein Compliance-Ressort in der Unternehmensleitung zu verankern, wobei das betreffende Mitglied der Unternehmensleitung dann von einem Corporate bzw. Chief Compliance Officer (CCO) unterstützt wird. Ist ein solches Ressort in der Unternehmensleitung vorhanden, wäre hier auch die Anbindung von IT-Compliance an der Unternehmensspitze zu verorten. Hinzu kommt, dass allen Mitgliedern einer Unternehmensleitung eine Gesamtverantwortung zukommt. Insofern zeichnet ggf. auch das für die IT verantwortliche Mitglied der Unternehmensleitung (d. h. der CIO) für IT-Compliance mitverantwortlich.

Für die Unternehmensleitung (Board) bzw. die C-Ebene, d. h. CEO, CFO, COO und CIO, prägt sich die Compliance-Verantwortung nach COBIT© 2019 zum einen in der IT-Governance-Domäne EDM, zum anderen in der Management-Domäne MEA aus. Gemäß den Governance-Praktiken EDM01.01 und EDM01.03[1] hat die Unternehmensleitung (ggf. auch ein Aufsichtsorgan) darüber Rechenschaft abzulegen, dass

- die rechtlichen, regulatorischen u. vertraglichen Verpflichtungen und Compliance-Trends im Geschäftsumfeld analysiert und identifiziert werden,
- externe Vorschriften, gesetzliche und vertragliche Verpflichtungen berücksichtigt und ihre Anwendung im Rahmen der IT-Compliance festgelegt wird,
- überwacht wird, inwieweit die IT ihren Verpflichtungen (Regulierungsvorgaben, Gesetzen, Verträgen), internen Richtlinien, Normen/Standards und professionellen Leitlinien nachkommt,
- überwacht wird, inwieweit reguläre und routinemäßige Mechanismen sicherstellen, dass die IT-Nutzung den einschlägigen Verpflichtungen (Regulierungsvorgaben, Gesetzen, Verträgen), Normen und Standards sowie Richtlinien entspricht.[2]

In MEA richtet sich die Verantwortung der Chief-Ebene im Wesentlichen auf die Managementpraktiken »Optimieren der Reaktion auf externe Anforderungen« (MEA03.02) und »Überprüfen der externen Compliance« (MEA03.03). Nur der CIO ist zudem noch für die Durchführung der Managementpraktiken »Identifizieren externer Compliance-Anforderungen« (MEA03.01) und »Erhalten von Compliance-Bestätigungen« (MEA03.04) mit verantwortlich (vgl. [ISACA 2018b, S. 287]).

Die zweite Ebene der IT-Compliance-Organisation ergibt sich durch die Wahrnehmung wesentlicher Aufgaben der IT-Compliance im Rahmen der Corporate Compliance. Ob in dieser zentralen Compliance-Funktion eine oder mehrere Stellen oder gar eine Abteilung für IT-Compliance einzurichten sind bzw. ist, hängt von den situativen Bedingungen des Unternehmens ab. Vor dem Hintergrund der digitalen Transformation der Wirtschaft dürften umfangreichere Strukturen für IT-Compliance eher kurzfristig notwendig werden.

Bei einer aufbauorganisatorischen Integration von IT-Compliance in die Corporate Compliance würde sich somit eine hierarchische Anbindung als Linienstelle mit mittelbarer oder unmittelbarer Zuordnung zum CCO ergeben. Eine Alternative könnte die Zuordnung der zentralen IT-Compliance zum Chief Information Officer sein, wobei diese Lösung eher als Stabstelle ausgeprägt sein und die Compliance der IT-Funktion im Vordergrund stehen würde.

Die zentralen IT-Compliance-Aufgaben richten sich auf die Unterstützung des CCO bzw. des CIO in allen IT-Compliance-relevanten Fragen sowie die Gestaltung und Weiterentwicklung des Managementsystems für IT-Compliance. Weiterhin kommen folgende IT-Compliance-Aufgaben infrage (in Anlehnung an [Klotz 2020, S. 876f.]):

(1) Koordination bzgl. übergreifender Compliance-Fragen
(2) Kommunikation mit externen Stellen, vor allem externen IT-Auditoren und IT-Beratern
(3) Identifizierung wesentlicher IT-Compliance-Anforderungen an das Unternehmen
(4) Initiierung der Analyse des Regelungsbedarfs hinsichtlich IT-Compliance und Steuerung der Umsetzung in Richtlinien, Verfahrensanweisungen etc.
(5) Bestimmung fachbereichsübergreifender IT-Compliance-Risiken, inkl. Abstimmung mit IT-Risikomanagement und IT-Sicherheitsmanagement
(6) Einleitung fachbereichsübergreifender IT-Compliance-Maßnahmen und Überwachung ihrer Ausführung
(7) Realisierung von Synergien aus der Konsolidierung dezentraler IT-Compliance-Maßnahmen
(8) Konzeption und Weiterentwicklung des IT-Compliance-Managementsystems und Koordination und Dokumentation der Umsetzung des IT-Compliance-Management-Systems
(9) Sicherstellen von Compliance-Information und -Kommunikation (IT-Compliance-Berichtswesen)
(10) Steuerung der dezentralen IT-Compliance-Stellen
(11) Entgegennahme und Konsolidierung der Berichte seitens der dezentralen IT-Compliance-Stellen und Berichterstattung an den CCO bzw. den IT-Compliance-Ausschuss
(12) Initiierung und Steuerung von Konzeption und Betrieb eines Überwachungssystems zur Einhaltung der IT-Compliance-Anforderungen
(13) Mitwirkung an der Aufdeckung von Non-Compliance sowie Initiierung und Überwachung von Maßnahmen zur Ursachenanalyse und Schadensminderung

Die Organisationseinheit »Compliance« ist in COBIT© 2019 nur in der Managementpraktik MEA03 in einer verantwortlichen Rolle tätig. Diese richtet sich auf die Identifizierung externer Compliance-Anforderungen (MEA03.01), die Bestätigung der externen Compliance (MEA03.03) und den Erhalt von Compliance-Bestätigungen (MEA03.04). Daneben ist die Position des Datenschutzbeauftragten umfangreicher an IT-Governance- und IT-Managementpraktiken in den Domänen APO, BAI, DSS und MEA verantwortlich beteiligt (vgl. [Klotz 2019, S. 33]).

[1] Nach [Klotz 2019, S. 21ff.], vgl. [ISACA 2018b, S. 29ff.].
[2] Ein Compliance-Bezug kann jedoch auch in den anderen Governance-Praktiken identifiziert werden. Hierzu sind die Aktivitäten hinsichtlich IT-Compliance entsprechend auszulegen, vgl. [Klotz 2019, S. 22ff.].

Die zentralen IT-Compliance-Aufgaben haben eher steuernden und überwachenden Charakter. Dagegen obliegt die Durchführung eher in der Verantwortung der dezentralen IT-Compliance-Stellen (vgl. Abbildung 6–2).

Die dezentralen Positionen in der IT-Abteilung und in den Fachabteilungen stellen die dritte Ebene der IT-Compliance-Organisation dar. In größeren Unternehmen werden weitere Ebenen und auch eine regionale Dimension (z. B. Compliance-Verantwortliche in Landesgesellschaften) hinzukommen müssen.

Die Beziehung zwischen der zentralen IT-Compliance in Corporate Compliance und den dezentralen IT-Compliance-Stellen kann von einer reinen Berichtslinie über eine projektbezogene oder begrenzte funktionale Weisungsbefugnis bis zu einer vollständigen fachlichen Unterstellung reichen. Die Aufgaben der dezentralen IT-Compliance-Stellen sind (in Anlehnung an [Klotz 2020, S. 878]):

(1) Identifizierung der für den jeweiligen Bereich relevanten Regelwerke und IT-Compliance-Anforderungen
(2) Bestimmung der fachbereichsbezogenen IT-Compliance-Risiken
(3) Einleitung der fachbereichsbezogenen IT-Compliance-Maßnahmen und Überwachung ihrer Ausführung
(4) Dokumentation und Berichterstattung an die zentrale IT-Compliance
(5) Zusammenarbeit mit zentraler IT-Compliance/CCO und anderen Stellen, z. B. Rechtsabteilung, bei Vorliegen von Non-Compliance

In COBIT© 2019 sind an der Durchführung dieser Aufgaben die Fachabteilungen in Form der betroffenen geschäftsprozessverantwortlichen Stellen beteiligt. Dies betrifft vor allem die Identifizierung der Compliance-Anforderungen (MEA03.01), die Durchführung korrektiver Maßnahmen bei Non-Compliance (MEA01.05/ MEA04.09) und die Analyse der Risiken von Non-Compliance (APO12.02) (vgl. [ISACA 2018b, S. 134, 276, 287, 293]).

Je nach Größe und Gegenstand des Unternehmens kann es sinnvoll sein, das Drei-Ebenen-Modell um einen IT-Compliance-Ausschuss zu ergänzen, der im Kern aus dem CIO, dem CCO, den IT-Beauftragten (vor allem dem Datenschutzbeauftragten und dem IT-Sicherheitsbeauftragten) sowie Vertretern der Rechtsabteilung und der IT-Revision bestehen kann. In dieses Gremium können bei Bedarf weitere unternehmensinterne Zentralfunktionen sowie betroffene IT-Fachfunktionen aktiv eingebunden werden.

Der IT-Compliance-Ausschuss hat sowohl eine Unterstützungs- als auch eine Überwachungsaufgabe. Die Unterstützung bezieht sich im Wesentlichen auf notwendige Abstimmungen in der Planungs- und Vorbereitungsphase von Compliance-Maßnahmen. Die Aufgaben des IT-Compliance-Committee sind im Einzelnen (in Anlehnung an [Klotz 2020, S. 878f.]):

(1) Übergreifende (IT-)GRC-Koordination
(2) Koordination mit der Corporate Compliance
(3) Risikobasierte Priorisierung von IT-Compliance-Maßnahmen

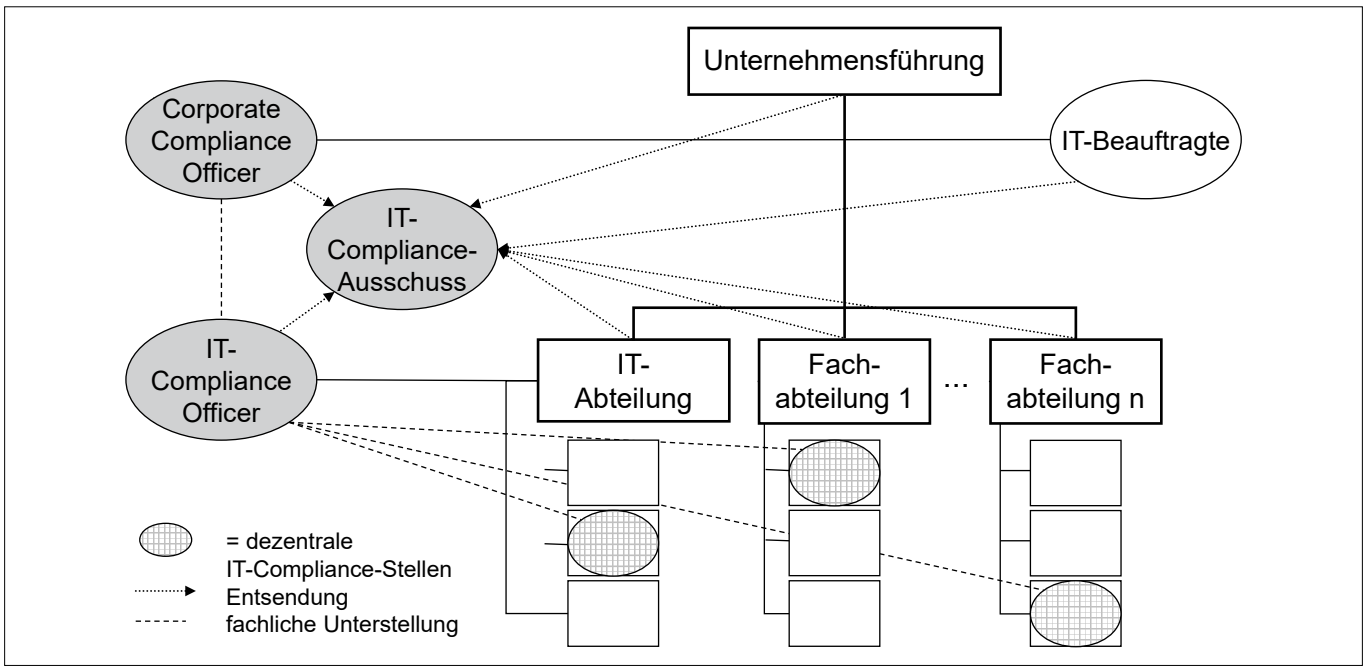


Abb. 6–2: Organisationsstruktur für IT-Compliance (nach [Klotz 2009, S. 8])

(4) Abstimmungen und Ressourcenbereitstellung in der Planungs- und Vorbereitungsphase von Compliance-Maßnahmen
(5) Unternehmensinterne Promotion für IT-Compliance, insbesondere in speziellen Bereichen, beispielsweise Datenschutz und Datensicherheit
(6) Kontrolle von IT-Compliance-Maßnahmen (vor allem infolge von Compliance-Verstößen)
(7) Entgegennahme der IT-Compliance-Statusberichte

COBIT© 2019 berücksichtigt neben einer zentralen Compliance-Funktion und dem CIO auch ein I&T Governance Board, das im Rahmen von Compliance-Management-Praktiken beteiligt ist. Dieses Gremium wirkt verantwortlich an der Überprüfung und Anpassung von Richtlinien, Prinzipien, Standards, Verfahren und Methoden mit, um Compliance mit gesetzlichen, behördlichen und vertraglichen Anforderungen und deren Kommunikation im Unternehmen sicherzustellen (MEA03.02). Ebenso liegt die Sicherstellung der Befolgung dieser Richtlinien, Prinzipien, Standards, Verfahren und Methoden in der Verantwortung des I&T Governance Board (MEA03.03) (nach [ISACA 2018b, S. 286f.]).

6.2 Die IT-Compliance im Rahmen des Drei-Linien-Modells

Das Modell der Verteidigungslinien, der »Three Lines of Defense«, hat sich seit seiner Entstehung ab 2011 schnell verbreitet und wurde in vielen Unternehmen umgesetzt (vgl. [Mertmann/Scharr 2016, S. 4]). Den Ausgangspunkt des Modells bildet die Beobachtung, dass in Unternehmen verschiedene Experten der Internen Revision, des Risikomanagements, der Compliance, des Qualitätsmanagements, der Unternehmenssicherheit etc. zusammenarbeiten müssen, um effektive und effiziente Strukturen für Risikomanagement sowie Unternehmenssteuerung und -überwachung zu etablieren. Die hierfür notwendige Zusammenarbeit der beteiligten Stakeholder ist in einer konsistenten Rollen- und Verantwortungsstruktur zu organisieren, um Lücken ebenso wie Dopplungen oder Überschneidungen im Steuerungs- und Überwachungssystem zu vermeiden (nach [IIA 2013, S. 1]). Diese Zielsetzung ist auch für die aktualisierte Version des Modells gültig, das als Drei-Linien-Modell (Three Lines Model, TLM) bezeichnet wird.

In der Übertragung des allgemeinen TLM auf die IT-Governance werden diejenigen Verantwortungsträger fokussiert, deren Zusammenspiel für einen effektiven IT-Einsatz und zur Steuerung von IT-Risiken zu organisieren ist. Die verschiedenen Akteure stellen sich wie folgt dar (vgl. Abbildung 6–3):

Die Unternehmensleitung und ein ggf. obligatorisches Aufsichtsgremium als Leitungsorgane des Unternehmens stehen für Integrität, Führung und Transparenz in Bezug auf die Unternehmens-IT und stellen das Bindeglied zu den externen Stakeholdern dar. Jedoch werden nicht alle Mitglieder der Unternehmensleitung mit der Steuerung und Überwachung der IT befasst sein. Stattdessen wird dies in die Ressortverantwortung eines der Mitglieder der Unternehmensleitung fallen, z. B. des CIO. Die Verantwortung dieser Position richtet sich auf

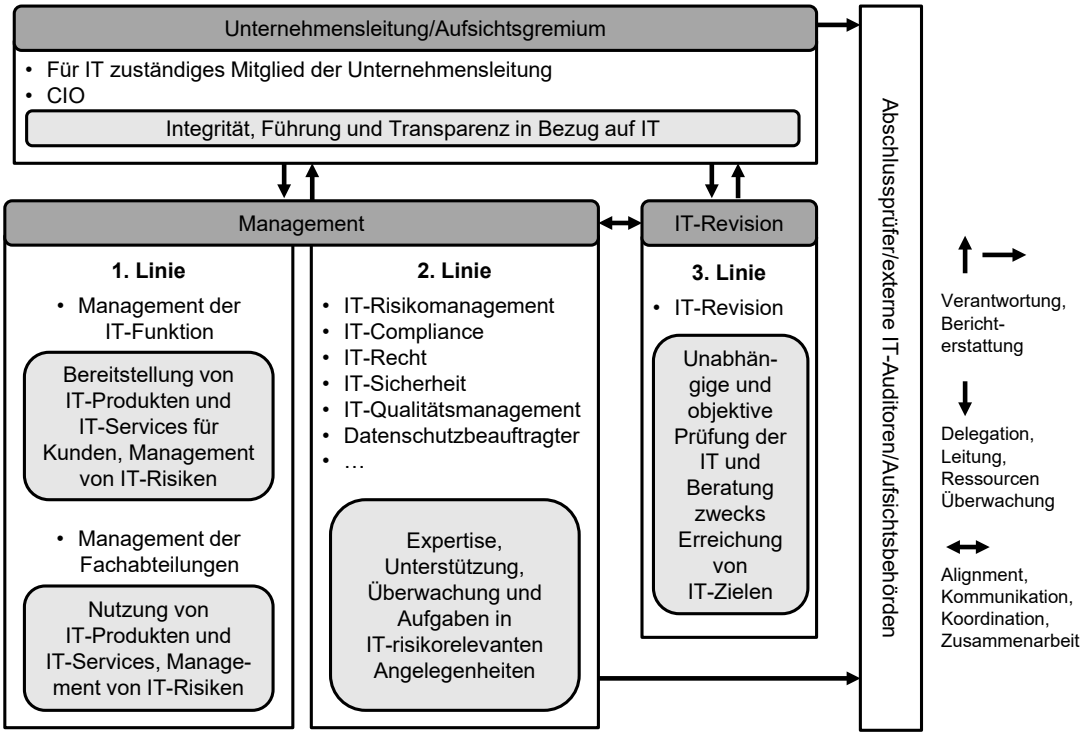


Abb. 6-3: IT-Compliance im Drei-Linien-Modell

- die Etablierung von IT-Governance-Strukturen und -Prozessen sowie einer unterstützenden IT-Kultur, die ethischen Ansprüchen gerecht wird,
- die Definition der IT-Risikobereitschaft,
- die Einrichtung und Beaufsichtigung der IT-Revision,
- die Genehmigung und Bereitstellung ausreichender Ressourcen für die IT,
- die Überwachung der IT-Compliance (vgl. [Eulerich 2020, S. 211], [IIA 2020, S. 5]).

Es liegt im Ermessen des CIO bzw. der Unternehmensleitung, zusätzliche Gremien oder Ausschüsse für die Steuerung und Überwachung der IT einzurichten. Zum Beispiel könnte sich ein IT-Lenkungsausschuss mit Fragen der Allokation von IT-Ressourcen oder einer längerfristigen Applikationsplanung befassen. Ein weiteres Beispiel wäre das bereits erwähnte IT-Compliance-Committee.

Das Management in der ersten Linie agiert als Risikoeigner (Risk Owner) und ist für die Steuerung und Überwachung des von ihm verantworteten Bereichs zuständig. Als Management ist hier sowohl das Management der IT-Funktion als auch das Management der Fachabteilungen angesprochen.

- Das Management der IT-Funktion, d.h. die IT-Leitung und die ihr zugeordneten IT-Managementpositionen (Leitung der Anwendungsentwicklung, Leitung IT-Infrastruktur, Leitung Anwendungssysteme etc.) haben ihren Verantwortungsbereich auf Effektivität und Effizienz in der Unterstützung der Geschäftsprozesse hin zu steuern und zu überwachen – und zwar unter Minimierung der IT-Risiken.
- Das Management der Fachabteilungen hat den IT-Einsatz in seinen Verantwortungsbereichen in Zusammenarbeit mit der IT-Funktion und unter Nutzung der von der zweiten Verteidigungslinie etablierten IT-Managementsysteme zu steuern und zu überwachen (vgl. [Klotz 2016b, S. 146f.]).

Beide Managementgruppen haben zur Erreichung ihrer Ziele Verantwortlichkeiten und Prozesse festzulegen und in ihrer Wahrnehmung und Ausführung zu steuern und zu überwachen. Hierzu ist ein effektives Risikomanagement mit angemessenen internen Kontrollen einzurichten. Dieses umfasst neben anderen IT-Risiken auch die Analyse, Überwachung, Steuerung, Berichterstattung und Evaluation von IT-Compliance-Risiken (nach [Eulerich 2020, S. 214], [IIA 2020, S. 5]).

Das Management in der zweiten Linie unterstützt mit seinen Fachkenntnissen die erste Linie. Die zweite Linie beinhaltet die IT-Spezialisierung der entsprechenden zentralen Funktionen, u.a. auch die IT-Compliance und das IT-Risikomanagement (vgl. [Ho 2018, S. 38]) als Spezialisierung der jeweiligen Unternehmensfunktionen sowie den Datenschutzbeauftragten. Die Zielsetzung der zweiten Linie besteht in der Regulierung, z.B. durch die Erstellung von Richtlinien, und Optimierung der Steuerungs- und Überwachungsstruktur, z.B. Risiko- oder Compliance-Management-Systemen, und damit in der Reduzierung von Risikopotenzialen. Dies beinhaltet auch die zugehörige Berichterstattung hinsichtlich der Angemessenheit und Wirksamkeit des IT-Risikomanagements einschließlich der IT-Kontrollen (nach [Eulerich 2020, S. 212]).

Die IT-Revision als Spezialisierung der zentralen Internen Revision stellt nach wie vor die dritte Linie dar. Sie bewertet »mit einem systematischen Ansatz die Angemessenheit und Wirksamkeit des IT-Risikomanagements, der IT-Controls und der Führungs- und Überwachungsprozesse in der IT« und hilft diese zu verbessern [Knoll/Bank 2015, S. 29]. Hierbei arbeitet sie mit der ersten Linie ebenso wie mit den IT-bezogenen Funktionsspezialisierungen der zweiten Linie – insbesondere auch der IT-Compliance – zusammen. Vor allem den Leitungsorganen des Unternehmens liefert die IT-Revision unabhängige und objektive Bestätigungen der Angemessenheit und Wirksamkeit der IT-Governance und des IT-Risikomanagements. Insofern sind die Leitungsorgane des Unternehmens die zentralen Adressaten der von der dritten Linie erstellten Berichte (nach [Eulerich 2020, S. 214], [IIA 2020, S. 6]).

Die drei internen Linien werden durch eine externe Linie ergänzt. Dieser sind die Prüfung der IT im Rahmen der Jahresabschlussprüfung sowie weitere IT-Prüfungen durch unabhängige, externe Auditoren zugeordnet. Auch externe IT-Prüfungen durch gesetzlich ermächtigte Behörden oder speziell eingerichtete Aufsichtsinstitutionen, wie z.B. das Finanzamt oder die BaFin, zählen zur externen Linie.

Die Verortung der IT-Compliance im TLM verdeutlicht ihren organisatorischen Abstimmungsbedarf in drei Richtungen:

- Grundlegend für die Ausgestaltung der IT-Compliance ist die Abstimmung innerhalb der zweiten Linie mit der unternehmensweit verantwortlichen Compliance-Funktion.
- Die Abstimmung innerhalb der zweiten Linie mit anderen Funktionen richtet sich insbesondere auf die Koordination in Bezug auf die Kontroll- und Überwachungsstruktur des Unternehmens. Vor allem die verschiedenen Managementsysteme (IT-Risiko-Management-System, IT-Compliance-Management-System, Informationssicherheitsmanagementsystem, IT-Kontrollsystem) sollten nicht isoliert voneinander konzipiert, installiert und betrieben werden.
- Die Abstimmung mit den anderen Linien betrifft die Unterstützung des operativen Tagesgeschäfts der ersten Linie bei der Wahrnehmung der Überwachungsverantwortung, z.B. durch die Weiterentwicklung von Richtlinien, Beratung in Fragen der IT-Compliance, Unterstützung von Self-Assessments oder Klärung von IT-Compliance-Anforderungen. Die Mitwirkung an Prüfungen der IT-Revision oder die Verarbeitung von Feststellungen im Ergebnisbericht der IT-Revision sind Beispiele für die Abstimmung mit der dritten Linie. Nicht zu vergessen ist zudem, dass die IT-Revision die Angemessenheit und Funktionsfähigkeit des IT-Compliance-Systems (ggf. als IT-CMS) zu prüfen hat (vgl. [Egner 2011, S. 22]).

Zwar wird das TLM in COBIT 2019 nicht explizit referenziert. Gleichwohl lässt sich die von COBIT 2019 verwendete generische Organisationsstruktur in eine TLM-adäquate Form überführen. Aufsichtsgremium und Unternehmensleitung sind in COBIT 2019 mit dem Board, dem Executive Committee, dem I&T Governance Board und insgesamt sieben Chief-Positionen (CEO, CFO, CIO etc.) umfangreich vertreten. Die erste Linie wird mit den verschiedenen IT-Bereichen sowie dem Business Process Owner abgedeckt. Der zweiten Linie sind die Positionen Information Security Manager, Business Continuity Manager, Privacy Officer, Legal Counsel und Compliance zuzuordnen (vgl. [ISACA 2018b, S, 299f.]). Die dritte Linie ist die Audit-Funktion. Da sich die Verantwortlichkeit dieser Stellen bzw. Funktionen in Responsible- oder Accountable-Rollen ausprägt, kann COBIT 2019 genutzt werden, um die Zusammenarbeit der IT-Stakeholder entsprechend dem TLM auf der Ebene der COBIT-Praktiken zu konkretisieren. Die externe Linie ist nicht als Organisationsstruktur erfasst, da sich diese lediglich auf die interne Unternehmensorganisation bezieht. Externe Prüfer werden jedoch im Rahmen der Komponente »Services, Infrastruktur und Anwendungen« als »Third-party internal assessment services« für Sicherheit, Compliance und Control angesprochen (vgl. [ISACA 2018b, S. 142, 263, 283, 288]). Ein weiterer Akteur der externen Linie wird von Aufsichtsbehörden (regulators) als externer Stakeholder gebildet (vgl. [ISACA 2018a, S. 15]).

6.3 Der IT-Compliance-Manager

Die Stelle eines IT-Compliance-Managers (ITCM) ist derzeit eher durch die Praxis geprägt.[3] In der Fachliteratur reicht das Verständnis von einer Führungskraft, die *für* die Gewährleistung von IT-Compliance verantwortlich zeichnet[4], bis hin zum Spezialisten in Stabstellen, die sich auf fachlich abgegrenzte Gesetze, IT-Normen oder -Standards fokussieren. Die theoretischen Möglichkeiten der Positionierung lassen sich im Rahmen einer organisationalen Genese der IT-Compliance bestimmen, beginnend mit einer Aufgabenzuweisung an bestehende zentrale Führungsstellen, über die Auslagerung an externe Spezialisten, die Einrichtung erst von Stabstellen, dann von Fachgruppen bis schließlich hin zu einem integrierten Bereich für Governance, Risk und Compliance (nach [Rath/Sponholz 2014, S. 151]). In dieser Abfolge könnte der IT-Compliance-Manager die Stabstelle bekleiden oder Leiter einer Fachgruppe »IT-Compliance« oder eben doch nur ein Fachspezialist innerhalb eines GRC-Bereichs sein.

Schon in der Stellenbezeichnung finden sich fast beliebige Kombinationen aus Officer oder Manager sowie IT-Compliance mit IT-Sicherheit, IT-Governance oder IT-Risikomanagement. Dies setzt sich in der Verbindung von IT-Compliance mit weiteren Fachthemen fort. Über die genannten hinaus sind dies vor allem IT-Audit, Datenschutz, Cybersicherheit sowie auch IT-Vertragswesen oder IT-Prozessmanagement. Die hierarchische Einordnung geht in der Praxis deutlich in Richtung einer fachlichen Expertenstellung. Dies prägt sich in Bezeichnungen wie »Referent/-in«, »Analyst (m/w)«, »Koordinator«, »Mitarbeiter/-in«, »Professional« und »Fachfunktion (m/w)« aus. Auch eine Position als »Officer« bedeutet nicht notwendig eine Leitungsposition. Die Leitungsaufgabe, die mit »Manager«- und »Officer«-Stellen verknüpft wird, bezieht sich häufig auf eine Projektleitung, wobei die Größe der Projekte von Teilprojekten bis hin zu internationalen Großprojekten reicht.

Die Aufgaben des IT-Compliance-Managers lassen sich in folgende Aufgabenkomplexe gliedern (vgl. Abbildung 6–4).

- **Sicherstellung von IT-Compliance**
  Als Kernaufgabe hat der ITCM die Einhaltung der gesetzlich-regulatorischen, sonstigen unternehmensexternen sowie der unternehmensinternen und vertraglichen Regelungen in Bezug auf die IT des Unternehmens sicherzustellen. Hierzu umfassen seine Aufgaben sowohl strategische als auch operative analytisch-konzeptionelle Aufgaben.

[3] Im Folgenden nach [Klotz 2018], wo die Ergebnisse einer Studie zu im Jahr 2017 publizierten einschlägigen Stellenanzeigen diskutiert werden.

[4] So z. B. Wittek/Strasser, für die es sich um eine Stelle mit disziplinarischen Befugnissen handelt; vgl. [Wittek/Strasser 2012, S. 68].

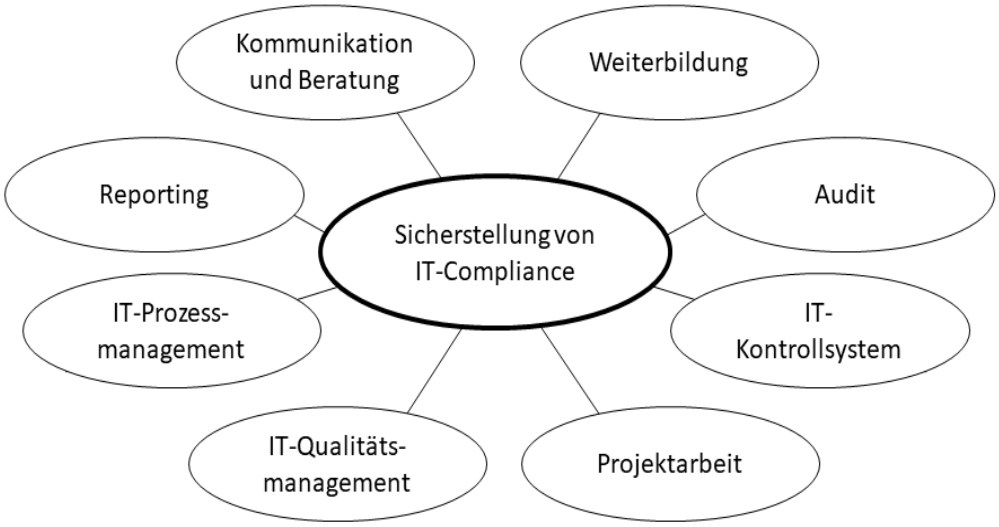


Abb. 6-3: IT-Compliance im Drei-Linien-Modell

Strategische Aufgaben richten sich auf die (Weiter-)Entwicklung der IT-Compliance-Strategie und den Aufbau eines IT-Compliance-Management-Systems. Dagegen beinhalten die operativen Aufgaben die Identifizierung und Steuerung von allgemeinen und branchenbezogenen IT-Compliance-Anforderungen, verbunden mit der Identifikation und Bewertung von IT-Compliance-Risiken. Weiterhin sind die (Weiter-)Entwicklung von Policies, Richtlinien, Hausstandards, Arbeitsanweisungen und sonstigen Regelungen sowie diesbezügliche Abweichungsanalysen zentrale Aufgaben des ITCM.

- **IT-Prozessmanagement**
  In Bezug auf das IT-Prozessmanagement hat der ITCM Qualitätssicherungsverfahren für spezifische IT-Compliance-Prozesse und vor allem die Analyse und Dokumentation von Geschäftsprozessen hinsichtlich IT-Compliance-Anforderungen und die Entwicklung von diesbezüglichen Verbesserungsmöglichkeiten zu unterstützen.
- **IT-Qualitätsmanagement**
  Das IT-Prozessmanagement ist eng mit dem IT-Qualitätsmanagement verknüpft. Im Rahmen der IT-Prozess-Dokumentation umfasst die vom ITCM vorzunehmende Dokumentation auch Anforderungs- oder Risikoanalysen in speziellen IT-Compliance-Bereichen (z. B. Datenschutz, Betriebs- und Notfallhandbuch, Lizenzmanagement) sowie das bestehende IT-Compliance-Kontrollsystem.
- **IT-Kontrollsystem**
  Hinsichtlich des IT-Kontrollsystems ist der ITCM beteiligt an der Implementierung von Compliance-bezogenen IT General Controls, der (Weiter-)Entwicklung von Compliance-bezogenen Aspekten des IT-Kontrollsystems und der Definition interner Kontrollanforderungen in Bezug auf IT-Compliance.
- **Audits**
  Mitunter kommt dem ITCM auch eine eigenständige Überwachungsverantwortung zu. In diesem Fall hat er an internen und externen Audits mitzuwirken oder diese selbst durchzuführen. Externe Audits betreffen Zertifizierungen oder den Jahresabschluss, interne Audits die Prüfungen durch die interne Revision oder IT-Compliance-Self-Assessments in der IT-Funktion.
- **Kommunikation und Beratung**
  Außerhalb der IT-Funktion ist der ITCM in Belangen der IT-Compliance Ansprechpartner und ggf. auch Berater der Unternehmensleitung, der Führungskräfte von Fachabteilungen und zentralen Unternehmensfunktionen der zweiten Linie, vor allem der Corporate Compliance und des Risikomanagements, der Revision, des Datenschutzbeauftragten, aber auch der IT-Anwender. Innerhalb der IT-Funktion sind die einzelnen IT-Fachfunktionen, z. B. IT-Sicherheits- und IT-Risikomanagement seine Adressaten. Darüber hinaus ist der ITCM auch Ansprechpartner für externe Stakeholder, insbesondere Vertreter von Aufsichtsorganisationen.
- **Weiterbildung**
  Eng verknüpft mit den kommunikativen Aufgaben ist das Engagement des ITCM im Bereich der Weiterbildung zu IT-Compliance. Diese reicht von der Planung und Durchführung von Awareness-Maßnahmen bis hin zur Ausarbeitung und Durchführung spezialisierter Schulungen für IT-Compliance.
- **Reporting**
  Das Reporting des ITCM soll darüber Auskunft geben, inwieweit die IT-Compliance-Ziele erreicht wurden. Dies umfasst das Bereitstellen und die Aufbereitung von IT-Compliance-Kennzahlen. Adressaten hierfür sind die Corporate Compliance und die Unternehmensleitung bzw. der CIO. Das Reporting kann sich als Regelkommunikation oder als Ad-hoc-Kommunikation vollziehen. Letzteres betrifft insbesondere Stellungnahmen und Handlungsempfehlungen für interne und externe Gremien.
- **Projektarbeit**
  Nicht zuletzt ist der ITCM in (IT-)Compliance-Projekte involviert. Diese Beteiligung reicht von fachlicher Projektmitarbeit über begleitende Beratung in IT-Compliance-Fragen bis hin zur Leitung von IT-Compliance-Projekten.

Als Fazit lässt sich festhalten, dass der IT-Compliance-Manager in der Praxis im Regelfall keine Mitarbeiter »managt«. Er ist vielmehr mit dem Management von Fachobjekten (IT-Compliance-Prozesse, -Projekte, -Anforderungen, Richtlinien, Berichte, IT-Compliance-Verstöße etc.) befasst. Wenn die Ausgestaltung der IT-Compliance in Unternehmen künftig einen höheren Reifegrad erreicht, sollte sich diese Ausrichtung in Richtung einer steuernden und überwachenden Verantwortung verschieben und ggf. in eine disziplinarisch leitende Stelle münden. Zu beachten sind dabei Überschneidungen zur Rolle des Informationssicherheitsbeauftragten. Unternehmensindividuell sind klare Abgrenzungen und Schnittstellen zwischen den beiden Rollen zu definieren.

COBIT© 2019 beinhaltet keine Position, die dem IT-Compliance-Manager entsprechen würde. Eine Vielzahl der genannten Aufgaben des ITCM verteilen sich im Rahmen des RACI-Modells von COBIT© 2019 auf unterschiedliche Stellen bzw. Rollen, vor allem die Compliance, das Audit, die Rechtsabteilung, den Datenschutzbeauftragten, die Geschäftsprozessverantwortlichen und den CIO.

Handlungsempfehlungen

- Die aufbauorganisatorische Gestaltung der IT-Compliance sollte sich nicht nur auf die Stelle eines »IT-Compliance-Managers« konzentrieren, sondern die Integration in die gesamte Unternehmensorganisation anstreben.
- Ankerpunkt für die Organisation der IT-Compliance ist die Organisation der Corporate Compliance.
- Vor allem an der praktizierten Balance zwischen Zentralisation und Dezentralisation von Compliance-Aufgaben muss sich auch die IT-Compliance orientieren.
- Die Ausgestaltung der IT-Compliance sollte ein Organisationsprojekt darstellen, an dem die verschiedenen IT-Stakeholder zu beteiligen sind, damit klare organisatorische Schnittstellen geschaffen werden.
- Insbesondere hinsichtlich IT-Risiko- und IT-Sicherheitsmanagements müssen organisatorische Schnittstellen zur IT-Compliance festgelegt werden.
- Nutzen Sie das Drei-Linien-Modell zur Strukturierung Ihrer IT-Governance und zur Verortung der IT-Compliance-Funktion. Für die Konzeption der Zusammenarbeit der IT-Stakeholder kann das TLM durch die Organisationsstruktur-Tabellen von COBIT 2019 konkretisiert werden.
- Um Missverständnisse zu vermeiden, sollte für die Stelle eines IT-Compliance-Managers klar festgelegt und kommuniziert werden, ob es sich um eine Fachposition oder eine Leitungsfunktion handelt.

7 Compliance-Management-System in der IT (IT-CMS)

7.1 Das IT-CMS im Rahmen unternehmensweiter Compliance

Um IT-Compliance als Unternehmensziel zu erreichen, bedarf es systematischer Aktivitäten im Rahmen einer effektiven und effizienten Struktur. Mit anderen Worten, es bedarf eines speziellen Managementsystems, dessen oberstes Ziel die Sicherstellung von IT-Compliance ist. In Übertragung der Definition des IDW PS 980 lassen sich unter einem IT-Compliance-Management-System (IT-CMS) Grundsätze und Maßnahmen verstehen, die beim Einsatz von IT im Unternehmen ein regelkonformes Verhalten – d.h. das Einhalten von Regeln und das Verhindern von wesentlichen Regelverstößen – der Unternehmensmitglieder und ggf. beteiligter Dritter sicherstellen (nach [IDW PS 980, Tz. 6]).

Bei einem IT-CMS eines Unternehmens handelt es sich i.d.R. nicht um ein eigenständiges System, das unabhängig und als »Silo« in der IT implementiert wird. Vielmehr hat sich die Ausgestaltung des IT-CMS an den Rahmenbedingungen des unternehmensweiten Compliance-Management-Systems zu orientieren. Dies gilt für alle Komponenten des IT-CMS. Beispielsweise sollten IT-Compliance-Ziele aus den Compliance-Zielen des Unternehmens abgeleitet bzw. in eine hierarchische Zielpyramide des Unternehmens integriert werden. Diese Festlegung hat situativ zu erfolgen. So werden in Unternehmen, in denen das operative Geschäft in hohem Maß von der Funktionsfähigkeit der IT sowie umfangreichen regulativen Vorgaben von Aufsichtsinstitutionen abhängt, die Ziele für die IT-Compliance eine wesentlich höhere Bedeutung haben als in Unternehmen, in denen die Abhängigkeit des operativen Geschäfts und die regulativen Vorgaben geringer sind. Innerhalb der unternehmensweiten Vorgaben sollte die IT-Compliance jedoch frei agieren können mit dem Ziel, alle relevanten Informationen zum Compliance-Status der IT in das Unternehmen zu kommunizieren und dabei IT-Compliance-Risiken systematisch durch geeignete Prozesse und Maßnahmen zu begegnen.

Aufgrund des Sachverhaltes, dass ein IT-CMS nicht unabhängig installiert wird, ist es nicht Ziel dieses Leitfadens, ein vollständiges IT-Compliance-Management-System zu beschreiben. Zum einen müssen vollumfängliche Systeme vor allem branchen- und größenabhängig ausgestaltet sein, zum anderen existieren bereits anerkannte und bewährte Vorgaben, wie z.B. der Prüfungsstandard IDW PS 980 oder die Norm DIN ISO 19600, die Ausführungen zur Planung, zur Organisation, zum Betrieb und zur Weiterentwicklung eines Compliance-Management-Systems beinhalten. Tabelle 7–1 stellt die Gliederungen der beiden Regelwerke für ein CMS gegenüber.

IDW PS 980	DIN ISO 19600
Compliance-Kultur	Kontext der Organisation
Compliance-Ziele	Führung
Compliance-Risiken	Planung
Compliance-Programm	Unterstützung
Compliance-Organisation	Betrieb
Compliance-Kommunikation	Bewertung der Leitung
	Verbesserung

Tab. 7–1: Struktur eines CMS (vgl. [IDW PS 980, Tz. 23], [DIN ISO 19600:2016, S. 5])

Wie zu erkennen ist, beinhaltet der IDW PS 980 eine Gliederung nach inhaltlichen Komponenten, die in verschiedene Managementmaßnahmen münden. Dagegen nimmt die DIN ISO 19600 eine prozessorientierte, an den PDCA-Zyklus angelehnte Sicht ein, die im Ergebnis zu den verschiedenen Komponenten führt, beispielsweise zu einer Compliance-Organisation mittels einer Zuordnung von Compliance-Verantwortlichkeiten und der Schaffung einer Compliance-Funktion. Letztlich lassen sich die CMS-Komponenten des IDW PS 980 auch in der von der DIN ISO 19600 vorgenommenen Beschreibung CMS-Prozesse wiederfinden.[1] Umgekehrt kann ein nach DIN ISO 19600 ausgestaltetes CMS grundsätzlich die Basis für ein angemessenes und wirksames CMS gemäß IDW PS 980 darstellen (nach [Schmidt 2016, S. 1449]).

Die Struktur eines IT-CMS festzulegen, ist eine wichtige Aufgabe der IT-Governance. Dies kann nur unternehmensspezifisch entsprechend den unterschiedlichen Compliance-Anforderungen an die Unternehmens-IT und den situativen organisatorischen und geschäftlichen Gegebenheiten für den IT-Einsatz

[1] Ein detaillierter Vergleich von ISO 19600 und IDW PS 980 findet sich in [Withus 2017].

erfolgen.[2] Deswegen wird an dieser Stelle keine Empfehlung für die strukturelle Ausgestaltung eines IT-CMS getroffen. Die folgenden Ausführungen konzentrieren sich vielmehr auf wesentliche Aspekte für die Implementierung eines IT-CMS.

Im Gegensatz z. B. zum Informationssicherheitsmanagementsystem verwendet COBIT 2019 den Begriff des Compliance-Management-Systems nicht. Trotzdem beschreibt COBIT ein IT-CMS, indem sich die verschiedenen Komponenten der IT-Governance- und IT-Managementzielsetzungen auf IT-Compliance richten. Insofern wird auch ein IT-CMS gebildet aus: a) Prozessen, b) Organisationsstrukturen (Verantwortlichkeiten), c) Richtlinien und Arbeitsanweisungen, d) Informationsflüssen und -elementen, e) Kultur, Ethik und Verhalten, f) Mitarbeiter, Fähigkeiten und Kompetenzen sowie g) Services, Infrastruktur und Anwendungen (vgl. [Klotz 2019, S. 21ff.]). Aussagen zu IT-Compliance und einem IT-CMS sind vor allem in den verschiedenen COBIT-Prozessen enthalten. Gleichwohl beinhaltet COBIT 2019 in der IT-Managementzielsetzung MEA03 (Managed Compliance With External Requirements) einen zentralen IT-Compliance-Prozess.

7.2 Compliance-Kultur und Awareness

Die Compliance-Kultur eines Unternehmens ergibt sich aus der fortlaufenden Kommunikation der Unternehmensmitglieder und dem damit verbundenen Abgleich von Annahmen, Einstellungen und Verhaltensmustern (in Anlehnung an [Wendt 2016, S. 293]). In der IT eines Unternehmens spiegelt sich die Compliance-Kultur insbesondere in den aufgestellten und kommunizierten Verhaltensgrundsätzen zur regelkonformen Nutzung der IT-Systeme sowie im Führungsstil der IT-Führungskräfte und der Personalpolitik des Unternehmens in Bezug auf die IT-Arbeitsplätze und die benötigten Kenntnisse und Fähigkeiten bezüglich IT-Compliance wider.

Wie die Compliance-Kultur insgesamt wird die IT-Compliance-Kultur durch den gelebten Wertekanon seitens der Unternehmensleitung, des Fach- und IT-Managements sowie der Mitarbeiter geprägt. Hierbei kommen der Unternehmensleitung und ggf. einem Aufsichtsorgan folgende grundlegende Aufgaben zu:

- Die Basis für eine effektive Compliance-Kultur und damit auch IT-Compliance-Kultur ist das Bekenntnis der Unternehmensleitung zu regelkonformem Verhalten. Dies umfasst neben einem sichtbaren persönlichen Commitment eine Festlegung der Grundwerte der Organisation, der Compliance-Politik und der Compliance-Ziele. Die diesbezüglichen Ergebnisse sind zu dokumentieren und für die Unternehmensmitglieder verfügbar zu machen. Wenn es ein IT-Leitbild gibt, sollte es auch Aussagen zur IT-Compliance enthalten.
- Neben den dokumentierten Vorgaben der Unternehmensleitung beeinflussen das individuelle Verhalten und die persönlichen kommunizierten Grundeinstellungen der Mitglieder der Unternehmensleitung die Compliance-Kultur. Dieser Aspekt wird gewöhnlich als »Tone at the top« adressiert (vgl. [IDW PS 980, Tz. 23]), wobei es darauf ankommt, dass das persönliche Verhalten mit den postulierten Grundwerten und Zielen sichtbar übereinstimmt.
- Die Durchsetzung von IT-Compliance ist seitens der Unternehmensleitung durch die effektive Implementierung von Richtlinien, Verfahren und Prozessen sicherzustellen.
- Weiterhin hat die Unternehmensleitung Compliance-Verantwortlichkeiten und Befugnisse an die Führungskräfte des Unternehmens zu delegieren, um deren Führungsrolle bzgl. IT-Compliance deutlich zu machen. Dies umfasst auch die Verantwortung dafür, dass die IT-Compliance-Anforderungen in die Geschäftsprozesse der Organisation integriert werden.
- Die Unternehmensleitung hat ein Klima zu fördern, das sowohl die Führungskräfte als auch Mitarbeiter dazu animiert, ohne Angst vor Nachteilen Compliance-Verstöße zu melden. Mitarbeiter sind im Hinblick auf die Unterscheidung zwischen IT-Compliance und IT-gestützter Compliance sowohl IT-Mitarbeiter innerhalb der IT-Funktion als auch IT-Nutzer außerhalb der IT-Funktion.
- Nicht zuletzt liegt die fortgesetzte Bewilligung der erforderlichen finanziellen, organisatorischen (d. h. personellen und prozessualen) und technischen Ressourcen (d. h. Tools für Compliance-Management und Automatisierung von Compliance-Maßnahmen) zur Durchsetzung eines regelkonformen IT-Betriebs in den Händen der Unternehmensleitung.

Allein mit der Vermittlung von Werten und der Erstellung von Dokumentationen ist jedoch noch nicht gewähreistet, dass die gewünschte Kultur in der IT auch gelebt wird. Eine der wesentlichen Voraussetzungen für die Etablierung der angestrebten Kultur ist die Sicherstellung der erforderlichen personellen Ausstattung zur Erreichung bzw. Aufrechterhaltung von IT-Compliance. Dies bezieht sich nicht allein auf die Ressourcen einer IT-Compliance-Funktion. Eine unzureichend ausgestattete IT-Security-Einheit z. B. wird nicht die zunehmenden erforderlichen Sicherheitsmaßnahmen einführen und überwachen und zusätzlich noch die Security Awareness im Unternehmen optimieren können. Im täglichen Geschäftsbetrieb führt dies zu Frustration und beeinträchtigt die Kultur.

Werte, Einstellungen und Verhaltensweisen sollten zur Förderung einer gewünschten Compliance-Kultur bereits bei der Initiierung des Arbeitsverhältnisses thematisiert werden. Geeignete und zu der zu besetzenden Position angemessene Hintergrund-Recherchen zum Werdegang von Bewerbern können dabei unterstützen, die passenden Mitarbeiter zu finden. Zudem bietet es sich an, neuen Mitarbeitern umfangreiche Informationen zur Corporate Compliance und zu IT-Compliance bereitzustellen und sie, z. B. in Onboarding-Veranstaltungen des Unternehmens, mit den geltenden Compliance-Anforderungen vertraut zu machen. Trotz dieser

[2] Nach [DIN ISO 19600:2016, S. 4] ist die Ausgestaltung eines CMS abhängig von Kontext, Art, Komplexität und Tätigkeit der Organisation sowie der Größe und dem Reifegrad eines vorhandenen CMS. Nach [IDW PS 980, Tz. 23] hängt die Ausgestaltung des CMS »insb. von den festgelegten Compliance-Zielen, der Größe des Unternehmens sowie von Art und Umfang der Geschäftstätigkeit des Unternehmens ab«.

Maßnahmen besteht die Gefahr, dass das Thema »in Vergessenheit gerät«, wenn Mitarbeiter nur vereinzelt oder anlassbezogen mit IT-Compliance in Berührung kommen. Als Folge wird von den Mitarbeitern nicht realisiert, dass jede operative Tätigkeit Einfluss auf die IT-Compliance hat. Daher bietet es sich an, mindestens einmal im Jahr in aggregierter Form über den IT-Compliance-Status zu informieren und folgende Fragen zu beantworten:

- Wie hat das Unternehmen seine IT-Compliance-Ziele erreicht?
- Wie sind die IT-Compliance-Ziele der Stakeholder erfüllt worden?
- Wo kann sich das gesamte Unternehmen in seiner IT-Compliance verbessern?

Eine kontinuierliche Kommunikation und ein Informationsaustausch über alle Führungsebenen hinweg sind wichtig für die gelebte IT-Compliance-Kultur. Die IT-Compliance-Kommunikation bedient sich dabei der üblichen Instrumente der internen Unternehmenskommunikation, z. B. Richtlinien, Prozessbeschreibungen, Handbücher oder Newsletter. Die persönliche Kommunikation mit dem IT-Compliance-Manager ist ebenfalls ein wichtiger Kommunikationskanal, der ein offenes Auftreten seitens des ITCM auf der einen Seite und das Vertrauen der Mitarbeiter in die Integrität des ITCM auf der anderen Seite erfordert (vgl. [Hastenrath 2017, S. 102f.]). IT-Compliance muss zudem auch Gegenstand der Mitarbeiterführung sein. Neben bedarfsgerechten Schulungsmaßnahmen müssen die Führungskräfte in der IT und den Fachabteilungen IT-Compliance-Themen kontinuierlich ansprechen und den Stellenwert von IT-Compliance verdeutlichen. Auch die Einrichtung einer Beratungsstelle (Compliance-Helpline), an die sich die Mitarbeiter mit ihren Fragen zu Compliance wenden können (vgl. [Schulz 2017, S. 37]), ist eine sinnvolle Einrichtung, die ggf. mit einer IT-Hotline zu verbinden ist und auch anonym genutzt werden kann.

Die Compliance-Kultur bildet somit das Fundament für sämtliche Aktivitäten zur Erfüllung der Compliance-Ziele. Ebenfalls dem Fundament zuzuordnen ist die Durchführung von umfangreichen Awareness-Maßnahmen. Die Anforderungen zu kennen ist die eine Seite, die andere ist, den Mitarbeiter in die Lage zu versetzen, so zu handeln, dass seine Tätigkeit nicht zu Compliance-Verstößen führt. Diese Verantwortung obliegt nicht allein der IT-Compliance-Funktion. Diese hat die Aufgabe, dem Unternehmen und allen Mitarbeitern IT-Compliance als Thema (z. B. was ist Compliance, die Rolle eines jeden Einzelnen, Definitionen und Erläuterung des IT-CMS, Folgen von Verstößen etc.) näherzubringen. Während generische, d. h. für das gesamte Personal relevante Schulungsbedarfe u. a. vom Compliance-Management oder der CISO-Organisation definiert werden sollten, verbleibt es in Verantwortung der Linienorganisationen, fachspezifische Schulungsbedarfe zu identifizieren. In jedem Fall sollte die fristgerechte und regelmäßige Durchführung von Schulungen durch eine Zentralinstanz (HR- bzw. Personalabteilung) organisiert und hinsichtlich der Teilnahme nachgehalten werden.

Gerade im Bereich der Informationssicherheit gilt es sicherzustellen, dass jedem Mitarbeiter derjenige Wissensumfang vermittelt wird, der für seine Arbeit relevant ist. Dazu gehört auch die Vermittlung von komplexen Richtlinien und Verfahrensanweisungen, vor allem, wenn diese sich ändern. Nicht zuletzt, weil der Gesetzgeber angemessene Schulungsmaßnahmen festschreibt, sollte die IT-Compliance-Funktion darauf hinwirken und überwachen, dass Inhalte durch die jeweiligen Verantwortlichen vermittelt werden. Hierbei können die definierten Handlungsfelder der IT (vgl. Abschnitt 2.6) zur Ableitung der Schulungsinhalte dienen.

In Bezug auf die Gewährleistung der Informationssicherheit wäre es fahrlässig, nur die IT einzubeziehen. Auch zur Sicherstellung der IT-gestützten Compliance sollte in Abstimmung mit der Corporate Compliance ein Schulungsprogramm erstellt werden, sodass auch Mitarbeiter außerhalb der IT verstehen, welche Bedeutung ihr Handeln für die Compliance-Ziele der IT hat. Die meisten Cyberangriffe nehmen ihren Weg in eine Organisation über einen sogenannten »Endpoint«, begünstigt durch Fehler oder Fahrlässigkeit von Endanwendern. Daher stellt eine regelmäßige Mitarbeitersensibilisierung mittels szenario- und rollenspezifischer Schulungen einen wichtigen Baustein im Programm der Compliance-Maßnahmen dar.

Um das Aufdecken von Compliance-Verstößen zu fördern, muss unternehmensweit sichergestellt sein, dass Verstöße im Kontext von dolosen Handlungen (Fraud) zeitnah, konsequent und ohne Berücksichtigung der hierarchischen Position sichtbar geahndet werden. Ein Abweichen von dieser stringenten Linie ist strikt zu vermeiden. Die Sanktionierung von Non-Compliance wird im Unternehmen von den Mitarbeitern aufmerksam verfolgt. Werden Regelverstöße toleriert, entsteht sehr schnell der Eindruck, dass betrügerische Handlungen keine oder nur geringfügige Konsequenzen nach sich ziehen und Compliance nur ein »Lippenbekenntnis« darstellt (vgl. [Schulz 2017, S. 46]).

Mitarbeiter in der IT, die nicht in der zweiten Line nach dem TLM tätig sind, können IT-Compliance-Aufgaben, die mit der eigentlichen Arbeit vermeintlich nicht in Zusammenhang stehen, schnell als lästig empfinden. Trotzdem müssen regelmäßig Schutzbedarfsanalysen, (IT-)Risikobewertungen, (IT-)IKS-Abfragen, (IT-)Compliance-Erhebungen etc. erstellt werden. Ohne detaillierte Informationen zur Zielsetzung, zu Zusammenhängen und zur Abgrenzung der Abfragen bzw. Erhebungen besteht die Gefahr, dass diese als Doppelarbeit oder sinnlose Zulieferung zu Datenfriedhöfen angesehen werden. Im Ergebnis werden die Abfragen mit fehlender Sorgfalt beantwortet, sodass der Informationsgehalt abnimmt und IT-Compliance-Risiken nicht angemessen identifiziert, bewertet und gesteuert werden. Die IT-Compliance-Funktion muss daher die Motivation zum IT-Compliance-Reporting durch eine adäquate Kommunikation sicherstellen und idealerweise die Datenerhebung in den gewohnten Arbeitslauf so integrieren, dass es nicht als Zusatzaufwand wahrgenommen wird.

Teil des IT-Governance- und IT-Managementsystems COBIT 2019 ist die Komponente »Kultur, Ethik und Verhalten«, die als Erfolgsfaktor für IT-Governance- und IT-Managementaktivitäten nicht unterschätzt werden darf (vgl. [ISACA 2018a, S. 22], [Gaulke 2019, S. 7]). Zu dieser Komponente zählt eine Kultur, in der Service Level eingehalten werden und diesbezügliche Non-Compliance sanktioniert wird (nach [ISACA 2018b, S. 117]). COBIT 2019 empfiehlt zudem, das Erreichen von individuellen Leistungszielen mit dem Belohnungs- und Vergütungssystem zu verbinden (vgl. [ISACA 2018b, S. 208]). Dies gilt dann auch für IT-Compliance-Ziele, die die Mitarbeiter zu erreichen haben.

7.3 Identifizierung von Anforderungen für die IT und Ableitung von konkreten Handlungsanweisungen

Die systematische Ableitung von Anforderungen an die IT aus Regelwerken und ihre Überführung in konkrete Handlungsanweisungen ist wesentlicher Bestandteil eines IT-CMS. In der Praxis erweist sich dieser Prozess jedoch als nicht trivial und stellt oftmals aus folgenden Gründen eine Herausforderung dar:

- Die Anzahl der Regelwerke und der in ihnen enthaltenen IT-Anforderungen nimmt kontinuierlich zu, sodass es Unternehmen schwerfällt, alle Anforderungen zu berücksichtigen.
- Es ist nicht immer genau ersichtlich, ob Anforderungen an die IT gerichtet sein könnten.
- Die Formulierungen in gesetzlichen oder regulatorischen Regelwerken sind einem IT-Fachbereich häufig nicht sofort verständlich, sodass dieser sie nicht angemessen umsetzen kann.
- Eine neue Anforderung kann auf alte Regelungen Einfluss haben und erfordert ggf. die Anpassung von Geschäftsprozessen.
- Neue Anforderungen können oft nicht ohne weitere Analysen direkt in eine organisatorische Einheit eingebunden werden und erfordern ggf. ein eigenes Umsetzungsprojekt (z. B. zur Klärung von Zuständigkeiten).

Zusammengefasst deutet die Aufzählung auf die Gefahr hin, dass Anforderungen u. U. unzureichend oder auch gar nicht vom Unternehmen berücksichtigt werden. Daher sollte das IT-CMS einen Prozess enthalten, der die ordnungsmäßige und strukturierte Erhebung und Ableitung von Anforderungen und ihren Auswirkungen auf das Unternehmen sicherstellt. Dieser Prozess besteht im Kern aus folgenden Phasen (vgl. Abbildung 7–1):

1. Um alle relevanten Anforderungen identifizieren zu können, muss die IT-Compliance-Funktion über interne und externe, personelle oder technische Quellen verfügen, die bei der Identifizierung von Anforderungen unterstützen bzw. Neuerungen kommunizieren. Eine konkrete und detaillierte Auseinandersetzung mit neuen Anforderungen ist in diesem Schritt noch nicht erforderlich. Als Quellen für die Identifizierung von Anforderungen können dienen:

   - Interne Informationen und Hinweise durch die Corporate Compliance oder die Rechtsabteilung (kann auch aktuelle Gerichtsurteile einschließen)
   - Externe Rechtsinventare, z. B. mit Nennung von neuen oder angepassten Regelwerken. Hierfür können spezialisierte Dienstleister in Anspruch genommen werden.
   - Kommunikation von Anforderungen auf Basis von Informationen aus Verbänden, Fachzeitschriften, Hinweisen von externen Prüfern, Newslettern von Behörden, Analyse der Webseiten von Behörden, Fortbildungsmaßnahmen (von allen IT-Bereichen)
   - Projekte, die neue Anforderungen aufgreifen
   - Informationen aus dem IT-Vertragsmanagement
   - Berücksichtigung von Stakeholder-Interessen

   Anhand der vorstehenden Beispiele lässt sich ableiten, dass die IT-Compliance-Funktion den Prozess formal gestalten und schriftlich fixieren muss, damit aktiv Informationen an sie herangetragen werden. Die IT-Compliance-Funktion sollte hierbei keine »Holschuld« haben. Alle Verantwortlichen stehen in der Pflicht, das externe sowie interne Umfeld regelmäßig zu überwachen. An dieser Stelle sind wieder die erwähnten Handlungsfelder hilfreich, da die IT-Compliance-Funktion einen Überblick benötigt, welche Themengebiete wesentlich sind. Auf dieser Basis

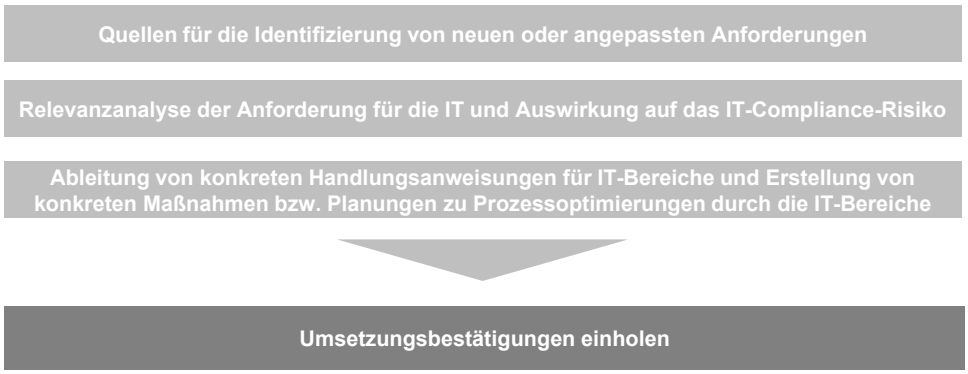


Abb. 7–1: Prozess zur Erhebung und Ableitung von Anforderungen

kann sie prüfen, ob der hier beschriebene Anforderungsidentifikationsprozess effektiv und effizient implementiert ist.

2. Im zweiten Schritt gilt es, IT-Compliance-Anforderungen in den Quellen zu identifizieren und dahingehend zu analysieren, welche Relevanz sie für die IT haben. Die Analyse kann z. B. zu folgenden Ergebnissen führen:

   - Eine Anforderung ist neu und bisher nicht in den Prozessen verankert – Verantwortlichkeit ist geklärt.
   - Eine Anforderung ist neu und bisher nicht in den Prozessen verankert – Verantwortlichkeit ist nicht geklärt.
   - Eine Anforderung ist neu und kann/soll jedoch erst zu einem späteren Zeitpunkt umgesetzt werden.
   - Eine Anforderung ist nicht neu und bereits durch Prozesse abgedeckt.
   - Eine Anforderung hat keinen Einfluss auf die IT.

   Die IT-Compliance-Funktion sollte die Analyse zwar federführend durchführen, jedoch nicht selbstständig ohne Qualitätssicherung und ohne Abstimmung mit den Fachabteilungen und dem Management Entscheidungen zum weiteren Umgang mit neuen Anforderungen treffen. Dies nicht zuletzt deswegen, weil in der Regel die IT-Compliance-Funktion nicht das erforderliche technische Fachwissen vorhält. Wird ein grundsätzlicher Handlungsbedarf festgestellt, ist das IT-Compliance-Risiko zu betrachten. Die Risikoerhebung und -bewertung hat Einfluss auf die konkrete Ausgestaltung des Handlungsbedarfs oder hilft, Priorisierungen für die Umsetzung von Aufgaben vorzunehmen. Folgende Fragen sind hierbei beispielsweise relevant:

   - Mit welchen Konsequenzen ist zu rechnen, wenn neue oder geänderte Vorgaben bzw. Anforderungen nicht, nicht zeitnah oder nur in Teilen umgesetzt werden? Konsequenzen können z. B. sein: negative monetäre oder aufsichtsrechtliche Folgen, Belastung von Kundenbeziehungen, Reputationsverlust, Vertragsverletzung oder Auswirkungen auf Produkte und Dienstleistungen.
   - Was sind die Ursachen, die zu Non-Compliance führen können (in diesem Fall bezogen auf die betroffene Anforderung und das betroffene Handlungsfeld)? Die Ursachenanalyse ist relevant, da daraufhin Maßnahmen und konkrete Handlungen ergriffen werden.

   Die neuen Anforderungen sind mit ihrem Inhalt, Daten zum Regelwerk und der vorgenommenen Bewertung in ein Anforderungsregister aufzunehmen. Dieses sollte auch die Maßnahmen in Bezug auf jede Anforderung beinhalten, sodass ihr gesamter Lebenszyklus dokumentiert und damit nachvollziehbar ist.

3. Basierend auf den Erkenntnissen aus Schritt zwei sind konkrete Handlungsanweisungen abzuleiten, welche die Einhaltung von Anforderungen an die IT sicherstellen. Dabei muss es das Ziel sein, die Anforderungen und Anweisungen möglichst klar, d. h. ohne Interpretationsspielraum, zu beschreiben. Um dies zu erreichen, sollte auf Originalauszüge, z. B. aus Gesetzen, verzichtet werden, da diese für den Fachbereich nur bedingt verständlich sind. Es ist vielmehr Aufgabe der IT-Compliance-Funktion, die Anforderungen gemeinsam mit sachverständigen IT-Experten verständlich zu formulieren. Die Anweisung sollte nicht zu allgemein oder aggregiert formuliert sein. Sie sollte aber auch keine Umsetzungsdetails beinhalten. Folgendes Beispiel verdeutlicht diese Überlegung:

   Die DSGVO sichert jedem Menschen das sogenannte »Recht auf Vergessenwerden« zu, gleichbedeutend mit dem Recht auf unumkehrbare Löschung eigener personenbezogener Daten aus IT-Systemen. Die Fachabteilung sollte sich jedoch nicht mit der DSGVO auseinandersetzen müssen. Vielmehr muss das Informationssicherheitsmanagement die spezifische Anforderung in einer Datenschutzrichtlinie berücksichtigen. In dieser Richtlinie könnte das »Recht auf Vergessenwerden« dann mit folgender Anforderung abgedeckt werden:

   »Systeme, die zur Erfassung, Verarbeitung und Speicherung von personenbezogenen Daten vorgesehen sind, sind entsprechend zu klassifizieren und zu inventarisieren. Für die betroffenen Plattformen sind Löschkonzepte zur Umsetzung der DSGVO zu erarbeiten und umzusetzen. Für Bestandssysteme, bei denen eine Löschung personenbezogener Daten nicht möglich ist oder unverhältnismäßig hohen Aufwand bedeutet, ist eine Risikomeldung abzugeben und eine Entscheidung nachzuhalten.«

4. Kennen die betroffenen Bereiche ihre Aufgabe, so haben sie bestehende Prozesse und deren Dokumentation auf Handlungsbedarf (z. B. Kontrollanpassungen, Prozesserweiterungen) hin zu überprüfen, diesen zu kommunizieren und die Umsetzung zu planen. Hierbei können die betroffenen Fachabteilungen, sofern zutreffend, anerkannte Standards und andere praxisbewährte Verfahren für die Umsetzung der Anforderung heranziehen. Die IT-Compliance-Funktion sollte die Umsetzung der risikominimierenden Maßnahmen und Prozessoptimierungen überwachen und sich die Umsetzung bestätigen lassen.

   Es sollte auch darauf geachtet werden, dass frühzeitig die Auseinandersetzung mit neuen Anforderungen mit wesentlichem Einfluss auf das IT-Compliance-Risiko erfolgt, auch wenn z. B. im Rahmen einer Konsultationsphase Änderungen in der finalen Version eintreten können. Die Dokumentation kann z. B. in Form einer Matrix dargestellt werden (Quellanforderung zu Handlungsanweisung mit Nennung des Verantwortlichen bzw. des Handlungsfelds). Diese Matrix stellt gleichzeitig die Grundlage für die Überwachung durch die IT-Compliance-Funktion dar.

Das generelle Anforderungsmanagement behandelt COBIT 2019 in BAI02.01 (Define and maintain business functional and technical requirements). Compliance wird hier explizit als wichtiger Aspekt bei der Überprüfung der Akzeptanz der Anforderungen angesprochen (vgl. [ISACA 2018b, S. 164]). Die spezielle Identifizierung externer Compliance-Anforderungen ist Inhalt der beiden Praktiken MEA03.01 (Identify external compliance requirements) und MEA03.02 (Optimize response to external requirements). Die Identifizierung externer Compliance-Anforderungen beruht auf der Zuweisung einer Verantwortlichkeit für das Erkennen von neuen oder geänderten IT-bezogenen Anforderungen und beinhaltet eine Auswirkungsanalyse, insbesondere auch für IT-Verträge mit Dritten. Im Ergebnis dieser Praktik sollte das Unternehmen ein Register der Compliance-Anforderungen führen und ein Protokoll der erforderlichen Compliance-Maßnahmen erstellen. Im Rahmen der Reaktion auf externe Anforderungen soll durch Überprüfung und Anpassung von Richtlinien, Prinzipien, Standards, Verfahren und Methoden sichergestellt werden, dass den gesetzlichen, regulatorischen und vertraglichen Anforderungen Rechnung getragen wird. Vor allem sind neue und geänderte Anforderungen an alle relevanten Mitarbeiter zu kommunizieren (nach [ISACA 2018b, S. 285f.]).

7.4 Steuerung von IT-Compliance-Risiken

Das Management der IT-Compliance kann als Ausbalancierung zwischen Compliance-Anforderungen und wirksamer Umsetzung korrespondierender Maßnahmen verstanden werden. Verändern bzw. verschärfen sich die Anforderungen oder erreichen die implementierten Maßnahmen nicht ihre Wirkungsziele, wird diese Balance gestört und es entsteht Non-Compliance. Dieses IT-Compliance-Risiko gilt es, permanent zu überwachen und angemessen zu steuern, z. B. durch geeignete Kontrollen, die den Compliance-Status sichern und damit auch die Umsetzung der Compliance-Ziele gewährleisten. Das interne Kontrollsystem (IKS) in der IT und damit zusammenhängende Prüfungen (Revision oder externe Prüfungen) stellen Informationen zum Design und der Wirksamkeit von Kontrollen bereit.

Zur Erfüllung der Kontrollanforderungen für Compliance-Zielvorgaben sind nach COBIT 2019 die Kontrollaktivitäten wichtiger Geschäftsprozesse zu identifizieren und zu dokumentieren. Hierbei hat eine Priorisierung anhand des inhärenten Geschäftsrisikos zu erfolgen (nach [ISACA 2018b, S. 266]).

Eine permanente Optimierung der Compliance-Maßnahmen soll aber nicht nur auf Basis von Prüfungsergebnissen erfolgen. Die IT-Bereiche sollten angehalten werden, eigene Bewertungen (Self-Assessments) durchzuführen und sich dabei kritisch zu hinterfragen. Das betrifft Bereiche der ersten Linie, aber auch der zweiten Linie. Compliance-Verstöße werden nicht allein durch die operativen Organisationseinheiten der IT verschuldet. In vielen Fällen sind die Vorgaben aus der zweiten Linie nicht in der Form formuliert, dass Vorgaben aus dem Anforderungsregister eingehalten werden können.

Neben den Assessments und Prüfungen trägt gerade in der IT ein wirksames Testmanagement zur Sicherstellung der Compliance bei. Das beinhaltet nicht nur Implementierungstests und Tests im Rahmen von Changes, sondern auch regelmäßige Regressionstests, mithilfe derer bestehende Prozesse und Funktionen überprüft werden.

COBIT 2019 sieht ein Post-Implementation-Review vor (BAI07.08 Perform a post-implementation review), um sicherzustellen, dass Compliance-Anforderungen erfüllt wurden. Auf der anderen Seite weist COBIT 2019 aber auch darauf hin, dass in Bezug auf die Einrichtung einer Testumgebung (BAI07.04 Establish a test environment) die Verwendung von Testdaten ggf. gesetzlichen oder regulatorischen Anforderungen unterliegt, z. B. hinsichtlich der Verwendung bereinigter Daten sowie der Aufbewahrung oder Vernichtung der Testergebnisse (nach [ISACA 2018b, S. 158ff.]).

Wie erwähnt sind Schulungen elementar für die Compliance-Kultur. Regelmäßige Schulungen sensibilisieren und vermitteln erforderliches Wissen, um Prozesse und Kontrollen effektiv durchzuführen, was zur Reduzierung des Compliance-Risikos beiträgt. Allerdings sollten nicht alle Compliance-Risiken als kritisch dargestellt werden. Wenn sich kritische Risiken mit ihren Bedrohungen und Schwachstellen nicht als real erweisen, wird ihre Bedeutung gemindert und die Risiko-Kommunikation verwässert (vgl. [Freund 2020, S. 21]).

Unternehmen, die wesentliche Teile der IT ausgelagert haben, sollten sicherstellen, dass der Dienstleister effektive Kontrollen implementiert hat und durchführt. Mit der Auslagerung werden keine Verantwortlichkeiten delegiert. Das Unternehmen steht weiterhin in der Verantwortung, Compliance sicherzustellen. Hierfür muss das Unternehmen Nachweise über die Ordnungsmäßigkeit des IKS des Dienstleisters einholen. Dies kann mittels unabhängiger Prüfungen durch Wirtschaftsprüfer (z. B. mittels einer Prüfung nach IDW PS 951 oder ISAE 3402) oder ein vertraglich eingeräumtes Prüfungsrecht erfolgen. Von diesem Prüfungsrecht sollte regelmäßig Gebrauch gemacht werden. Neben den Prüfungen bedarf es aber auch einer effektiven Steuerung des Dienstleisters.

7.5 Monitoring und Messung des IT-Compliance-Levels

Compliance-Monitoring zielt darauf ab, den Grad der Konformität messbar zu machen, den Status des IT-Compliance-Risikos zu überwachen und einen Überblick zu verschaffen, ob die Vorgaben zu IT-Compliance eingehalten werden. Zusammengefasst gilt es, Informationen zu erheben, um die Effektivität des IT-CMS zu beurteilen.

Im einfachsten Fall kann der Status mithilfe eines Compliance-Scores, ähnlich einer Schulnote, als Zahl dargestellt werden. Regelmäßig erhoben, erhält die Organisation eine Trendaussage über den Stand der IT-Compliance. Der Compliance-Score kann hierbei aus der Effektivitätsbewertung aller technischen und organisatorischen Maßnahmen, wie z. B. durch

die Überwachungsaktivitäten der IT-Compliance-Funktion, durch Erkenntnisse aus Audits, technisches Monitoring und vor allem aus den Einzelergebnissen der sogenannten Control Assessments, gemessen und aggregiert werden. Bei den Control Assessments handelt es sich um »Eigenprüfungen« oder »Self-Assessments«, die von den Kontrollverantwortlichen durchgeführt werden. Sie finden ergänzend zu den regelmäßigen internen und externen Audits statt. Durch die erhöhte Prüffrequenz lassen sich nachteilige Trends frühzeitig erkennen und handhaben. Unter das oben aufgeführte technische Monitoring fallen Maßnahmen, die sich durch Einsatz von IT-Lösungen automatisch überprüfen lassen. Es handelt sich also in aller Regel um technische Lösungen zur Sammlung und Auswertung von Informationen bzw. Log-Events (z. B. SIEM, Technical Compliance Monitoring, Dokumentenmanagement), die eine eigene Investition oder die Beschaffung als Managed (Security) Service erforderlich machen.

Für die Durchführung des Monitorings ist die Compliance-Funktion auf die Zulieferung der Fachabteilungen und vor allem der weiteren Funktionen der zweiten Linie angewiesen. Auch an dieser Stelle können die definierten Handlungsfelder bei der Strukturierung unterstützen. Die IT-Compliance-Funktion kann erforderliche Informationen für die Durchführung des Monitorings bei den Verantwortlichen abfragen. Der Compliance-Score kann als Zahl gegenüber einem maximal erreichbaren Zielwert dargestellt werden.

Angelehnt an die DIN ISO19600 sind für die Messung der Compliance-Leistung bekannte Compliance-Verstöße, »Beinahverluste« (Verstöße ohne negative Auswirkungen) und eine Einschätzung über die Entwicklung der Compliance-Kultur einzubeziehen (vgl. [DIN ISO 19600:2016, S. 31]). Letztere zu bewerten stellt eine Herausforderung dar. Die Anzahl von Schulungsmaßnahmen ist sicherlich ein Indikator.

Zusammengefasst dienen die Überwachungsaktivitäten dazu, den Status des IT-Compliance-Risikoprofils darzustellen und zu beurteilen, ob sich dieses innerhalb der individuell definierten Wesentlichkeitsgrenzen befindet. Darüber hinaus nehmen die Ergebnisse des Monitorings auf die Außendarstellung des Unternehmens Einfluss und können intern zur Begründung von Investitionen und operativem Aufwand für Compliance-unterstützende Maßnahmen dienen.

Das IT-Compliance-Level des Unternehmens ist auch ein Indikator für die Bewertung des IT-CMS bzw. der IT-Compliance-Funktion an sich, die ebenfalls kritisch hinterfragt werden muss, um sich kontinuierlich weiterzuentwickeln.

Für die Überwachung der IT-Compliance sieht COBIT 2019 in der Praktik MEA03.03 (Confirm external compliance) eine regelmäßige Bewertung der Compliance von Richtlinien, Standards und Verfahren ebenso wie von Geschäfts- und IT-Prozessen mit gesetzlichen, regulatorischen und vertraglichen Anforderungen vor. Hierbei identifizierte Lücken sind zeitnah zu bearbeiten. Zudem ist nach MEA03.04 (Obtain assurance of external compliance) das IT-Compliance-Level auf der Basis von regelmäßigen, ggf. unabhängigen internen und externen Reviews zu bestimmen (nach [ISACA 2018b, S. 286]).

7.6 Kontinuierliche Verbesserungen des IT-CMS

In verschiedenen Standards und Governance-Referenzmodellen (ISO 9001, ISO/IEC 27001, ITIL, COBIT) ist ein kontinuierlicher Verbesserungsprozess (KVP) zur Optimierung der beschriebenen Qualitäts-, Informationssicherheitsmanagement-, IT-Servicemanagement-, IT-Governance- und IT-Managementsysteme integriert und kann insofern auch für das IT-CMS angewendet werden. Ein wesentliches Ziel des KVP ist es, die Eignung, Angemessenheit und Effektivität des IT-CMS zu überprüfen, um die Eintrittswahrscheinlichkeit für eine Nichtkonformität zu verringern und um Maßnahmen zu definieren, welche die IT-Compliance-Prozesse optimieren. Die IT-Compliance-Funktion sollte hierbei u. a. folgende Faktoren berücksichtigen:

- Die Effektivität der eigenen Managementkontrollen (auch die IT-Compliance-Funktion sollte Kontrollen implementiert haben)
- Die Angemessenheit und Aktualität von Richtlinien zu IT-Compliance und zugehörige Arbeitsanweisungen
- Die Zielerreichung der IT-Compliance-Ziele und den Umsetzungsgrad der Compliance-Planung
- Entwicklungen der externen Anforderungen an die Ausgestaltung eines IT-CMS
- Die Optimierung des Compliance Universe durch die Überprüfung der Handlungsfelder
- Ergebnisse aus Prüfungen des IT-CMS

Grundlage der Verbesserung kann eine freiwillige externe Prüfung des IT-CMS auf Basis des IDW PS 980 sein. Die Prüfung wird sich häufig auf die Wirksamkeit des IT-CMS richten, kann aber auch nur als Konzeptions- oder Angemessenheitsprüfung angelegt sein. In den beiden letzten Fällen erhält das Unternehmen eine unabhängige Beurteilung des Entwicklungsstandes des IT-CMS, die als Grundlage von Verbesserungsmaßnahmen dienen kann (vgl. [IDW PS 980, Tz. 14]). Zur Unterstützung der kontinuierlichen Verbesserung des IT-CMS bietet sich der PDCA-Zyklus nach Deming an, unter Berücksichtigung von wenigen, aber zielführenden Key Performance Indicators (KPI). Auf dieser Basis kann ein IT-Compliance-Berichtswesen über den Umsetzungsstand der kontinuierlichen Verbesserung des IT-CMS informieren.

Die kontinuierliche Verbesserung bezieht sich in COBIT 2019 auf das IT-Managementsystem insgesamt (APO01.11 Manage continual improvement of the I&T management system). Grundlage der Verbesserung sind u.a. eine kontinuierliche Leistungsbewertung, die Identifizierung kritischer Prozesse und die Analyse von fehlenden Fähigkeiten oder Lücken in der Überwachung. Verbesserungsmaßnahmen beziehen sich z.B. auf Schulung, Dokumentation, Standardisierung oder Prozessautomatisierung (vgl. [ISACA 2018b, S. 60]). Hinsichtlich der IT-Compliance sollten nach MEA03.03 Richtlinien, Standards, Verfahren und damit verbundene Prozesse und Aktivitäten auf der Grundlage von regelmäßigen Reviews und der daraus gezogenen Schlussfolgerungen kontinuierlich verbessert werden. Hinsichtlich des IT-Compliance-Berichtswesens sollte die Berichterstellung zu gesetzlichen, regulatorischen und vertraglichen Anforderungen auf unternehmensweiter Ebene integriert werden und alle Geschäftsbereiche des Unternehmens einbeziehen (nach [ISACA 2018b, S. 286]).

7.7 Der Umgang mit Non-Compliance und der Einsatz von Korrekturmaßnahmen im IT-CMS

Abweichungen von festgelegten Compliance-Vorgaben können immer wieder aus unterschiedlichen Gründen auftreten (z.B. Datenmissbrauch, Korruption, unabsichtliche Regelbrüche). Diese Nichtkonformität ist häufig aber kein Anzeichen dafür, dass das IT-CMS ineffektiv ist. Anders ausgedrückt erweist sich ein IT-CMS gerade dann als effektiv, wenn es zur Aufdeckung von Compliance-Verstößen beiträgt. Oft können Abweichungen dazu genutzt werden, das vorhandene IT-CMS zu verbessern. Folgende Schritte sind zu empfehlen (in Anlehnung an [DIN ISO 19600:2016, S. 37]):

(1) Kurzfristige Reaktion auf Nichtkonformität (Kontrollieren oder Korrigieren der Abweichung und die Konsequenzen dieser Entscheidung managen)
(2) Review der Abweichung
    a. Ursachenanalyse
    b. Risikoanalyse und Entscheidung über Risikobehandlung (Korrekturmaßnahmen)
(3) Implementierung von Korrekturmaßnahmen
(4) Bewertung der Effektivität von Korrekturmaßnahmen
(5) Anpassung des IT-CMS

Grundsätzlich sollte der Umgang mit Abweichungen auf Basis der Vorgaben der Corporate-Ebene erfolgen. Zu berücksichtigen beim Einsatz von Korrekturmaßnahmen ist, dass die durchzuführenden Maßnahmen hinsichtlich des Ressourceneinsatzes (Budget, Personalkraft, Materialeinsatz etc.) zur Abwehr oder Reduzierung der Nichtkonformität den eigentlichen Ressourceneinsatz für die Beibehaltung der Nichtkonformität nicht übersteigen. Eine Kosten-Nutzen-Analyse bei der Bestimmung von Korrekturmaßnahmen sollte daher stets zugrunde gelegt und dem Risiko gegenübergestellt werden. Auf den ersten Blick scheint die Umsetzung von Anforderungen häufig zwingend zu sein. In der Praxis jedoch wird ein »100%-Compliance-Status« kaum erreicht werden können. Es ist legitim, dass sich z.B. ein Finanzdienstleister die Frage stellt, ob die Anschaffung einer teuren IT-Anwendung zweckmäßig ist, um einen seltenen Haftungsfall aus dem Zivilrecht zu vermeiden, bei dem der Geschädigte (der erst Klage erheben muss) Anspruch auf einen geringen Schadensersatz hat. Dies soll nicht zu Non-Compliance animieren, sondern eine Fragestellung thematisieren, die in der Praxis täglich gestellt wird. Die IT-Compliance-Funktion muss sensibilisiert werden, abzuwägen, welche Optimierungsvorschläge unter Beachtung des Compliance-Risikos betriebswirtschaftlich sinnvoll sind, um nicht »über das Ziel hinauszuschießen«.

Jede Abweichung und die damit verbundene Behandlungs- oder Akzeptanzentscheidungen sind nachprüfbar zu dokumentieren. Gegebenenfalls ist das Unternehmen auch gesetzlich dazu verpflichtet, die Abweichung an eine öffentliche Einrichtung oder Aufsicht zu melden. Beispielsweise ist für KRITIS-Betreiber nach § 8b Abs. 4 BSIG bei erheblichen Störungen eine Meldung an das BSI vorgeschrieben. Dies kann in manchen Fällen auch freiwillig erfolgen, um von der öffentlichen Einrichtung Unterstützung bei Korrekturen zu erhalten. Da ein Bekanntwerden in der Öffentlichkeit i.d.R. bei größeren Vorfällen nicht zu vermeiden ist – allein schon, weil oftmals auch Kunden informiert werden müssen –, ist es wichtig, die externe Kommunikation zu steuern. Für eine ggf. erforderliche professionelle Krisenkommunikation sollten Unternehmensleitung, PR-Abteilung, Rechtsabteilung, Corporate Compliance/IT-Compliance und Datenschutz in einer Taskforce zusammenarbeiten. Idealerweise sollten für derartige Situationen Szenarien mit vorbereiteten Kommunikationsstrategien vorliegen (nach [Bensinger 2017, S, 744f.]).

Die Erkenntnisse aus einer Abweichung sollen auch dazu genutzt werden, um:

- die Produkte und Service-Performance zu überprüfen,
- eine Verbesserung oder ein Redesign von Produkten oder Services vorzunehmen,
- eine Änderung von organisatorischen Praktiken und Vorgehensweisen zu initiieren,
- Trainings von Mitarbeitern durchzuführen und die Compliance-Kultur zu fördern,
- Informationsketten zu bewerten,
- frühzeitige Warnungen und Alarmmeldungen neu einzuführen oder zu optimieren,
- ein Redesign oder Review von vorhandenen Kontrollen vorzunehmen (ggf. ist auch der verantwortliche Bereich dahingehend zu sensibilisieren, die Durchführung der Control Assessments zu optimieren) und/oder
- Eskalationssysteme (intern und extern) zu überarbeiten.

Letzteres sollte klar kommuniziert und dokumentiert werden, damit jede Nichtkonformität an verantwortliche Führungskräfte berichtet wird, die entsprechende Compliance-Funktion angemessen informiert werden kann und entsprechende Korrekturmaßnahmen mit Unterstützung durchgesetzt werden können. Hierzu ist es notwendig, dass ein effektives IT-CMS einen Mechanismus enthält, der es Mitarbeitern auf jeder Organisationsstufe ermöglicht, verdächtige Abweichun-

gen oder Verstöße auf vertraulicher Basis melden zu können, ohne negative Folgen fürchten zu müssen. Dies ist die Anforderung des Art. 19 Nr.1 der sogenannten Whistleblowing-Richtlinie der EU[3], die sich ausdrücklich auch gegen Verstöße in den Bereichen Schutz der Privatsphäre, Datenschutz und Sicherheit von Netz- und Informationssystemen richtet.

Nach COBIT 2019 sind Verfahren zur Aufrechterhaltung der Compliance mit Richtlinien und anderen Komponenten des Kontrollrahmenwerks erforderlich (APO01.09 Define and communicate policies and procedures). Insbesondere wird die Durchsetzung von Konsequenzen bei Non-Compliance gefordert. Auf der anderen Seite sind i. S. von Korrekturmaßnahmen aber auch die Richtlinien zumindest jährlich zu evaluieren und ggf. an das sich ändernde Betriebs- oder Geschäftsumfeld anzupassen (nach [ISACA 2018b, S. 59]).

[3] Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

Handlungsempfehlungen

- Orientieren Sie sich bei der Ausgestaltung des IT-CMS am unternehmensweiten CMS.
- Nutzen Sie für die Strukturierung Ihres IT-CMS verbreitete Standards und Normen, insbesondere den IDW PS 980 oder die Norm DIN ISO 19600.
- Klären Sie, welche Werte, Einstellungen und Verhaltensweisen die gewünschte IT-Compliance-Kultur umfassen soll.
- Sorgen Sie für ein entsprechendes Engagement der Unternehmensleitung, der IT-Leitung und der Leitungen der Fachabteilungen.
- Eine Awareness für IT-Compliance erfordert neben Informations- und Schulungsmaßnahmen das Engagement der Unternehmensleitung, des IT-Compliance-Managers und der Führungskräfte in der IT sowie den Fachabteilungen.
- Compliance-Anforderungen sind klar und verständlich zu erfassen, in einem Anforderungsregister zu dokumentieren und an die betroffenen Stellen zu kommunizieren.
- Sorgen Sie dafür, dass Mitarbeiter Fälle von Non-Compliance melden können, ohne dass sie Nachteile befürchten müssen.
- Stellen Sie sicher, dass aufgedeckte Non-Compliance konsequent und sichtbar sanktioniert wird.
- Im Rahmen eines kontinuierlichen Verbesserungsprozesses sollte die Eignung, Angemessenheit und Effektivität des IT-CMS gemessen und optimiert werden.
- Vor Ergreifen einer Korrekturmaßnahme infolge von Non-Compliance müssen Aufwand und Nutzen der Maßnahme abgewogen werden.
- Bereiten Sie für Fälle erheblicher Non-Compliance eine Strategie für die externe Kommunikation vor.

8 Ausblick

Auf die Treiber von IT-Compliance wurde bereits zu Beginn dieses Leitfadens eingegangen. Es dürften sich alle Compliance-Beteiligten einig sein, dass eine Tendenz zu einem immer stärker regulierten IT-Umfeld mit immer anspruchsvolleren Anforderungen besteht. Die Geschwindigkeit, mit der neue, Compliance-relevante Informationstechnologien auftreten, und ihre Möglichkeiten zur Einflussnahme auf Gesellschaft, Unternehmen und Arbeitnehmer erhöhen den Stellenwert der IT-Compliance in Unternehmen. Die Frage »Quo vadis IT-Compliance?« wird sowohl die Verantwortlichen für IT-Compliance als auch die sonstigen von IT-Compliance betroffenen Personen und Gruppen weiterhin beschäftigen. Der Druck auf die Unternehmen, vor allem auf Dienstleister im Rahmen einer Auslagerung, ein ordnungsgemäßes IT-Compliance-Management-System vorzuhalten, wird stetig zunehmen. Mit der neuen ISO 37301 (ersetzt die ISO 19600) besteht ab 2021 die Möglichkeit, Compliance-Management-Systeme zertifizieren zu lassen, um eben jene Ordnungsmäßigkeit nachzuweisen. Darüber hinaus ergibt sich für die nähere Zukunft die Aufgabe der Integration der verschiedenen IT-Managementsysteme (IT-CMS, ISMS etc.) mit dem IT-Kontrollsystem. Hier kann COBIT 2019 helfen, eine Abstimmung sowohl hinsichtlich der verschiedenen Governance-Komponenten als auch in Bezug auf Performance-Management, Audit und Berichterstattung zu bewerkstelligen (vgl. [Steuperaert 2019, S. 19]).

Es werden neue Themen stärker in den Fokus rücken, wie z.B. Artificial Intelligence, Machine Learning oder Kryptowährungen. Normative und regulative Anforderungen müssen diesbezüglich angepasst bzw. neu geschaffen werden. In der Folge bedarf es stärker als in der Vergangenheit einer engen Zusammenarbeit und Abstimmung zwischen IT-Compliance und weiteren Funktionen wie IT-Security und Corporate Compliance, um komplexer werdende Anforderungen zu interpretieren und ordnungsgemäß im Unternehmen zu berücksichtigen. In der Konsequenz zeichnet es sich ab, dass das IT-Compliance-Risiko stetig zunehmen wird und dessen Beurteilung vertieftes IT-Expertenwissen erfordert. Wird man als Unternehmen dieser Herausforderung nicht gerecht, so sind hohe Sanktionen bzw. Strafzahlungen, wesentliche Prüfungsfeststellungen oder auch Lizenzentzüge die Folge. Zudem bieten ineffektive Strukturen für IT-Compliance ein höheres Bedrohungspotenzial für Fraud. Als Chance steht diesen Gefahren allerdings ein Wettbewerbsvorteil gegenüber, da ein Unternehmen mit entsprechender IT-Compliance Markteintrittsbarrieren überwinden und in der Außenwirkung Vorteile erlangen kann.

Abschließend kann an dieser Stelle zur Risikofrage aufgeführt werden, dass bei allen Anstrengungen eines Unternehmens die Personalpolitik einen wesentlichen Faktor darstellt. Für erfahrene Spezialisten aus den hier beispielhaft aufgeführten Gebieten müssen Mittel bereitgestellt werden. Einsparungsvorhaben zulasten einer angemessenen Ressourcenausstattung für IT-Compliance und sonstiger Governance-Funktionen werden in Zukunft genauer begründet werden müssen.

IT-Compliance erfordert eine kontinuierliche Fort- und Weiterbildung, um sich auf dem Laufenden zu halten. Nicht nur hinsichtlich der verschiedenen Regelwerke, sondern auch in Bezug auf Methoden und Techniken des Managements der IT-Compliance. Die ISACA wird ihre Mitglieder hierin weiter mit Seminaren, Zertifizierungen und Publikationen – nicht zuletzt in der Zeitschrift »IT-Governance« – unterstützen.

Abkürzungsverzeichnis

3D	dreidimensional
A	Accountable
AG	Alignment Goal
AGB	Allgemeine Geschäftsbedingungen
AIM	Access & Identity Management
AktG	Aktiengesetz
AO	Abgabenordnung
APO	Align, Plan and Organise
ArbStättV	Arbeitsstättenverordnung
Art.	Artikel
AT	Allgemeiner Teil
B2B	Business-to-Business
BaFin	Bundesanstalt für Finanzdienstleistungs-aufsicht
BAI	Build, Aquire and Implement
BAIT	Bankaufsichtliche Anforderungen an die IT
BAK	Branchenarbeitskreis
BCM	Business Continuity Management
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BilMoG	Bilanzrechtsmodernisierungsgesetz
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BMF	Bundesministerium für Finanzen
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	BSI-Kritisverordnung
BYOD	Bring your own device
C	Chief
CAD	Computer Aided Design
CAPEX	capital expenditure
CCO	Corporate / Chief Compliance Officer
CCTA	Central Computer and Telecommunications Agency
CDD	Compliance Due Diligence
CDN	Content Delivery Network
CDO	Chief Digital Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMI®	Capability Maturity Model Integration
CMS	Compliance-Management-System
COBIT®	Control Objectives for Information and Related Technology
CON	Konzeption und Vorgehensweisen
COO	Chief Operating Officer
COSO	Committee of Sponsoring Organizations
CRD	Capital Requirements Directive
CRM	Customer Relationship Management
CRO	Chief Risk Officer
CRR	Capital Requirements Regulation
CSA	Cloud Security Alliance
DCGK	Deutscher Corporate Governance Kodex
DE	Deutsch
DIIR	Deutsches Institut für Interne Revision e. V.
DIN	Deutsches Institut für Normung e. V.
D&O	Directors & Officers
DSB	Datenschutzbeauftragter
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DSS	Deliver, Service and Support
DV	Datenverarbeitung
EAM	Enterprise Architecture Management
EBA	European Banking Authority
E-Commerce	Electronic Commerce
EDM	Evaluate, Direct and Monitor
E-Mail	Electronic Mail
EN	Europäische Norm
ERM	Enterprise Risk Management
EStG	Einkommenssteuergesetz
ET	Enforcement Tracker
EU	Europäische Union
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen

FAIT	Fachausschuss für die Informationstechnologie
FG	Fachgruppe
F&E	Forschung und Entwicklung
G20	Gruppe der Zwanzig (wichtigsten Industrie- und Schwellenländer)
GDPR	General Data Protection Regulation
GL	Guideline
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
GRC	Governance, Risk, Compliance
HEG-KI	Hochrangige Expertengruppe für KI
HGB	Handelsgesetzbuch
HR	Human Resources
ICT	Information and Communication Technology
IDW	Institut der Wirtschaftsprüfer in Deutschland
IEC	International Electrotechnical Commission
IIA®	Institute of Internal Auditors®
IKS	Internes Kontrollsystem
IP	Intellectual Property
ISA	International Standard on Auditing
ISACA	Information Systems Audit and Control Association
ISAE	International Standard on Assurance Engagements
ISF	Information Security Forum
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
I&T	Information and Technology
IT	Informationstechnologie
ITCM	IT-Compliance-Manager
ITGI	IT Governance Institute
ITIL®	Information Technology Infrastructure Library
ITSM	IT-Servicemanagement
kDL	kritische Dienstleistung
KG	Kommanditgesellschaft
KI	Künstliche Intelligenz
KPI	Key Performance Indicator
KRITIS	Kritische Infrastrukturen
KVP	Kontinuierlicher Verbesserungsprozess
KWG	Kreditwesengesetz
MaGo	Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen
MaRisk	Mindestanforderungen an das Risikomanagement
MEA	Monitor, Evaluate and Assess
NIA	Normenausschuss Informationstechnik und Anwendungen
NIS	Netz- und Informationssicherheit
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
OLG	Oberlandesgericht
OPEX	operational expenditure
OWiG	Gesetz über Ordnungswidrigkeiten
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan – Do – Check – Act
PMBOK® Guide	A Guide to the Project Management Body of Knowledge
PR	Public Relations
PS	Prüfungsstandard
R	Responsible
RACI	Responsible, Accountable, Consulted, Informed
ROI	Return on Investment
RS	Stellungnahme zur Rechnungslegung
SEC	Security and Exchange Commission
SFIA®	Skills Framework for the Information Age
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOX	Sarbanes-Oxley Act
SPEC	Specification
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism
STAR	Security, Trust and Assurance Registry
StGB	Strafgesetzbuch
TLM	Three Lines Model
TMG	Telemediengesetz
TOGAF®	The Open Group Architecture Framework
TOM	technisch-organisatorische Maßnahmen
UP	Umsetzungsplan
UrhG	Urheberrechtsgesetz
US	United States
USA	United States of America
USA Freedom Act	Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act

USA Patriot Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
UStG	Umsatzsteuergesetz
VAG	Versicherungsaufsichtsgesetz
VAIT	Versicherungsaufsichtliche Anforderungen an die IT
VerSanG	Gesetz zur Sanktionierung von verbandsbezogenen Straftaten im Rahmen des Entwurfs eines Gesetzes zur Stärkung der Integrität in der Wirtschaft
WpHG	Wertpapierhandelsgesetz

Quellenverzeichnis

[BaFin 2017a] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Anlage 1: Erläuterungen zu den MaRisk in der Fassung vom 27.10.2017, online unter: *https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba.pdf?__blob=publicationFile&v=5* (letzter Abruf: 08.10.2020).

[BaFin 2017b] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): BAIT: BaFin veröffentlicht Anforderungen an die IT von Banken, 06.11.2017, online unter: *https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171106_BAIT.html;jsessionid=D4B65F00C54BF8EC9D542349431E1B1D.1_cid298* (letzter Abruf: 08.10.2020).

[BaFin 2018a] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Digitalisierungsstrategie der BaFin, August 2018, online unter: *https://www.bafin.de/SharedDocs/Downloads/DE/dl_digitalisierungsstrategie.pdf?__blob=publicationFile&v=5* (letzter Abruf: 08.10.2020).

[BaFin 2018b] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter, November 2018, online unter: *https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/BA/dl_181108_orientierungshilfe_zu_auslagerungen_an_cloud_anbieter_ba.pdf?__blob=publicationFile&v=4* (letzter Abruf: 08.10.2020).

[BaFin 2018c] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018, online unter: *https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=9* (letzter Abruf: 08.10.2020).

[Behringer 2013] Behringer, Stefan: Die Organisation von Compliance in Unternehmen. In: Behringer, Stefan (Hrsg.): Compliance kompakt – Best Practice im Compliance-Management. 3. Aufl., ESV Erich Schmidt Verlag, Berlin, 2013, S. 376-384.

[Bensinger 2017] Bensinger, Viola: Cybersecurity, IT-Sicherheit und Krisenmanagement. In: Schulz, Martin R. (Hrsg.): Compliance Management im Unternehmen – Strategie und praktische Umsetzung. Deutscher Fachverlag, Frankfurt/M., 2017, S. 721-746.

[Bitkom/DIN 2020] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom); Deutsches Institut der Normung e.V. (DIN), Normenausschuss Informationstechnik und Anwendungen (NIA): ISO/IEC 27001 Information security management systems – Requirements / Informationssicherheitsmanagementsysteme – Anforderungen, online unter: *https://kompass-sicherheitsstandards.de/Allgemeine-ISMS/ISO-IEC-27001* (letzter Abruf: 08.10.2020).

[BMF 2019] Bundesministerium für Finanzen (BMF): Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD), Schreiben vom 28.11.2019, online unter: *https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf?__blob=publicationFile&v=9* (letzter Abruf: 08.10.2020).

[Böhm 2008] Böhm, Markus: IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT. HMD – Praxis der Wirtschaftsinformatik, Jg. 45 (2008), Heft 263, S. 15-29.

[Boeselager 2018] Boeselager, Friedrich von: Der Chief Digital Officer. Springer, Wiesbaden, 2018.

[BSI 2017] Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0 vom Oktober 2017, online unter: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7* (letzter Abruf: 08.10.2020).

[BSI 2019] Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): Baustein CON.6 Löschen und Vernichten. In: IT-Grundschutz-Kompendium, Edition 2019, online unter: *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_6_L%C3%B6schen_und_Vernichten.html* (letzter Abruf: 08.10.2020).

[Bürkle 2016] Bürkle, Jürgen: Compliance-Beauftragten-System. In: Hauschka, Christoph E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 3. Aufl., Beck, München, 2016, S. 1152-1184.

[DCGK 2019] Regierungskommission Deutscher Corporate Governance Kodex (Hrsg.): Deutscher Corporate Governance Kodex, in der Fassung vom 16. Dezember 2019, online unter: *http://www.dcgk.de/de/kodex/aktuelle-fassung/praeambel.html* (letzter Abruf: 08.10.2020).

[Deloitte 2019] Deloitte (Hrsg.): Künstliche Intelligenz im Compliance-Umfeld von Banken & Co. Whitepaper der Deloitte Touche Tohmatsu Limited, 2019, online unter: *https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Whitepaper-K%C3%BCnstliche-Intelligenz-im-Compliance-Umfeld-von-Banken-und-Co.pdf* (letzter Abruf: 08.10.2020).

[DIN EN ISO/IEC 27001:2017] Informationstechnik – Sicherheitsverfahren –Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015), deutsche Fassung der ISO/IEC 27001:2013, Ausgabedatum 2017-06.

[DIN EN ISO/IEC 27002:2017] Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015), deutsche Fassung der ISO/IEC 27002:2013, Ausgabedatum 2017-06.

[DIN ISO 19600:2016] Compliance-Managementsysteme – Leitlinien (ISO 19600:2014), deutsche Fassung der ISO 19600:2014, Ausgabedatum 2016-12.

[DIN SPEC 66399-3:2013] *Büro- und Datentechnik* – Vernichten von Datenträgern – Teil 3: Prozess der Datenträgervernichtung, Ausgabedatum 2013-02.

[DSGVO 2018] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), online unter: *https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE* (letzter Abruf: 08.10.2020).

[DSK 2019] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, online unter: *https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf* (letzter Abruf: 08.10.2020).

[Egner 2011] Egner, Thomas: Begriff, Zielsetzung und Aufgaben. In: Freidank, Carl-Christian; Peemöller, Volker H. (Hrsg.): Kompendium der Internen Revision – Internal Auditing in Wissenschaft und Praxis. ESV Erich Schmidt Verlag, Berlin, 2011, S. 3-32.

[Eulerich 2020] Eulerich, Marc: Das neue Three Lines Model – Gemeinsamkeiten und Unterschiede zu den Three Lines of Defense. ZIR – Zeitschrift Interne Revision, Jg. 55 (2020), Nr. 5, S. 208-216.

[EVB-IT Instandhaltungs-AGB 2016] Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen, Version 2.0 vom 17.03.2016, online unter: *https://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Instandhaltung/ergaenzende_vertragsbedinungen_version_2-0_v_17032016_pdf.pdf?__blob=publicationFile* (letzter Abruf: 08.10.2020).

[Falk 2012] Falk, Michael: IT-Compliance in der Corporate Governance – Anforderungen und Umsetzung. Springer Gabler, Wiesbaden, 2012.

[Freund 2020] Freund, Jack: Communicating Technology Risk to Nontechnical People. ISACA Journal, 2020, Nr. 3, S. 20-27.

[Fröhlich 2019] Fröhlich, Martin: IT-Prüfung – Prüfung von Blockchain-Anwendungen. IT-Governance, Jg. 13 (2019), Nr. 30, S. 26-32.

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

[Gaulke 2020] Gaulke, Markus: Praxiswissen COBIT – Grundlagen und praktische Anwendung in der Unternehmens-IT. 3. Aufl., dpunkt.verlag, Heidelberg, 2020.

[GDPR ET] CMS Hasche Sigle GmbH (Hrsg.): GDPR Enforcement Tracker, online unter: *http://www.enforcementtracker.com/* (letzter Abruf: 08.10.2020).

[Gruber et al. 2013] Gruber, Jörg; Bewernick, Martin; Kempelmann, Klaus: Achtung Compliance: Was der berufliche Einsatz privater Endgeräte von Unternehmen und Mitarbeitern fordert. IT-Governance, Jg. 7 (2013), Nr. 14, S. 13-17.

[Gründer 2016] Gründer, Torsten: Risikomanagement und IT-Sourcing – ein kritischer Praxisexkurs. IT-Governance, Jg. 10 (2016), Nr. 23, S. 25-29.

[Hastenrath 2017] Hastenrath, Katharina: Kommunikationsmanagement und Schulungen. In: Schulz, Martin R. (Hrsg.): Compliance Management im Unternehmen – Strategie und praktische Umsetzung. Deutscher Fachverlag, Frankfurt/M., 2017, S. 93-134.

[Hauschka et al. 2016] Hauschka, Christoph E.; Moosmayer, Klaus; *Lösler, Thomas*: § 1, Einführung. In: Hauschka, Christoph E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 3. Aufl., Beck, München, 2016, S. 1-32.

[Heese/Fröhlich 2013] Heese, Klaus; Fröhlich, Martin: Bedeutung von IT und Organisation in Unternehmen. Die Wirtschaftsprüfung (WPg), Jg. 66 (2013), Nr. 12, S. 547-564.

[HEG-KI 2018] Hochrangige Expertengruppe für KI (HEG-KI): Ethik-Leitlinien für eine vertrauenswürdige KI. Europäische Kommission, Brüssel, 2018, online unter: *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425* (letzter Abruf: 08.10.2020).

[Ho 2018] Ho, Amelia: Roles of Three Lines of Defense for Information Security and Governance. ISACA Journal, 2018, Nr. 4, S. 38-42.

[IIA 2013] The Institute of Internal Auditors (IIA): The Three Lines of Defense in Effective Risk Management and Control. Position paper, 2013, online unter: *https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf* (letzter Zugriff am 08.10.2020).

[IIA 2020] The Institute of Internal Auditors (IIA): The IIA´s Three Lines Model – An update of the Three Lines of Defense, July 2020, online unter: *https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf* (letzter Zugriff am 08.10.2020).

[IDW PS 860] Institut der Wirtschaftsprüfer in Deutschland (Hrsg.): IDW PS 860 Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung, Stand: 02.03.2018.

[IDW PS 980] Institut der Wirtschaftsprüfer in Deutschland (Hrsg.): IDW PS 980 Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, Stand: 11.03.2011.

[IDW RS FAIT 1] Institut der Wirtschaftsprüfer in Deutschland (Hrsg.): IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), Stand: 24.09.2002.

[ISACA 2012] Information Systems Audit and Control Association (ISACA): COBIT® 5 – A Business Framework for the Governance and Management of Enterprise IT. ISACA, Rolling Meadows, 2012.

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

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

[ISACA 2018c] Information Systems Audit and Control Association (ISACA): COBIT 2019® – Design Guide: Designing an Information and Technology Governance Solution. ISACA, Schaumburg, 2018.

[ISACA 2018d] Information Systems Audit and Control Association (ISACA): COBIT 2019® – Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution. ISACA, Schaumburg, 2018.

[ISACA-FG IT-Revision 2015] ISACA-Fachgruppe IT-Revision: Grundlagen und Standards in der IT-Revision – ein Überblick. IT-Governance, Jg. 9 (2015), Nr. 21, S. 23-27.

[ITGI 2001] IT Governance Institute (Hrsg.): Board Briefing on IT Governance. IT Governance Institute (ITGI), Rolling Meadows, 2001.

[Jacobs 2017] Jacobs, Sven: IT-Compliance – Software-Lizenzmanagement, IT-Sicherheit und Blockchain. In: Schulz, Martin R. (Hrsg.): Compliance Management im Unternehmen – Strategie und praktische Umsetzung. Deutscher Fachverlag, Frankfurt/M., 2017, S. 695-720.

[Johannsen/Goeken 2011] Johannsen, Wolfgang; Goeken, Matthias: Referenzmodelle für IT-Governance – Strategische Effektivität und Effizienz mit COBIT, ITIL & Co. 2. Aufl., dpunkt.verlag, Heidelberg, 2011.

[Klotz 2007] Klotz, Michael: IT-Compliance – auf den Kern reduziert. IT-Governance, Jg. 1 (2007), Nr. 1, S. 14-18, online unter: *https://www.researchgate.net/publication/333173015_IT-Compliance_-_auf_den_Kern_reduziert* (letzter Abruf: 08.10.2020).

[Klotz 2008] Klotz, Michael: IT-Governance genormt – die neue ISO/IEC 38500. IT-Governance, Jg. 2 (2008), Nr. 1, S. 21-23, online unter: *https://www.researchgate.net/publication/333428759_IT-Governance_genormt_-_die_neue_ISOIEC_38500* (letzter Abruf: 08.10.2020).

[Klotz 2009] Klotz, Michael: IT-Compliance – Ein Überblick. dpunkt.verlag, Heidelberg, 2009, online unter: *https://www.researchgate.net/publication/333023584_IT-Compliance_-_Ein_Uberblick* (letzter Abruf: 08.10.2020).

[Klotz 2012] Klotz, Michael: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke. 2., überarb. u. erw. Aufl. SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, Jg. 4 (2012), Nr. 20, DOI: 10.13140/RG.2.2.15306.62409.

[Klotz 2014] Klotz, Michael: IT-Compliance nach COBIT – Gegenüberstellung zwischen COBIT 4.0 und COBIT 5. SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, Jg. 6 (2014), Nr. 25, DOI: 10.13140/RG.2.2.11178.57286/1.

[Klotz 2016a] Klotz, Michael: IT-Governance genormt – die neue ISO/IEC 38500 (reloaded). IT-Governance, Jg. 10 (2016), Nr. 24, S. 25-27, online verfügbar unter: *https://www.researchgate.net/publication/333428759_IT-Governance_genormt_-_die_neue_ISOIEC_38500* (letzter Abruf: 08.10.2020).

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

[Klotz 2018] Klotz, Michael: Aufgaben, organisatorische Einordnung und Qualifikation des IT-Compliance-Managers in der Praxis. IT-Governance, Jg. 12 (2018), Nr. 28, S. 15-21.

[Klotz 2019] Klotz, Michael: IT-Compliance nach COBIT® 2019. SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: Hochschule Stralsund, SIMAT Stralsund Information Management Team, Jg. 11 (2019), Nr. 34, DOI: 10.13140/RG.2.2.34583.11687/1.

[Klotz 2020] Klotz, Michael: IT-Compliance. In: Tiemeyer, Ernst (Hrsg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 7. Aufl., Hanser, München, 2020, S. 841-884.

[Klotz/Dorn 2008] Klotz, Michael; Dorn, Dietrich-W.: IT-Compliance – Begriff, Umfang und relevante Regelwerke. HMD – Praxis der Wirtschaftsinformatik, Jg. 45 (2008), Nr. 263, S. 5-14.

[Klotz/Dorn 2016] Klotz, Michael; Dorn, Dietrich-W.: Vertragsmanagement in der IT – Standards, Konzeption, Aufgaben und Vertragsarten. 2., neu bearb. Aufl., ESV Erich Schmidt Verlag, Berlin, 2016.

[Knoll 2019] Knoll, Matthias: Praxisorientiertes IT-Risikomanagement – Konzeption, Implementierung und Überprüfung. 2. Aufl., dpunkt.verlag, Heidelberg, 2019.

[Knoll/Bank 2015] Knoll, Matthias; Bank, Markus: Ein Blick zurück in die Zukunft der IT-Revision – Warum die IT-Revision schon immer wichtig war und heute unverzichtbar ist. ZIR – Zeitschrift Interne Revision, Sonderheft, Nr. 1, 2015, S. 27-36.

[Kochanek 2018] Kochanek, Thomas: Das NIST Cybersecurity Framework in der Praxis: »Framework for Improving Critical Infrastructure Cybersecurity«. IT-Governance, Jg. 12 (2018), Nr. 27, S. 13-18.

[Langenbucher et al. 2019] Langenbucher, Katja; Hoger, Andreas; Lauterwein, Constantin: Compliance Due Diligence bei M&A-Transaktionen zunehmend institutionalisiert. Compliance Due Diligence Studie 2019, online unter: *https://www.hengeler.com/fileadmin/user_upload/PDF/Artikel/2019-07_ComplianceDD-Studie_DE.pdf* (letzter Abruf: 08.10.2020).

[Mertmann/Scharr] Mertmann, Dorothea; Scharr, Christoph: Die Interne Revision in Deutschland – Dritte Verteidigungslinie der Corporate Governance. IT-Governance, Jg. 10 (2016), Nr. 24, S. 3-9.

[Nestler/Modi 2019] Nestler, Diana; Modi, Julian: Leitfaden IT-Compliance – Anforderungen, Chancen und Umsetzungsmöglichkeiten. IDW Verlag, Düsseldorf, 2019.

[OECD 2015] OECD (Hrsg.): Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. OECD Publishing, Paris. DOI: *http://dx.doi.org/10.1787/9789264245471-en*.

[OLG Hamm 2003] Oberlandesgericht Hamm, Urteil vom 01.12.2003, Az. 13 U 133/03.

[Pearce 2019] Pearce, Guy: Reporting on GDPR Compliance to the Board. ISACA Journal, 2019, Nr. 1, S. 32-39.

[Rath/Sponholz 2014] Rath, Michael; Sponholz, Rainer: IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen. 2. Aufl., ESV Erich Schmidt Verlag, Berlin, 2014.

[Reffgen 2019] Reffgen, Carsten: Versicherungsaufsichtliche Anforderungen an die IT. IT-Governance, Jg. 13 (2019), Nr. 29, S. 29-32.

[Rüter et al. 2006] Rüter, Andreas; Schröder, Jürgen; Göldner, Axel (Hrsg.): IT-Governance in der Praxis. Springer, Berlin, Heidelberg, 2006.

[Schmidt 2016] Schmidt, Stefan: Wirtschaftsprüfung und CMS-Prüfung. In: Hauschka, Christoph E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 3. Aufl., Beck, München, 2016, S. 1406-1451.

[Schulz 2017] Schulz, Martin R.: Compliance-Management – Grundlagen, Zusammenhänge und Strategien. In: Schulz, Martin R. (Hrsg.): Compliance Management im Unternehmen – Strategie und praktische Umsetzung. Deutscher Fachverlag, Frankfurt/M., 2017, S. 1-49.

[Steuperaert 2019] Steuperaert, Dirk: COBIT 2019: A significant Update. The EDP Audit, Control, and Security Newsletter (EDPACS), Vol. 59 (2019), No. 1, p. 14-18, DOI: 10.1080/07366981.2019.1578474.

[Stögmöller 2019] Stögmöller, Thomas: IT-Security und IT-Compliance im Unternehmen. Juristische Informationen für die Unternehmensleitung. 6. Aufl., Trend Micro Deutschland GmbH, 2019, online verfügbar unter: *https://resources.trendmicro.com/Rechtlicher_Leitfaden_2019_6.Auflage_Herunterladen.html* (letzter Abruf: 08.10.2020).

[Süme/Sens 2019] Süme, Oliver; Sens, Daniel: Blockchain – Rechtsrahmen und Governance. IT-Governance, Jg. 13 (2019), Nr. 30, S. 23-25.

[Terwort/Wilop 2018] Terwort, Andre; Wilop, Karsten: Bankaufsichtliche Anforderungen an die IT (BAIT). IT-Governance, Jg. 12 (2018), Nr. 27, S. 27-29.

[Teubner/Feller 2008] Teubner, Alexander; Feller, Tom: Informationstechnologie, Governance und Compliance. Wirtschaftsinformatik, Jg. 50 (2008), Nr. 5, S. 400-407.

[Thelemann/Bunzel 2011] Thelemann, Karin; Bunzel, Michael: IT-Revision. In: Freidank, Carl-Christian; Peemöller, Volker H. (Hrsg.): Kompendium der Internen Revision – Internal Auditing in Wissenschaft und Praxis. ESV Erich Schmidt Verlag, Berlin, 2011, S. 145-169.

[UP KRITIS 2018] UP KRITIS – BAK Datacenter & Hosting mit CDN (Hrsg.): Branchenspezifischer Sicherheitsstandard zur IT-Sicherheit, Version 1.05, Stand 30.04.2018, online verfügbar unter: *https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/B3S_ITK_V1.05.pdf;jsessionid=D86B1E7B4AED37FE8FAC4ED036F95034.2_cid355?__blob=publicationFile* (letzter Abruf: 08.10.2020).

[Wendt 2016] Wendt, Mathias: Compliance-Kultur – Grundlagen und Evaluierung. In: Hauschka, Christoph E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 3. Aufl., Beck, München, 2016, S. 273-296.

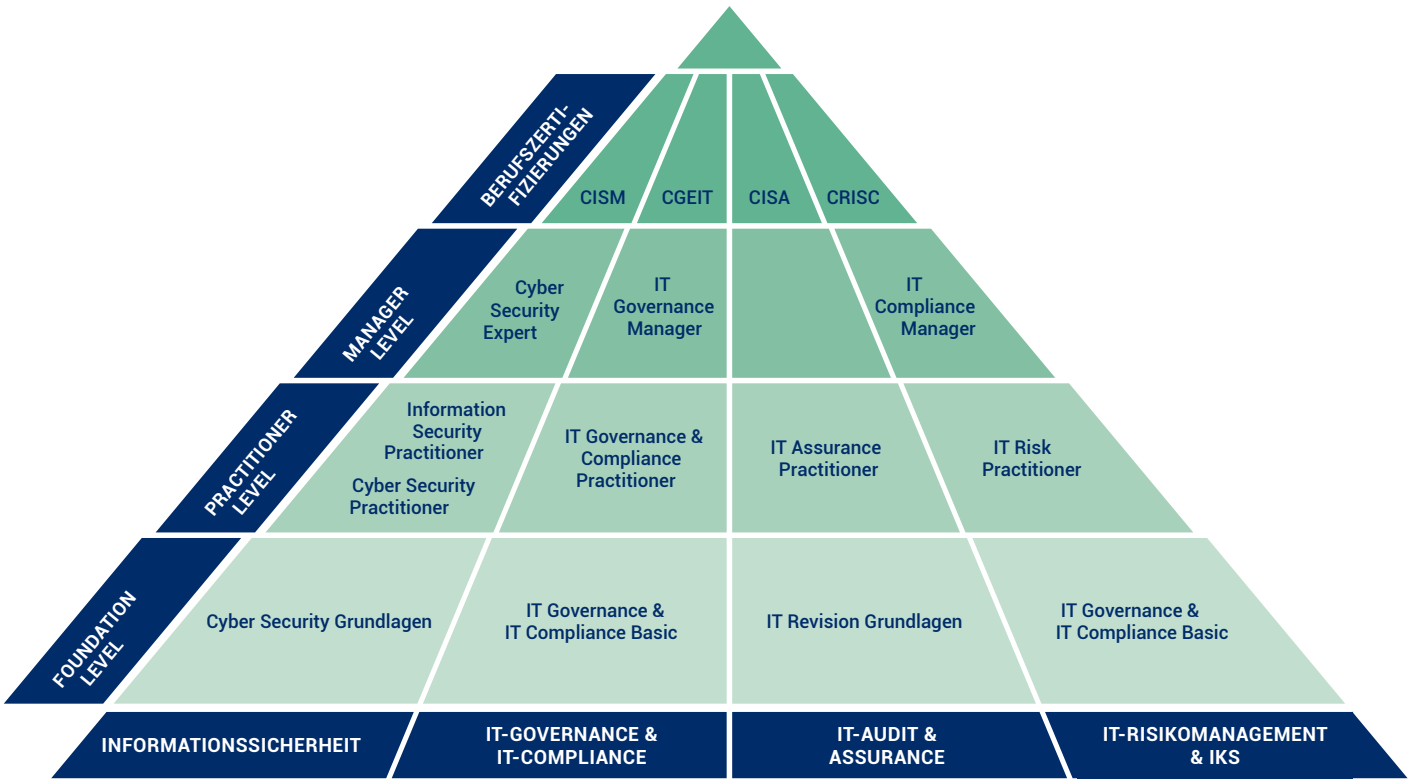
[Withus 2017] Withus, Karl-Heinz: Auswirkungen des ISO-Standards 19600 auf die Prüfung von Compliance-Management-Systemen nach IDW PS 980. In: Schulz, Martin R. (Hrsg.): Compliance-Management im Unternehmen – Strategie und praktische Umsetzung. Deutscher Fachverlag, Frankfurt/M., 2017, S. 157-171.

[Wittek/Strasser 2012] Wittek, Michael; Strasser, Artur: IT-Compliance-Officer – Verantwortung, Aufgaben, Befugnisse und Qualifikationen. Wirtschaftsinformatik & Management, Jg. 4 (2012), Nr. 4, S. 66-71.

ISACA Germany Chapter

Ihr Partner für Weiterbildung:
Der ISACA Germany Chapter e. V.

Der deutsche Berufsverband der IT-Revisoren, IT-Sicherheitsmanager sowie IT-Governance-Experten fördert Ihre berufliche Weiterentwicklung durch Examensvorbereitungskurse auf die internationalen Berufszertifizierungen CISA, CISM und CRISC.

Unterstützend bieten wir Ihnen ein thematisch breit gefächertes Zertifikatsprogramm basierend auf dem Rahmenwerk COBIT 2019.

Unser komplettes Kursangebot können Sie auf unserer Webseite **www.isaca.de/seminare** einsehen. Neben Präsenzseminaren bieten wir alle Kurse auch als **Online-Seminare** an.
Für sämtliche Kurse erhalten Sie einen anerkannten Berufsfortbildungsnachweis (sog. CPE-Stunden).