Klotz, Michael

Working Paper

IT-Compliance: Begrifflichkeit und Grundlagen

SIMAT Arbeitspapiere, No. 06-14-028

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

Suggested Citation: Klotz, Michael (2014) : IT-Compliance: Begrifflichkeit und Grundlagen, SIMAT Arbeitspapiere, No. 06-14-028, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund, https://nbn-resolving.de/urn:nbn:de:0226-simat06140289

This Version is available at:
https://hdl.handle.net/10419/102710

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 06-14-028

IT-Compliance – Begrifflichkeit und Grundlagen

Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

Juli 2014

ISSN 1868-064X

Klotz, Michael: IT-Compliance – Begrifflichkeit und Grundlagen. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2014 (SIMAT AP, 6 (2014), 28), ISSN 1868-064X

Download über URN vom Server der Deutschen Nationalbibliothek:
http://nbn-resolving.de/urn:nbn:de:0226-simat06140289

Impressum

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.fh-stralsund.de
www.simat.fh-stralsund.de

Herausgeber

Prof. Dr. Michael Klotz
Fachbereich Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@fh-stralsund.de

Druck

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

Autor

Prof. Dr. Michael Klotz lehrt und forscht am Fachbereich Wirtschaft der FH Stralsund auf den Gebieten der Unternehmensorganisation und des Informationsmanagements. Er ist u. a. Wissenschaftlicher Leiter des SIMAT, regionaler Ansprechpartner der gfo Gesellschaft für Organisation e.V., Mitglied des wissenschaftlichen Beirats und Academic Advocate der ISACA sowie Mitherausgeber der Zeitschrift „IT-Governance“.

IT-Compliance – Begrifflichkeit und Grundlagen

Prof. Dr. Michael Klotz[1]

Zusammenfassung: IT-Compliance bezeichnet einen Zustand, in dem alle die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden. Damit stellt IT-Compliance einen auf den IT-Einsatz im Unternehmen spezialisierten Teilbereich der Corporate Compliance dar. Wie bei dieser stellen sich Fragen der Bedeutung und des Umfanges sowie der methodischen und organisatorischen Ausgestaltung und Integration in die betrieblichen Verantwortungs- und Entscheidungsstrukturen. Aus akademischer Sicht stehen zuerst einmal die grundlegenden Fragen nach Begriff und Umfang des Handlungsobjekts „IT-Compliance“ im Vordergrund. Hierzu werden in diesem Arbeitspapier die Einbettung des Begriffs der IT-Compliance in die Corporate und IT-Governance einerseits und die Beziehung zwischen Governance und Compliance andererseits diskutiert. Hierbei wird die Verpflichtung zu IT-Compliance ebenso thematisiert wie der Bezug zu den Unternehmenszielen. Anschließend wird der Begriff der IT-Compliance entfaltet. Von zentraler Bedeutung für die Reichweite der IT-Compliance erweist sich der Umfang der für IT-Compliance als relevant erachteten Regelwerke, die vom Unternehmen und seinen Mitgliedern einzuhalten sind. Zur Einteilung dieser Regelwerke wird ein Klassifizierungsmodell („House of IT-Compliance“) vorgestellt, dessen einzelne Kategorien (rechtliche Regelwerke sowie unternehmensinterne und -externe Regelwerke) diskutiert werden.

Gliederung

[1] Prof. Dr. Michael Klotz, FH Stralsund, Fachbereich Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@fh-stralsund.de

Schlüsselwörter: Corporate Compliance – Corporate Governance – IT-Compliance – IT-Governance – IT-Management – IT-Recht – IT-Verträge – Normen – Rechtsprechung – Regelwerke – Standards

JEL-Klassifikation: L15, M10, M21, M42

Vorwort

IT-Compliance war bereits Gegenstand mehrerer Arbeitspapiere. So widmete sich gleich das erste Arbeitspapier dem Datenschutz in kleinen und mittleren Unternehmen sowie den Lehren, die für die IT-Compliance aus einer als ungenügend dargestellten Situation zu ziehen sind (Klotz, AP 1/2009). In Verbindung mit dem IT-Servicemanagement-Standard „IT Infrastructure Library®“ kehrte die Datenschutz-Compliance später wieder zurück (Klotz/Kriegel, AP 19/2012). Die Diskussion um eine Konformität von Projektmanagementsoftware mit den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) war ein weiterer Beitrag zu einer spezialisierten Erörterung der IT-Compliance (Klotz/Sulk/Wieck, AP 17/2012). In einer grundlegenderen Weise näherten sich dagegen die beiden Arbeitspapiere zu den Regelwerken der IT-Compliance der Thematik. Das erste von beiden – mittlerweile in der zweiten Auflage befindlich – richtet sich auf die rechtlichen Regelwerke, d. h. Gesetze und Rechtsverordnungen, Verwaltungsvorschriften, referenzierte Regelwerke und Urteile, aber auch Verträge (Klotz, AP 20/2012). Das nächste Arbeitspapier setzt die Darstellung der Regelwerke fort und befasst sich mit Normen, die sich an das Management der IT richten (Klotz, AP 24/2013). Ergänzt wurde diese Abfolge zuletzt mit der Analyse des Begriffsverständnisses der IT-Compliance nach dem Standard „COBIT®“ (Control Objectives for Information and Related Technology), basierend auf einer Gegenüberstellung von COBIT® 4.0 und COBIT® 5 (Klotz, AP 25/2014).

Bisher beinhaltete lediglich das Arbeitspapier zu den rechtlichen Regelwerken eine kurze Beschreibung der Begrifflichkeit und der grundlegenden Konzepte der IT-Compliance. Diesem Mangel soll mit dem vorliegenden Arbeitspapier zur Begrifflichkeit und den Grundlagen der IT-Compliance abgeholfen werden. Es bildet damit zudem die Einführung zu einer für die nähere Zukunft geplanten Gesamtdarstellung zur IT-Compliance.

Prof. Dr. Michael Klotz

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
AO	Abgabenordnung
AP	Arbeitspapier
APO	Align, Plan and Organise
AS	Australian Standard
AT	Allgemeiner Teil
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAI	Build, Acquire and Implement
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BildscharbV	Bildschirmarbeitsverordnung
BITV 2.0	Barrierefreie Informationstechnik-Verordnung
BMF	Bundesministerium für Finanzen
BSC	Balanced Scorecard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BGH	Bundesgerichtshof
BYOD	Bring Your Own Device
CD-ROM	Compact Disc Read-Only Memory
CEN	Comité Européen de Normalisation
CIO	Chief Information Officer
CISR	Center for Information Systems Research
CMMI	Capability Maturity Model Integration
CMS	Compliance-Managementsystem
COBIT®	Control Objectives for Information and Related Technology
CRM	Customer Relationship Management
DAX	Deutscher Aktienindex
DB	Deutsche Bahn
DCGK	Deutscher Corporate Governance Kodex
DIN	Deutsche Institut für Normung e. V.
DSS	Deliver, Service and Support
EBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
E-Bilanz	Elektronische Bilanz
E-Commerce	Electronic Commerce
ECM	Enterprise Content Management
EDM	Evaluate, Direct and Monitor
EDV	Elektronische Datenverarbeitung

E-Mail	Electronic Mail
EN	Europäische Norm
EStG	Einkommensteuergesetz
eTOM	Enhanced Telecom Operations Map
EU	Europäische Union
e. V.	eingetragener Verein
FAIT	Fachausschuss für die Informationstechnologie
FBI	Federal Bureau of Investigation
FISC	Foreign Intelligence Surveillance Court
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
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
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungs-systeme
GRC	Governance – Risk – Compliance
GuV	Gewinn- und Verlustrechnung
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
IDS	Intrusion Detection System
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
ISACA	Information Systems Audit and Control Association
ISAE	International Standard on Assurance Engagements
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
ISO/IEC JTC1	ISO/IEC Joint Technical Committee 1
IT	Informationstechnik / Informationstechnologie
ITGI	IT Governance Institute
ITIL®	IT Infrastructure Library®
ITSM	IT-Service-Management
KunstUrhG	Kunsturhebergesetz
KWG	Kreditwesengesetz
LG	Landgericht
MaComp	Mindestanforderungen an die Compliance
MaRisk	Mindestanforderungen an das Risikomanagement

MEA	Monitor, Evaluate and Assess
MIT	Massachusetts Institute of Technology
NIA	Normenausschuss Informationstechnik und Anwendungen
OECD	Organisation for Economic Co-operation and Development
OWiG	Gesetz über Ordnungswidrigkeiten
PAngV	Preisangabenverordnung
PCI DSS	Payment Card Industry Data Security Standard
PRINCE 2®	Projects in controlled environments
PS	Prüfungsstandard
QM	Qualitätsmanagement
RACI	R = responsible, A = accountable, C = consulted, I = informed
ROI	Return on Investment
RS	Stellungnahme zur Rechnungslegung
SAM	Software Asset Management
SAS	Statement on Auditing Standards
SEC	Security and Exchange Commission
SC	Subcommittee
SOX	Sarbanes-Oxley Act
SPICE	Software Process Improvement and Capability Determination
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOGAF®	The Open Group Architecture Framework
UrhG	Urheberrechtsgesetz
US	United States
USA	United States of America
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
UStG	Umsatzsteuergesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VOI	Verband Organisations- und Informationssysteme
WpHG	Wertpapierhandelsgesetz
ZPO	Zivilprozessordnung

1 Corporate Governance und IT-Governance

Umfeld der IT-Compliance

IT-Compliance als Teil der Corporate Compliance ist nicht zu trennen von ihrem Umfeld, das durch die IT-Governance gebildet wird. Diese ist wiederum Teil der Corporate Governance. Corporate Governance ist ein mittlerweile breit akzeptierter Ansatz der Unternehmensführung und -überwachung. Kaum ein größeres Unternehmen äußert sich heute nicht auf seiner Website zu seiner Auffassung von Corporate Governance und seiner unternehmensspezifischen Ausgestaltung. Als wesentliche Handlungsfelder der Corporate Governance finden sich Aussagen zu Führung und Kontrolle, zur Zusammenarbeit der Unternehmensorgane, zum Umgang mit Mitarbeitern und Kapitaleignern sowie zu Rechnungslegung und Unternehmenskommunikation. Tabelle 1 enthält einige Beispiele für Website-Aussagen zur Corporate Governance großer deutscher Unternehmen.

1.1 Corporate Governance

Begriff der Corporate Governance

Der Begriff „Corporate Governance“ entstammt der seit Anfang der 1990er Jahre geführten angelsächsischen Diskussion um eine effektive Unternehmensführung und -überwachung. Das Wort „Governance“ geht zurück auf das griechische Wort „kybernétes“ (Steuermann) bzw. das lateinische Verb „gubernare“ (steuern, herrschen). Eine deutsche Übersetzung für „Corporate Governance“ existiert nicht, sodass die Bezeichnung mittlerweile als eigenständiger Begriff Eingang in die hiesige Fachdiskussion und -literatur[2] gefunden hat, wobei sich die wissenschaftliche Betrachtung vor allem auf börsennotierte Publikumsgesellschaften richtet.[3] Mitunter wird der Begriff der Unternehmensverfassung als Übersetzung angeboten; dieser deckt jedoch nur einen Teilbereich der Governance-Bedeutung ab.[4]

Öffentliche Wahrnehmung

In der Öffentlichkeit fand die Governance-Thematik ab Mitte der 1990er Jahre durch spektakuläre Bilanzfälschungen (beispielsweise der Firmen Enron und Worldcom in den USA, Flowtext in Deutschland) bzw. Unternehmenskrisen (beispielsweise von Balsam, Metallgesellschaft, Phillip Holzmann) Beachtung. Missmanagement und Betrugsfälle werfen seitdem Fragen bezüglich der Effektivität von Kontroll- und Risikomanagementsystemen, interner Revision und externer Prüfung auf. Hierbei gerät auch die Rolle der betref-

[2] Siehe z. B. *Hilb 2013*, *Stiglbauer 2010, Welge/Eulerich 2012*.
[3] Nach *Hilb 2013*.
[4] Vgl. *Stiglbauer 2010*, S. 14f.

fenden Verantwortungsträger in den Fokus – häufig in Verbindung mit vermeintlich zu hohen Gehalts-, Prämien- oder Abfindungszahlungen.

Tabelle 1
Beispiele für Website-Aussagen zur Corporate Governance

Unternehmen	Aussagen zur Corporate Governance
Deutsche Bahn AG	„Corporate Governance steht für eine verantwortliche, auf langfristige Wertschöpfung ausgerichtete Unternehmensleitung und -überwachung sowie für die Ausgestaltung der dafür erforderlichen Strukturen und Prozesse. Corporate Governance-Regelungen sollen eine gute, verantwortungsvolle und wertorientierte Unternehmensführung sicherstellen. Wir sind davon überzeugt, dass eine gute Corporate Governance eine wesentliche Grundlage für den Erfolg unseres Unternehmens ist. Es ist unser Ziel, den Unternehmenswert nachhaltig zu steigern und dabei die Interessen von Kunden, Geschäftspartnern, Investoren, Mitarbeitern und der Öffentlichkeit zu fördern sowie das Vertrauen in die DB AG zu wahren und auszubauen.“
Deutsche Bank AG	„Wirkungsvolle Corporate Governance, die hohen internationalen Standards entspricht, ist Teil unseres Selbstverständnisses. Wir stellen dadurch eine verantwortungsbewusste, auf nachhaltige Wertschöpfung ausgerichtete Leitung und Kontrolle der Bank sicher. Vier Elemente sind für unsere Corporate Governance kennzeichnend: Gute Beziehungen zu den Aktionären, eine effektive Zusammenarbeit von Vorstand und Aufsichtsrat, ein erfolgsorientiertes Vergütungssystem für Führungskräfte und Mitarbeiter sowie eine transparente Rechnungslegung und frühzeitige Berichterstattung.“
Lufthansa AG	„Der Begriff Corporate Governance steht nach internationalem Verständnis für die Ausgestaltung der Strukturen und Prozesse zur guten und verantwortungsvollen Führung, Verwaltung und Überwachung von Unternehmen. In den letzten Jahren wurden dafür internationale Standards entwickelt, die insbesondere die Interessen der Aktionäre berücksichtigen. Neben effizienten Strukturen und Prozessen legt der Lufthansa Konzern großen Wert auf Offenheit und Klarheit in der Unternehmenskommunikation. Dies ist eine wichtige Voraussetzung, um bei unseren Kapitalgebern, unseren Mitarbeitern und in der Öffentlichkeit das Vertrauen in die Lufthansa zu bewahren und auszubauen.“
Siemens AG	„Gute Corporate Governance ist die Grundlage unserer Entscheidungs- und Kontrollprozesse. Sie steht für eine verantwortungsbewusste, wertebasierte und auf den langfristigen Erfolg ausgerichtete Führung und Kontrolle des Unternehmens, eine zielgerichtete und effiziente Zusammenarbeit zwischen Vorstand und Aufsichtsrat, die Achtung der Interessen unserer Aktionäre und Mitarbeiter, Transparenz und Verantwortung bei allen unternehmerischen Entscheidungen sowie einen angemessenen Umgang mit Risiken.“
Quellen: *DB AG 2014*, *Deutsche Bank 2014*, *Lufthansa 2014*, *Siemens 2014*	

OECD-Grundsätze

In der internationalen Diskussion um Corporate Governance sind vor allem die Corporate Governance-Grundsätze der Organisation for Economic Co-operation and Development (OECD) von nachhaltiger Wirkung gewesen. Diese von der OECD 1999 aufgestellten und 2004 angesichts der zahlreichen Unternehmensskandale überarbeiten Grundsätze waren in vielen Staaten ein Initiator für Reformen von Governance-Regularien. Nach dem Verständnis der OECD richtet sich Corporate Governance auf das „Geflecht der Beziehungen zwischen dem Management eines Unternehmens, dem Aufsichtsorgan, den Aktionären und anderen Unternehmensbeteiligten (Stakeholder)“ sowie auf „den strukturellen Rahmen für die Festlegung der Unternehmensziele, die Identifizierung der Mittel und Wege zu ihrer Umsetzung und die Modalitäten der Erfolgskontrolle“[5].

Deutscher Corporate Governance Kodex (DCGK)

Die Corporate Governance-Grundsätze der OECD fanden in Deutschland im Rahmen des so genannten „Deutschen Corporate Governance Kodex“ (DCGK) Berücksichtigung. Erstellt wurde der DCGK durch die 2001 einberufene „Regierungskommission Deutscher Corporate Governance Kodex“. Die erste Fassung des Kodex wurde 2003 vorgelegt. Seitdem finden jährliche Überprüfungen und ggf. Anpassungen statt. Ein grundlegendes Verständnis von Corporate Governance und die Zielsetzung des DCGK sind in seiner Präambel enthalten:

> „Der Deutsche Corporate Governance Kodex (der "Kodex") stellt wesentliche gesetzliche Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften (Unternehmensführung) dar und enthält international und national anerkannte Standards guter und verantwortungsvoller Unternehmensführung. Der Kodex hat zum Ziel, das deutsche Corporate Governance System transparent und nachvollziehbar zu machen. Er will das Vertrauen der internationalen und nationalen Anleger, der Kunden, der Mitarbeiter und der Öffentlichkeit in die Leitung und Überwachung deutscher börsennotierter Gesellschaften fördern.“[6]

1.2 IT-Governance

Cadbury-Report

Neben den OECD-Grundsätzen zur Corporate Governance finden zahlreiche nationale Reports in der Literatur Erwähnung. Der wohl am häufigsten zitierte Bericht ist der so genannte „Cadbury Report“. Benannt ist er nach Adrian Cadbury, dem Leiter einer Arbeitsgruppe, die sich mit der Verbesserung der Corporate Governance in der britischen Wirtschaft befasste. Die

[5] *OECD 2004*, S. 11.
[6] *DCGK 2013*.

Ergebnisse der Arbeitsgruppe wurden 1992 als „Report of the Committee on the Financial Aspects of Corporate Governance" vorgelegt. In dem Bericht findet sich die knappe Definition von Corporate Governance, die seitdem häufig zitiert wird und in verschiedene Normen und Standards Eingang gefunden hat:

> „Corporate governance is the system by which companies are directed and controlled."[7]

ISO/IEC 38500

Diese Definition wurde elf Jahre später, im Jahr 2008, von der ISO/IEC-Norm 38500 übernommen, die auf die Governance des Unternehmens-IT abzielt. Die Norm verwendet statt des IT-Governance-Begriffs die Bezeichnung „Corporate Governance of IT" und versteht darunter

> „The system by which the current and future use of IT is directed and controlled."[8]

Definitionen für IT-Governance

Vor der Veröffentlichung der ISO/IEC 38500 gab es bereits zahlreiche Definitionsversuche für den Begriff der IT-Governance, siehe Tabelle 2, die jedoch beträchtlich divergieren.[9] Vor allem an dem von PETER WEILL geleiteten Center for Information Systems Research (CISR) am Massachusetts Institute of Technology (MIT) entstanden einflussreiche Arbeiten zu Konzepten und Modellen der IT-Governance. Die am CISR zugrunde gelegte Definition von IT-Governance stellt die Entscheidungs- und Verantwortungsstruktur in Bezug auf die Nutzung von IT in den Vordergrund. VAN GREMBERGEN stellt ebenfalls auf die Verantwortungsstruktur ab und orientiert sich hierbei eng am Stakeholder-Konzept der Corporate Governance, wenn er auf das organisatorische Zusammenspiel von Aufsichtsgremium, Unternehmensleitung und Leitung der IT-Funktion abstellt.[10] Weiterhin wird hier sowie in der Definition des „IT Governance Institute" (ITGI) die strategische Ausrichtung („Alignment") der IT am Business i. S. der Unternehmensziele und -strategien in den Mittelpunkt gestellt. Die Definition des ITGI ergänzt zudem die aufbauorganisatorischen Strukturen durch eine prozessuale Dimension.

Die beiden Ansätze der ISO/IEC 38500 und des ITGI werden aufgrund ihrer breiten Rezeption im Folgenden näher betrachtet.

---

[7] *The Committee 1992*, Ziffer 2.5.
[8] *ISO/IEC 38500*, S. 3.
[9] Nach *Johannsen/Goeken 2011*, S. 22.
[10] Vgl. *van Grembergen 2002*.

Tabelle 2
Definitionen für IT-Governance

Autor/ Institution	Jahr	Definition
ITGI	2001	„IT-Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives."
Weill/ Woodham	2002	We define IT governance as *specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT*" (Hervorhebung im Original).
van Grembergen	2002	"IT governance is the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT."
ISO/IEC 38500	2008	"The system by which the current and future use of IT is directed and controlled. Corporate Governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization."
Quellen: ITGI 2001, S. 9; Weill/Woodham 2002, S. 1; van Grembergen 2002; ISO/IEC 38500:2008, S. 3		

1.3 IT-Governance nach ISO/IEC 38500

ISO/IEC 38500:2008

Die Norm "ISO/IEC 38500:2008 Corporate governance of information technology" wurde im Juni 2008 publiziert. Sie basiert auf der australischen Norm „AS8015:2005", die im so genannten „fast-track"-Verfahren vom JTC1 übernommen wurde. Derzeit befindet sich die Norm in der Überarbeitung („Review stage"); ein Entwurf liegt seit Beginn 2014 vor.[11]

Zielgruppe

Auch die ISO/IEC 38500 beruft sich auf die Governance-Grundsätze der OECD. [12] Zielgruppe der Norm sind demgemäß in erster Linie die obersten Stakeholder eines Unternehmens. Explizit genannt werden Unternehmensinhaber, Mitglieder der Aufsichtsorgane, der Unternehmensleitung und des oberen Managements sowie alle diejenigen, die diesem Adressatenkreis assistieren bzw. ihm prüfend oder beratend zur Seite stehen. Diese Zielgruppe hat für die Etablierung einer „Corporate governance of IT" zu sorgen, durch

[11] Der Entwurf ISO/IEC DIS 38500 befand sich bis April 2014 in der Abstimmungsphase. Mit einer kurzfristigen Verabschiedung einer neuen Version der Norm ist somit zu rechnen.
[12] Im Folgenden nach *Klotz 2008*.

die 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 systematische Bewertung des IT-Einsatzes sowie die kontinuierliche Überwachung der Planrealisierung spielen hierbei eine zentrale Rolle.[13]

Zielsetzungen

Entsprechend dem geringen Umfang der Norm (15 Seiten) wird lediglich ein grundlegendes Modell der IT-Governance entworfen, das sich auf Zielsetzungen guter IT-Governance im Rahmen von sechs Prinzipien konzentriert, siehe Tabelle 3.

Tabelle 3
Prinzipien der IT-Governance nach der ISO/IEC 38500

Nr.	Prinzip	Ziele
1	Verantwortlichkeit (responsibility)	- Kenntnis und Akzeptanz der Verantwortlichkeiten für IT-Nachfrage und -Angebot
2	Strategie (strategy)	- Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung - Ausrichtung der IT-Strategie an der Unternehmensstrategie
3	Beschaffung (acquisition)	- Bedarfsgerechtigkeit von IT-Investitionen - Transparenz und Fundierung des Entscheidungsprozesses
4	Performanz (performance)	- Verfügbarkeit der IT-Services entsprechend den Leistungs- und Qualitätsanforderungen der Geschäftsbereiche
5	Konformität (conformance)	- Konformität der IT mit rechtlichen Vorgaben, Normen, professionellen Standards etc.
6	Verhalten (human behaviour)	- Beachtung der Bedürfnisse von Personen, die in irgendeiner Weise von der im Unternehmen eingesetzten IT betroffen sind (als Nutzer, IT-Spezialisten, Kunden, Lieferanten etc.)

Quelle: ISO/IEC 38500:20080, S. 6

Führungsfunktionen

Zum Erreichen dieser Zielsetzungen werden verschiedene Maßnahmen in den drei Führungsfunktionen

- Bewertung der IT,
- Leitung der IT und
- Überwachung der IT

[13] Vgl. *ISO/IEC 38500*, S. 3.

empfohlen. In der Kombination von drei Führungsfunktionen und sechs Prinzipien der IT-Governance ergeben sich 18 Handlungsfelder, für die die Norm insgesamt 46 normative Aussagen für eine gute IT-Governance postuliert. Schwerpunkte liegen insbesondere auf den beiden Bereichen „Wertbeitrag der IT“ und „Business/IT-Alignment“, die beide vor allem von den Prinzipien der Beschaffung und Performanz adressiert werden. Ebenfalls systematisch abgebildet werden Forderungen der IT-Compliance, allerdings unter dem Begriff der Conformance. Weniger explizit wird das IT-Risikomanagement adressiert, risikobezogene Aktivitäten tauchen jedoch in verschiedenen Handlungsfeldern auf. In Anwendung des Stakeholder-Ansatzes stellt die Norm das Handeln derjenigen Personen, die von der IT in unterschiedlichen Rollen betroffen sind, im Rahmen des Prinzips „Verhalten“ in den Vordergrund. Hierbei geht es sowohl darum, dass die Bedürfnisse der Nutzer bei der Gestaltung der IT berücksichtigt werden, als auch um die aufgaben- und sachgemäße Nutzung der IT durch die Mitarbeiter.[14]

1.4 IT-Governance nach ITGI

ITGI

Das IT Governance Institute (ITGI) ist eine Tochterorganisation des international agierenden Prüfungsverbandes ISACA (Information Systems Audit and Control Association). Im Rahmen des IT-Governance Frameworks „COBIT“ (Control Objectives for Information and Related Technology) hat das ITGI seine 2003 formulierte Auffassung von IT-Governance überarbeitet und in einem Grundsatzpapier, das sich an die Unternehmensleitung richtet, publiziert. Hiernach werden durch IT-Governance folgende Ziele verfolgt:

- Ausrichtung der IT an den Erfordernissen des Unternehmens;
- Realisierung des versprochenen Nutzens von IT-Investitionen;
- Steigerung des Unternehmenswertes durch Ausschöpfen von Potentialen der IT und Maximierung des Nutzens durch IT;
- verantwortungsvoller Umgang mit IT-Ressourcen;
- angemessenes Management von IT-Risiken.[15]

Stakeholder im Mittelpunkt

Diesen Zielsetzungen entspricht das grundlegende Zyklus-Modell, das die wesentlichen Aufgabenbereiche der IT-Governance beinhaltet, siehe Abbil-

[14] Vgl. *ISO/IEC 38500*, S. 15.
[15] Nach *ITGI 2003*, S.11

dung 1. Die fünf Aufgabenbereiche der IT-Governance werden getrieben durch die Ziele und Nutzenerwartungen der verschiedenen Anspruchs- und Interessengruppen (Stakeholder). IT Value Delivery und Risk Management sind die beiden ergebnisorientierten Aufgabenbereiche: Das wesentliche Resultat ist der Wertbeitrag der IT, der über ein effektives Risikomanagement bei akzeptablen Risiken erreicht werden soll.

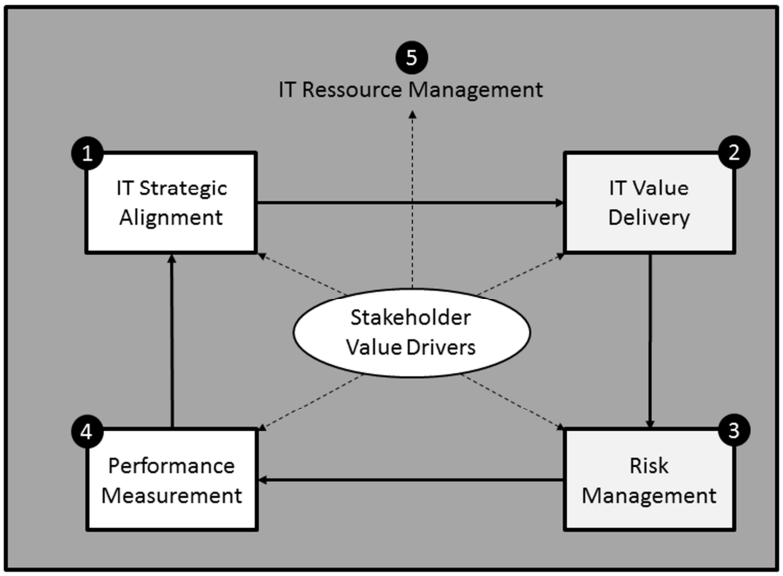

Abbildung 1
Aufgabenbereiche der IT-Governance[16]

Zyklus-Modell der IT-Governance

Der Zyklus startet mit dem IT Strategic Alignment (1), d. h. der Abstimmung zwischen Unternehmens- und IT-Zielen, der Abstimmung zwischen Unternehmens- und IT-Strategie sowie der effektiven und effizienten IT-Unterstützung der Geschäftsprozesse. Auf dieser Basis wird das IT-Projektportfolio beschlossen, IT-Projekte werden durchgeführt und in deren Folge werden IT-Systeme und -Services betrieben. Hieraus resultiert der Wertbeitrag der IT (2), der sich auch darin zeigt, dass die Kosten des IT-Einsatzes minimiert und die aus dem IT-Einsatz resultierenden Risiken durch das Risikomanagement (3) beherrscht werden. Im Rahmen des regelmäßigen bzw. kontinuierlichen Performance Measurement (4) erfolgen die Überwachung der Erreichung der strategischen IT-Ziele, die Fortschrittskontrolle in den IT-Projekten und die Leistungsmessung von IT-Services und IT-Prozessen. Abweichungen des Ist vom Soll werden berichtet. Etwaige Anpassungsmaß-

[16] Eigene Darstellung nach *ITGI 2003*, S. 20.

nahmen führen im nächsten Zyklus zu einem erneuten IT Alignment. Die Durchführung aller Aufgaben des Zyklus beruht auf einem effizienten Einsatz der IT-Ressourcen (Mitarbeiter, IT-Anwendungen, informationstechnische Infrastruktur, Daten). Hierzu ist ein Ressourcenmanagement (5) erforderlich, das im Rahmen des IT-Outsouring auch externe IT-Ressourcen einbezieht.[17]

1.5 Governance und Compliance

Compliance-Verpflichtung des DCGK

Dass Compliance eng mit Governance verbunden ist, zeigt vor allem die Historie der Diskussion um Corporate Governance. Wie geschildert, wurde diese durch Betrugsvergehen und Missmanagement, also durch Fälle von Non-Compliance, getrieben. Dies schlug sich dann auch im Deutschen Corporate Governance Kodex nieder, der dem Vorstand eine explizite Compliance-Verpflichtung zuerkennt. Hiernach hat der Vorstand „für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und ... auf deren Beachtung durch die Konzernunternehmen“[18] hinzuwirken. Ebenso soll sich die Informationspflicht des Vorstands gegenüber dem Aufsichtsrat unter anderem auch auf relevante Fragen der Compliance erstrecken.[19] Allerdings wurden die betreffenden Passagen des DCGK nicht in das Aktiengesetz übernommen. Zusätzlich soll sich nach dem DCGK der vom Aufsichtsrat einzurichtende Prüfungsausschuss (Audit Committee) – falls kein anderer Ausschuss damit betraut ist – mit Compliance befassen.[20] Auch dieser Passus findet sich nicht im Aktiengesetz wieder. Aber immerhin handelt es sich hierbei um eine Empfehlung des DCGK,[21] für die die Aktiengesellschaft nach § 161 AktG zu erklären hat, ob ihr entsprochen wurde bzw. aus welchen Gründen dies nicht der Fall ist.

Trotz der mangelnden Verbindlichkeit schafft der DCGK einen deutlichen Zusammenhang zwischen Corporate Governance und Compliance. Hieraus resultiert ein struktureller Rahmen für die Unternehmensüberwachung, der auch die Compliance des Unternehmens insgesamt und seiner einzelnen Mitglieder adressiert.

---

[17] Vgl. *Meyer/Zarnekow/Kolbe 2003*; *ITGI 2003*, S. 19ff.
[18] *DCGK 2013*, Ziffer 4.1.3.
[19] Nach *DCGK 2013*, Ziffer 3.4.
[20] Nach *DCGK 2013*, Ziffer 5.3.2
[21] Vgl. *Benzler/Weber-Rey 2013*, S.702.

1.6 Compliance

Compliance-Begriff

Der Deutsche Corporate Governance Kodex versteht unter Compliance die Einhaltung von Gesetzen und unternehmensinternen Richtlinien. Allgemeiner formuliert handelt ein Unternehmen „compliant“, wenn es in seiner Geschäftstätigkeit bestimmte Vorgaben befolgt. Alternativ zu „Befolgung“ finden auch Begriffe wie „Konformität“, „Einhaltung“, „Übereinstimmung“, „Entsprechung“ oder „Erfüllung“ Verwendung. Welche Vorgaben in einer konkreten Situation relevant sind, ist zum einen unternehmensextern vorgegeben, wie beispielsweise bei Gesetzen, zum anderen selbst gewählt, wie beispielsweise bei unternehmensinternen Richtlinien.[22] In Bezug auf das Einhalten von Vorgaben bzw. den Verstoß gegen selbige gelten folgende Grundsätze:

- Non-Compliance stellt sich als wirtschaftliches Risiko für das Unternehmen und die Mitglieder der Unternehmensleitung dar. Gerade diese persönliche Betroffenheit bildet den wesentlichen Treiber von Compliance-Maßnahmen.
- Die Risikosichtweise erfordert eine bewusste Entscheidung darüber, welche Compliance-Risiken akzeptiert werden und auf welche Compliance-Risiken sich das Risikomanagement fokussieren muss.
- Zur Verhinderung von Compliance-Risiken ist ein Compliance-Managementsystem erforderlich, das Non-Compliance und dem damit verbundenen Schaden entgegenwirken soll.[23]

So, wie es hinsichtlich der Corporate Governance eine Spezialisierung für die Unternehmens-IT – die IT-Governance – gibt, lässt sich auch eine Spezialisierung der allgemeinen Compliance des Unternehmens für die IT – die IT-Compliance – ausmachen.

[22] Nach *Klotz 2009*, S. 3.
[23] Vgl. *Hauschka 2010*, S. 3f.

2 Der Begriff der IT-Compliance

Äußerlichkeiten von IT-Compliance

IT-Compliance zeigt sich physisch u. a. im Vorhandensein und Funktionieren informations- und kommunikationstechnischer Einrichtungen, im Vorliegen von Programmdokumentationen und Notfallplänen, in Richtlinien für IT-Sicherheit und andere Belange der IT, in der Dokumentation von IT-Kontrollen und Kontrollergebnissen, dem konkreten Umgang mit Daten sowie mit der Nutzung stationärer und mobiler IT-Gerätschaften. Dennoch stehen diese materiellen Objekte nicht für die Bedeutung des Begriffs „IT-Compliance“; dieser bezeichnet vielmehr einen immateriellen Zustand. Ob dieser Zustand zu einem bestimmten Zeitpunkt vorliegt, ist eine Frage, die sich nicht hinweisend durch Bezugnahme auf die genannten einzelnen Objekte beantworten lässt. Hierzu ist vielmehr eine Bewertung in Folge einer Prüfung erforderlich, ob die IT des Unternehmens bestimmten, relevanten Vorgaben entspricht.[24] Demgemäß lässt sich folgende Definition für IT-Compliance treffen:

Definition: IT-Compliance

> „IT-Compliance bezeichnet einen Zustand, in dem alle die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.“[25]

Einige Elemente der Definition bedürfen der Erläuterung.[26]

- IT-Compliance als Zustand stellt sich nicht von selbst ein, sondern wird durch geeignete Maßnahmen angestrebt. Weil Rechtsnormen und sonstige Regelungen einer kontinuierlichen Veränderung unterliegen und sich in Zahl und Umfang tendenziell vermehren, sind Unternehmen dem Zielzustand „IT-Compliance“ mal mehr, mal weniger nah. IT-Compliance ist somit ein „moving target“ in dem Sinne, dass IT-Compliance als Zustand immer „noch nicht ist“, aber auch nie komplett eintreten wird (was auch unwirtschaftlich sein dürfte). Jeder Zustand von Compliance ist somit notwendig mit einem gewissen Ausmaß an Non-Compliance verbunden. Hieraus folgt, dass ein entsprechendes Risiko implizit oder explizit akzeptiert werden muss.
- Die Forderung nach Nachweisbarkeit verweist darauf, dass Compliance nicht nur gelebt, sondern in seiner Wirksamkeit auch dokumentiert werden muss. Die faktische Nachweisbarkeit (z. B. mittels Verfahrensan-

[24] Nach *Klotz/Dorn 2008*, S. 5f.
[25] *Klotz 2013b*, S. 715.
[26] Im Folgenden nach *Klotz 2013b*, S. 709ff.

weisungen, Prozessbeschreibungen, archivierter Daten und Dokumente oder Prüfprotokollen) ist unternehmensintern gegenüber Aufsichtsorganen und Prüfungsinstitutionen (z. B. interne Revision, Wirtschaftsprüfer, externe Auditoren) notwendig, aber auch, um sich ggf. gegenüber externen Dritten im Verdachts- oder Streitfall exkulpieren zu können.

- Die Adressierung der Unternehmens-IT richtet sich an den betreffenden Verantwortungsträger, also die IT-Leitung. IT-Compliance ist Teil der Funktionsverantwortung der die IT leitenden Führungsposition. Dies gilt umso mehr, wenn die IT-Leitung als Chief Information Officer (CIO) Mitglied der Unternehmensleitung ist. Die IT-Leitung darf IT-Compliance nicht nur als Pflichtübung begreifen, sondern muss sich sichtbar dazu bekennen und als treibende Kraft agieren. Dies zeigt sich beispielsweise in einem deutlichen Bekenntnis zu IT-Compliance, verbunden mit einer konsequenten Sanktionierung von Compliance-Verstößen.

Klassifikation der Regelwerke

Der Umfang von IT-Compliance richtet sich wesentlich danach, welche Vorgaben bzw. Quellen von Vorgaben in Bezug auf die Compliance der IT berücksichtigt werden. Hier sind es nun drei Gruppen von Regelwerken, die als Quelle von an die IT gerichteten Vorgaben in Frage kommen, siehe Abbildung 2.

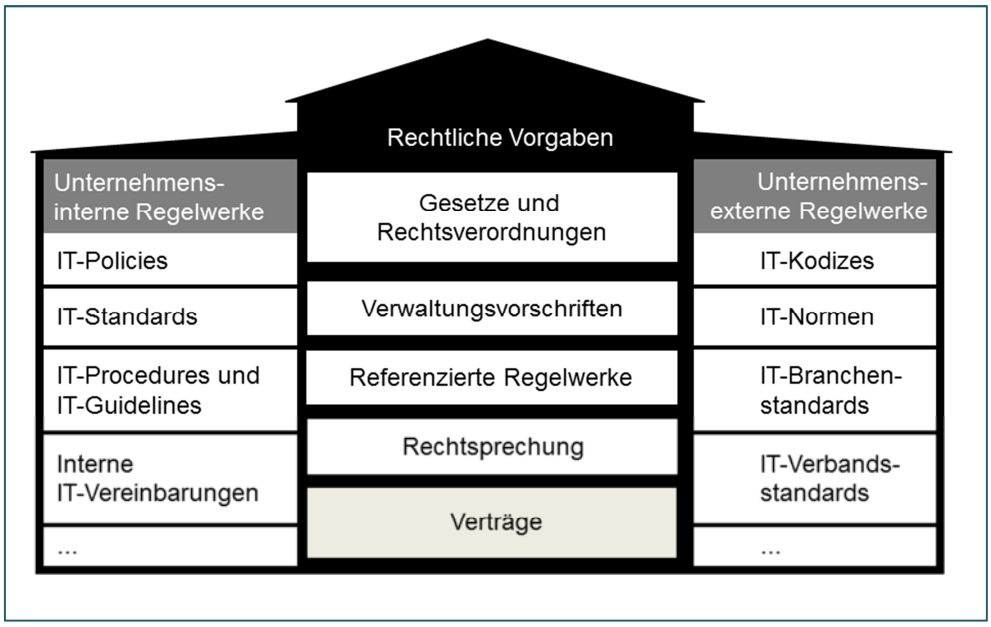

Abbildung 2
Das „House of IT-Compliance"[27]

[27] Nach *Klotz 2013b*, S. 733.

- Rechtliche Vorgaben an die IT, d. h. Rechtsnormen (Gesetze und Rechtsverordnungen), Rechtsprechung, Verwaltungsvorschriften und weitere referenzierte Regelwerke, auf die in Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften verwiesen wird oder die von der Rechtsprechung zur Auslegung herangezogen werden; weiterhin Verträge, mit Kunden, Lieferanten und sonstigen Vertragspartnern, soweit IT-relevante Vereinbarungen enthalten sind;
- unternehmensexterne, auf IT bezogene Regelwerke, wie Normen, Branchen- oder Verbandsstandards o. Ä.;
- unternehmensinterne Regelwerke in Bezug auf die Unternehmens-IT, d. h. IT-Policies und -Procedures, interne Vereinbarungen oder IT-Standards, soweit sie IT-relevante Vorgaben beinhalten.[28]

Unterschiedliche Risiken

Im Hinblick auf ein Management von IT-Compliancerisiken ist es wichtig zu beachten, dass sich die Regelwerke hinsichtlich ihrer Risiken unterscheiden. Bei Rechtsnormen und Verträgen sind die IT-Compliancerisiken deswegen tendenziell höher, weil hier oft ein monetäres Strafmaß entweder gesetzlich oder vertraglich geregelt ist bzw. aus Vertragsverletzungen hohe oder sogar bestandsgefährdende Schadensersatzpflichten resultieren können, vgl. Abbildung 3.

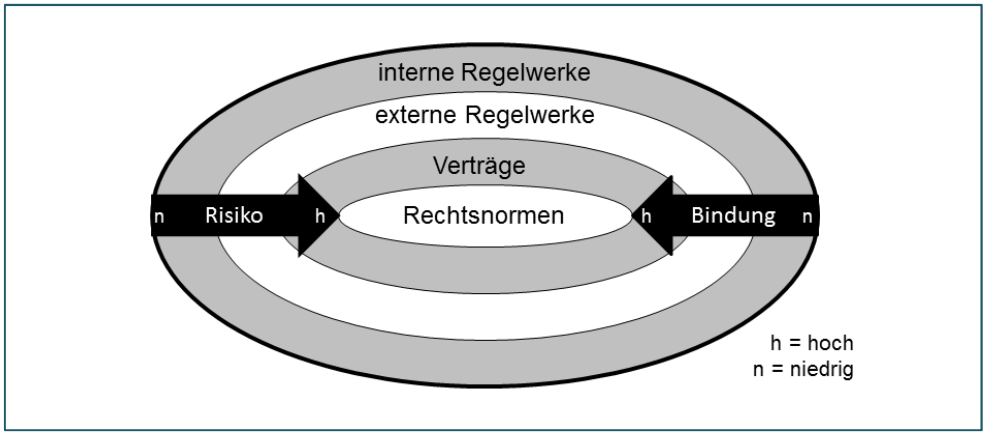

Abbildung 3
Bindung und Risiko der Regelwerke

Zudem kommen in diesen Fällen häufig ein Vertrauensverlust sowie Reputationsschäden hinzu. Durch strafverfolgende Institutionen bzw. Vertragspartner, die ihre Interessen aktiv verfolgen, ergibt sich auch eher die Wahrscheinlichkeit, dass bei Rechtsnormen und Verträgen ein Verstoß entdeckt

[28] Nach Nach *Klotz/Dorn 2008*, S. 11; *Klotz 2013b*, S. 733.

und ein Anspruch erhoben wird. Bei den externen Regelwerken ist zu beachten, dass diese ggf. aufgrund Verweis oder Heranziehung zur Auslegung der Rechtsnormen letztlich deren Bindungswirkung und das daraus resultierende Risiko teilen können.[29]

Unternehmensinterne Regelwerke

Bei unternehmensinternen Regelwerken „ist die Bindungswirkung auf dasjenige Unternehmen beschränkt, welches die jeweilige Regelung in Kraft setzt. Beispiele für unternehmensinterne Regelungen aus dem IT-Bereich sind interne IT-Richtlinien oder -Verfahrensvorgaben zur IT-Sicherheit (IT-Sicherheitsvorschriften, E-Mail-Richtlinie, Regelung zum Umgang mit Passwörtern etc.)“.[30] Durch die unternehmensinternen Regelwerke werden somit in erster Linie die Unternehmensmitglieder gebunden. Ein Verstoß gegen diese Regelwerke wird interne Sanktionsmaßnahmen nach sich ziehen, die sich negativ auf individuelle Karrieren auswirken können. Dem Unternehmen wird hier erst dann ein relevanter Schaden entstehen, wenn die betroffenen internen Regelwerke die Compliance mit externen Vorgaben sicherstellen sollten. Insofern sind interne Regelwerke in zweierlei Hinsicht relevant für IT-Compliance.

- Zum einen dienen sie dazu, die Beachtung der Anforderungen der rechtlichen Vorgaben und der externen Regelwerke sicherzustellen, indem sie den einzelnen Unternehmensmitgliedern konkrete Handlungsanweisungen vorschreiben.
- Hierdurch dokumentieren die unternehmensinternen Regelwerke zum anderen nach außen, dass den externen, insbesondere den rechtlichen Vorgaben nachgekommen wird und diesbezüglich obliegende Sorgfaltspflichten erfüllt werden.[31]

Interesse der IT-Praxis

Für die Praxis sind die rechtlichen Vorgaben sowie die für das IT-Management relevanten Normen und Standards von besonderem Interesse. Hinsichtlich der rechtlichen Vorgaben ergibt sich dieses aus dem Bestreben, Nachteile aus Strafzahlungen und -gebühren, Buß- und Zwangsgeldern, Vertragsstrafen oder Schadensersatzpflichten zu minimieren. Die Orientierung an Normen und Standards unterstützt dagegen ein effektives und effizientes IT-Management, indem IT-Kosten gesenkt, die Qualität und die Sicherheit von IT- und Geschäftsprozessen erhöht und damit auch IT-Risiken reduziert

[29] Nach *Klotz/Dorn 2008*, S. 11f.
[30] *Ebd.*, S. 13.
[31] *Ebd.*, S. 13f.

werden können. Trotzdem liegt der praktische Schwerpunkt von IT-Compliance oftmals auf den rechtlichen, speziell den gesetzlichen Vorgaben. Mit dieser Fokussierung lässt sich dann von einer „Legal IT Compliance“ sprechen. Eine derart ausgerichtete IT-Compliance hätte folgende Aufgabenfelder wahrzunehmen:

Legal IT Compliance

- Identifizierung von complinace-relevanten Normen und die Ableitung der vom Unternehmen einzuhaltenden Compliance-Anforderungen;
- „Schaffung einer betrieblichen Organisation von Prozessen, Verfahrensregelungen, Delegationen und (möglichst weitgehend automatisierten) Kontrollen zur Überwachung der Einhaltung aller Anforderungen der IT-Compliance;
- die Information aller in irgend einer Form im Hinblick auf die bestehenden Verpflichtungen handelnden Betriebsangehörigen und ggf. entsprechend eingesetzter Dritter über die einzuhaltenden Regelungen;
- die Dokumentation sowohl der Information als auch der Organisation und insbesondere deren Überwachung;
- Reaktion auf neue Entwicklungen der Anforderungen, z. B. innerhalb der aktuellen Rechtsprechung, oder erkannte Compliance-Schwachstellen“.[32]

[32] *Klotz 2007a*, S. 17.

3 Rechtsverpflichtung zu IT-Compliance

Vorgaben zur IT-Compliance

Dass sich Unternehmen an geltendes Recht zu halten haben, ist eine Selbstverständlichkeit – oder sollte es sein. Insofern enthält jedwede Rechtsnorm Vorgaben, denen Folge zu leisten ist. Dies gilt somit auch für IT-bezogene Vorgaben, die in verschiedenen Gesetzen und Verordnungen enthalten sind. Diese Vorgaben bilden die Rechtsgrundlagen der operativen IT-Compliance. Es stellt sich jedoch die Frage, ob Compliance selbst von Rechtsnormen gefordert wird, insbesondere hinsichtlich des Aufbaus einer Compliance-Organisation oder der Einrichtung eines Compliance-Managementsystems, wobei die IT-spezifische Ausprägung jeweils Bestandteil einer übergeordneten Corporate Compliance wäre.

DCGK, WpHG und MaComp

Wie beschrieben enthält der Deutsche Corporate Governance Kodex eine explizite Compliance-Verpflichtung des Vorstands. Allerdings stellt diese mangels Übernahme dieses Passus in das Aktiengesetz (AktG) lediglich eine Empfehlung des DCGK dar, aus der „eine Verpflichtung des Vorstands einer börsennotierten Aktiengesellschaft zur Einführung eines Compliance-Systems nicht abgeleitet werden“[33] kann. Somit stellt das Wertpapierhandelsgesetz (WpHG) derzeit das einzige Gesetz dar, das den Compliance-Begriff explizit verwendet. Hinsichtlich der Organisationspflichten regelt § 33 WpHG, dass „eine dauerhafte und wirksame Compliance-Funktion einzurichten ist, die ihre Aufgaben unabhängig wahrnehmen kann“. Für Kreditinstitute ergeben sich hieraus verbindliche Anforderungen an eine Compliance-Organisation, da die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die aus dem WpHG resultierenden Compliance-Pflichten mit den „Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen (MaComp)“ umfangreich konkretisiert hat. Hieraus kann aber keineswegs eine entsprechende Compliance-Verpflichtung für Unternehmen aller Branchen abgeleitet werden.

OWiG, GmbHG, AktG

Hinsichtlich einer für alle Unternehmen geltenden Pflicht zur Vermeidung von Rechtsverstößen kann das Gesetz über Ordnungswidrigkeiten (OWiG) herangezogen werden. Nach § 130 OWiG sind organisatorische Maßnahmen zu treffen, die Rechtsverstöße aus dem Unternehmen heraus verhindern sollen. Allerdings kann auch hieraus keine konkrete Verpflichtung zur organisatorischen, technischen oder personellen Ausgestaltung der Compliance-

[33] *Hauschka 2010*, S. 11.

Verantwortung im Unternehmen abgeleitet werden.[34] Ebenso vage bleibt die Verankerung von Compliance-Verpflichtungen in den im AktG und dem Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) festgeschriebenen Sorgfaltspflichten der Unternehmensleitung. So ist beispielsweise in § 93 Abs. 1 AktG geregelt, dass Vorstandsmitglieder „bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden“ haben. Ganz ähnlich stellt § 43 Abs. 1 GmbHG auf die „Sorgfalt eines ordentlichen Geschäftsmannes“ ab. Zu dieser Sorgfalt können auch Maßnahmen insbesondere zu Überwachung der Rechtskonformität gezählt werden. Gleichwohl lassen sich hieraus keine konkreten Vorgaben für Compliance-Organisation und -Management ableiten, schon gar nicht hinsichtlich der „Anwendung bestimmter IT-Normen oder IT-Standards“[35].

AktG, HGB

Weiterhin wird auch versucht, eine besondere Compliance-Verpflichtung aus der Bedeutung der IT für das Funktionieren des Tagesgeschäfts abzuleiten. IT stellt nach dieser Sichtweise für ein Unternehmen eine kritische Infrastruktur dar, deren Beeinträchtigung oder gar Ausfall hohe Schäden für das Unternehmen verursachen kann. Mithin stellt IT einen Risikobereich dar, der vom Risikomanagement des Unternehmens zu adressieren ist. Eine gesetzliche Verankerung wäre in dieser Sichtweise in § 91 Abs. 2 AktG zu finden, nach dem der Vorstand ein Überwachungssystem einzurichten hat, „damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“. In der Gesetzesbegründung wird die Verpflichtung des Vorstands hervorgehoben, für ein angemessenes Risikomanagement und eine angemessene interne Revision zu sorgen.[36] Im Handelsgesetzbuch (HGB) ist in § 317 Abs. 4 HGB festgeschrieben, dass bei der Jahresabschlussprüfung zu beurteilen ist, ob der Vorstand dieser Pflicht durch Maßnahmen in einer geeigneten Form nachgekommen ist „und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann“. Die Pflicht zur Einrichtung und Dokumentation eines Risikomanagementsystems besteht somit zweifellos. Die konkrete Ausformung – so wird in der Gesetzesbegründung festgestellt – hängt jedoch von situativen Faktoren, wie der Unternehmensgröße und -struktur, der Branche oder dem Kapitalmarktzugang ab. Bei den Entwicklungen, die den Fortbestand der Gesellschaft gefährden, werden in

[34] Nach *ebd.*
[35] *Rath/Sponholz 2009*, S. 69.
[36] Vgl. *Deutscher Bundestag 1998*, S. 15.

der Gesetzesbegründung zum Aktiengesetz explizit auch Verstöße gegen gesetzliche Vorschriften angeführt.[37] Trotzdem können all diesen Aussagen keine konkreten Vorgaben für die Ausgestaltung einer Compliance-Organisation oder eines Compliance-Managementsystems entnommen werden. Außerdem ist zu berücksichtigen, dass nicht jeder Fall von Non-Compliance eine Existenzbedrohung für das Unternehmen darstellt. Dies gilt insbesondere auch für die IT-Compliance, wo sowohl Auswirkungen als auch Bußgelder in den meisten Fällen als durchaus begrenzt bezeichnet werden dürfen.

Motivation des Top-Managements

Ob und in welchem Umfang eine Compliance-Organisation und ein Compliance-Managementsystem eingerichtet werden, bleibt der Entscheidung der Unternehmensleitung überlassen. Allerdings besteht vor dem Hintergrund der haftungsrechtlichen Konsequenzen für die Mitglieder der Unternehmensorgane eine starke persönliche Motivation der handelnden Personen, Compliance und IT-Compliance systematisch in organisatorischer, technischer und personeller Hinsicht im Unternehmen zu verankern.

[37] Nach *Deutscher Bundestag 1998*, S. 15.

4 Rechtliche Vorgaben

4.1 Gesetze und Rechtsverordnungen

Rechtsnormen

Im Zentrum der rechtlichen Vorgaben stehen Rechtsnormen, also vom Gesetzgeber erlassene Gesetze und Rechtsverordnungen. Hierzu zählen auch Verordnungen der Europäischen Union (EU) und ggf. auch von anderen Staaten erlassene Gesetze.[38] EU-Verordnungen bedürfen – anders als die Richtlinien der EU – keiner Umsetzung in nationales Recht und entfalten damit eine unmittelbare Durchgriffswirkung. So würde beispielsweise die derzeit als Entwurf diskutierte Datenschutz-Grundverordnung der EU nach ihrer Verabschiedung in den Mitgliedsstaaten unmittelbar geltendes Recht darstellen.

4.1.1 Ausländische Gesetze

SOX

In Literatur und Fachdiskussion zu IT-Compliance wird häufig auf den Sarbanes-Oxley Act (SOX) verwiesen. SOX ist ein im Jahr 2002 erlassenes US-Bundesgesetz, das in Folge der erwähnten Unternehmensskandale um Manipulationen und Bilanzfälschungen Regelungen für die Corporate Governance von Unternehmen traf. Dieses US-Gesetz ist für Unternehmen – inklusive deren Tochtergesellschaften und Wirtschaftsprüfer – relevant, die bei der US-Börsenaufsicht SEC (Security and Exchange Commission) registriert sind. Damit sind auch deutsche Unternehmen, die an der SEC gelistet sind[39], sowie deutsche Tochtergesellschaften von bei der SEC registrierten Unternehmen betroffen. Trotz der umfangreichen Beachtung, die der Sarbanes-Oxley Act auch in der Diskussion um IT-Compliance findet, richtet er sich nicht in erster Linie an die Unternehmens-IT. „Section 404 des SOX schreibt die Implementierung und Bewertung eines internen Kontrollsystems (IKS) 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.“[40]

USA PATRIOT Act

Weitere Anforderungen an die IT ergeben sich vor allem aus Gesetzen zur Bekämpfung des Terrorismus. So hat der USA PATRIOT Act (wobei das

[38] Im Folgenden nach *Klotz 2012*, S. 16ff.
[39] Mit dem Delisting der Siemens AG Anfang 2014 sind dies mittlerweile nur noch drei deutsche DAX-Unternehmen: SAP, Fresenius Medical Care und die Deutsche Bank.
[40] *Klotz 2012*, S. 24f.

Akronym für „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism“ steht) durch die zunehmende Verbreitung des Cloud-Computing an Aktualität gewonnen. Der USA PATRIOT Act ist ebenfalls ein US-amerikanisches Bundesgesetz, das am 25.10.2001 im Zuge der Terrorismusbekämpfung erlassen wurde. Nach Section 215 kann der Foreign Intelligence Surveillance Court (FISC) als das Gericht, das die Überwachungsaktivitäten der US-amerikanischen Auslandsgeheimdienste regelt, dem FBI (Federal Bureau of Investigation) Datenzugang bei einem Internet-Provider oder einen Cloud-Anbieter in den USA gewähren. Diese Verpflichtung kann sich aber auch an entsprechende Unternehmen in Europa richten, die sog. „minimum contacts“, mit den USA pflegen (z. B. dort eine Betriebsstätte unterhalten) und die Kontrolle über die von den US-amerikanischen Behörden angeforderten Zieldaten ausüben. Dabei dürften sich in der Regel der USA PATRIOT Act und das deutsche Bundesdatenschutzgesetz als inkompatibel erweisen.[41]

4.1.2 Verordnungen der EU

EU-Verordnungen zur Terrorismusbekämpfung

Ähnlich richten sich in der EU die Verordnungen Nr. 2580/2001 und Nr. 881/2002 auf die Terrorismusbekämpfung. „Beide Verordnungen sehen vor, dass Gelder, andere finanzielle Vermögenswerte und wirtschaftliche Ressourcen der gelisteten Personen, Organisationen, Vereinigungen und Unternehmen eingefroren werden. Ihnen dürfen zudem keine Gelder, sonstigen finanziellen Vermögenswerte, wirtschaftliche Ressourcen oder Finanzdienstleistungen zur Verfügung gestellt werden. Um diesen Verpflichtungen zu genügen, müssen Organisations- und Personenstammdaten mit den entsprechenden Sanktionslisten abgeglichen werden. Dies betrifft nicht nur die selbst erfassten und gepflegten Daten, sondern auch z. B. im Rahmen von Marketingaktionen zugekaufte Daten.“[42]

4.1.3 Deutsche Gesetze

„IT-Gesetze“

In Bezug auf die deutsche Gesetzgebung sind für IT-Compliance offensichtlich diejenigen Gesetze relevant, die sich schon vom Namen her auf die IT richten. Dies sind insbesondere das Bundesdatenschutzgesetz, das Telekommunikationsgesetz und das Telemediengesetz.

---

[41] Vgl. *Noerr/Denton 2011*.
[42] *Klotz 2012*, S. 27.

- Das Bundesdatenschutzgesetz (BDSG) regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen (Unternehmen). Für personenbezogene Daten ist jeweils für jede Nutzung (z. B. für Kundendaten in Data-Warehouse- bzw. CRM-Lösungen) zu prüfen, ob die Nutzung von den konkreten Vertragszwecken und damit von den Ermächtigungsvorschriften der §§ 27 ff. BDSG gedeckt ist. Weitere Regelungen des BDSG betreffen die Bestellung eines Datenschutzbeauftragten, den Umfang der Betroffenenrechte, die Transparenz und Dokumentation sowie die Nachvollziehbarkeit von Zugriffen, Änderungen und Weitergaben personenbezogener Daten an Dritte. Von besonderer Bedeutung für Unternehmen sind die Regelungen des § 11 BDSG zur Auftragsdatenverarbeitung. Kommen einem Unternehmen Daten abhanden oder werden diese unrechtmäßig weitergeleitet, regelt § 42a BDSG die Pflicht zur Mitteilung des Vorfalls an die Aufsichtsbehörde. Vor allem die Anlage zu § 9 BDSG enthält verschiedene technische und organisatorische Kontrollmaßnahmen, durch die ein Missbrauch personenbezogener Daten verhindert werden soll. BDSG

- Das Telekommunikationsgesetz (TKG) dient der Regulierung des Wettbewerbs im Bereich der Telekommunikation. Für Unternehmen erweist sich das TKG dann als relevant, wenn die private Nutzung von Internet und E-Mail durch die Belegschaft des Unternehmens als Anbieten von Übertragungswegen an Dritte i. S. d. TKG angesehen wird und ein Unternehmen dadurch Telekommunikationsdienste gemäß dem TKG erbringt.[43] Nach § 109 TKG wären dann angemessene technische Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme zu ergreifen. § 109 Abs. 4 TKG schreibt explizit die Erstellung eines IT-Sicherheitskonzepts und die Ernennung eines IT-Sicherheitsbeauftragten vor. TKG

- Das Telemediengesetz (TMG) bildet eine wichtige Grundlage für Internet-Dienste, indem es den Betrieb elektronischer Informations- und Kommunikationsdienste regelt. „Den Anbieter entsprechender Dienste treffen nach den §§ 5, 6 TMG umfangreiche Informationspflichten (z. B. Angaben zum Unternehmen, Erreichbarkeit, zu eventuellen Aufsichtsbehörden sowie zur Erkennbarkeit einer kommerziellen Kommunika- TMG

[43] Für eine ausführliche Diskussion dieser Problematik s. *BITKOM 2008*.

tion). Wichtig für die Frage der Haftung des Diensteanbieters für fremde Inhalte sind die §§ 7 ff. TMG. Hierin ist ein Haftungsausschluss geregelt, der jedoch nach § 10 TMG nur dann gilt, wenn die fremden Inhalte dem Unternehmen nicht bekannt gewesen oder die beanstandeten Daten unverzüglich nach Kenntnis entfernt oder gesperrt worden sind. Auch datenschutzrechtliche Anforderungen finden sich im TMG. So richtet sich die Bearbeitung personenbezogener Daten nach den §§ 14, 15 TMG."[44]

IT-Recht

Neben diesen IT-nahen Gesetzen beziehen sich zahlreiche weitere Gesetze auf die Unternehmens-IT. Sie adressieren den IT-Einsatz im Unternehmen in eher geringem Umfang. Zumeist stellt die IT ein Mittel dar, um Vorgaben vor allem in Bezug auf die Dokumentation und Archivierung von Daten und Dokumenten sowie hinsichtlich der Datenerfassung, -speicherung und -übermittlung sowie des Datenzugriffs im Rahmen des elektronischen Geschäftsverkehrs zu erfüllen. Diese IT-bezogenen Teilbereiche werden mit den oben genannten IT-spezifischen Gesetzen mitunter unter dem Oberbegriff „IT-Recht" zusammengefasst.[45] Im Kern sind folgende Gesetze für IT-Compliance relevant:

Abgabenordnung

- Die Abgabenordnung (AO) ist für das deutsche Steuerrecht von zentraler Bedeutung. Compliance-Vorgaben für die IT resultieren insbesondere aus den §§ 145 ff. AO, in denen die Aufzeichnungs- und Aufbewahrungspflichten sowie der Datenzugriff durch die Finanzbehörden geregelt wird. Ausgangspunkt bildet der § 147 Abs. 2 AO, nach dem die Aufbewahrung von Unterlagen auf Bildträgern oder anderen Datenträgern erlaubt ist, wenn die Daten „während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können". Um die Prüfung elektronisch gespeicherter Unterlagen und Daten zu ermöglichen, sind vom Unternehmen nach § 147 Abs. 5 AO Hilfsmittel zur Verfügung zu stellen. Noch weitergehend hat ein Unternehmen nach § 147 Abs. 6 AO bei einer Erstellung der Aufzeichnungen mit Hilfe eines IT-Systems nicht nur die „Einsicht" in diese Daten ermöglichen, sondern muss nach Vorgabe der Betriebsprüfung die Daten selbst auswerten oder den Finanzbehörden auf einem verwertbaren lesbaren Datenträger zur Verfügung stellen.

[44] *Klotz 2012*, S. 32.
[45] Siehe z. B. die Darstellungen von *Redeker 2012*, *Steckler 2007*.

Betriebsverfassungsgesetz

- Das Betriebsverfassungsgesetz (BetrVG) regelt die Beteiligung des Betriebsrates, z. B. durch Mitwirkungsrechte in der Planungsphase oder ggf. Mitbestimmungsrechte in der Einführungsphase von IT-Systemen. Nach § 80 Abs. 2 und § 90 BetrVG ist der Betriebsrat über die geplante Einführung von IT-Systemen, die Erweiterung ihres Einsatzes und die Einführung neuer Programme unverzüglich zu unterrichten. Darüber hinaus steht dem Betriebsrat ein Mitbestimmungsrecht zu, 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 (was bei den meisten IT-Systemen mit Protokollierungsfunktionalität der Fall sein dürfte).

Bürgerliches Gesetzbuch

- Die Bezüge des Bürgerlichen Gesetzbuchs (BGB) zur IT sind mittlerweile zahlreich. So regelt das BGB für Fernabsatzverträge in den §§ 312b bis f BGB die Nutzung von E-Mails, Tele- und Mediendiensten und legt in § 312g Pflichten im elektronischen Geschäftsverkehr fest. Nach § 312g Abs. 1 BGB muss bei einem Vertragsabschluss im Internet eine Möglichkeit zur Korrektur von Eingabefehlern bestehen und der Vertrag ist durch das Unternehmen unverzüglich elektronisch zu bestätigen. Zudem müssen der Inhalt und die Bedingungen des Vertrages gespeichert werden und für den Kunden abrufbar sein. Nach § 312g Absatz 3 BGB ist bei einer zahlungspflichtigen Bestellung eine ausdrückliche Bestätigung erforderlich. Außerdem gilt das Kauf- und Gewährleistungsrecht des BGB auch für Softwareerstellung und -kauf. Das Gewährleistungsrecht des BGB stellt sowohl im Kauf- als auch im Werkvertragsrecht auf die vereinbarte Sollbeschaffenheit ab (§§ 434 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.

Einführungsgesetz zum BGB

- Das Einführungsgesetz zum Bürgerlichen Gesetzbuche (EBGB) enthält in Artikel 246 Regelungen zu den Informationspflichten bei Fernabsatzverträgen, also bei elektronischem Geschäftsverkehr. Diese Pflichten richten sich auf zahlreiche Angaben zum Unternehmen, zu den Produkten und Leistungen sowie zu Vertragsbedingungen. Art. 246 § 3 EBGB enthält Vorgaben zu den Informationspflichten bei Verträgen im elektronischen Geschäftsverkehr, z. B. nach Art. 246 § 3 Nr. 1 EBGB über die einzelnen technischen Schritte, die zu einem Vertragsabschluss führen. Nach Art. 246 § 3 Nr. 5 EBGB hat ein Unternehmen seine Kunden

außerdem über Verhaltenskodizes, denen es sich unterwirft, sowie den Zugang zu diesen Regelwerken zu unterrichten.

Einkommensteuergesetz

- Das Einkommensteuergesetz (EStG) beinhaltet in § 5b EStG die aktuell für viele Unternehmen unter dem Begriff „E-Bilanz“ relevante Pflicht, den „Inhalt der Bilanz sowie der Gewinn- und Verlustrechnung nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung zu übermitteln“.

Geldwäschegesetz

- Das Geldwäschegesetz (GwG) schreibt in § 4 Abs. 1 die Identifizierung von Vertragspartnern – also beispielsweise auch IT-Dienstleistern – bereits vor Begründung der Geschäftsbeziehung oder Durchführung einer geschäftlichen Transaktion vor. In § 4 Abs. 4 GwG werden die für die Identifizierung zu nutzenden Daten bzw. Dokumente aufgeführt. Die erhobenen Informationen sind nach § 8 GwG aufzuzeichnen und für mindestens fünf Jahre aufzubewahren. Hierbei können nach § 8 Abs. 2 GwG Bild- oder andere Datenträger zum Einsatz gelangen. Dabei „muss sichergestellt sein, dass die gespeicherten Daten mit den festgestellten Angaben übereinstimmen, während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können“.

Handelsgesetzbuch

- Das Handelsgesetzbuch (HGB) beinhaltet Vorgaben für die elektronische Geschäftskommunikation und die Verwendung von Bild- und Datenträgern im Rahmen der Buchführung. Nach § 12 Abs. 1 HGB sind Anmeldungen zur Eintragung in das Handelsregister und Dokumente nach § 12 Abs. 2 HGB elektronisch einzureichen. Auch die Offenlegung von Jahresabschlüssen hat elektronisch zu erfolgen. Bei der Geschäftskorrespondenz ist zu beachten, dass gemäß § 37a HGB auf Geschäftsbriefen, d. h. auch E-Mails, Angaben zur Firmierung, Vertretung und Handelsregistereintragung enthalten sind. Die Aufbewahrung von Handelsbriefen kann nach den §§ 238 Abs. 2, 257 Abs. 3 HGB auch auf Datenträgern erfolgen. Diese müssen allerdings während der Dauer der Aufbewahrungsfrist verfügbar und jederzeit lesbar sein.

Kunsturhebergesetz

- Die Veröffentlichung von Mitarbeiterfotos richtet sich nach dem Kunsturhebergesetz (KunstUrhG). § 22 KunstUrhG regelt für Bildnisse, also auch Fotos, dass diese „nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden“ dürfen. Dies betrifft insbesondere Mitarbeiterfotos, die vom Unternehmen zu Image- oder Werbezwecken im Internet publiziert werden.

- Das Strafgesetzbuch (StGB) ist bereits ggf. bei Verstoß gegen die anderen hier genannten und weitere Gesetze relevant. Es enthält aber zudem IT-spezifische Tatbestände. Dies sind die §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten), 202c (Vorbereiten des Ausspähens und Abfangens von Daten), 263a (Computerbetrug), 269 (Fälschung beweiserheblicher Daten), 270 (Täuschung im Rechtsverkehr bei Datenverarbeitung), 274 (Unterdrücken beweiserheblicher Daten), 303a (Datenveränderung) und 303b (Computersabotage). Strafgesetzbuch
- Das Urheberrechtsgesetz (UrhG) regelt in den §§ 4 und 87a bis e UrhG das Datenbankurheberrecht. Auch Websites sind häufig als Datenbankwerke i. S. des § 4 Abs. 2 UrhG geschützt. Um nicht gegen Urheberrechte zu verstoßen, erfordert somit jede Publikation von Inhalten auf einer Website entsprechende Nutzungs- und Verwertungsrechte. Soweit für die Website fremde Texte, Bilder oder andere schutzfähige Werke verwendet werden, muss eine ausreichende Übertragung der Nutzungsrechte (§§ 31 ff. UrhG) erfolgt sein. Urheberrechtsgesetz
- Das Umsatzsteuergesetz (UStG) stellt Anforderungen an den Gebrauch elektronischer Rechnungen. Deren Verwendung bedarf nach § 14 Abs. 1 der Zustimmung des Empfängers. Nach § 14 Abs. 1 UStG müssen bei einer Rechnung, die auf elektronischem Wege übermittelt wurde, die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet sein. Umsatzsteuergesetz
- Auch das Gesetz gegen den unlauteren Wettbewerb (UWG) ist für den Betrieb einer Website relevant. Bei ihrer Gestaltung sind die einzelnen in den §§ 4 bis 7 UWG aufgeführten Tatbestände unlauteren Wettbewerbs zu berücksichtigen. Außerdem enthält § 7 UWG Vorgaben für die Nutzung werblicher E-Mails, die eine unzumutbare Belästigung der Adressaten verbieten. Gesetz gegen den unlauteren Wettbewerb
- Nach der Zivilprozessordnung (ZPO) kann ein Gericht in einem Gerichtsverfahren die Anforderung stellen, im Besitz befindliche Unterlagen (Urkunden) vorzulegen. Dies stellt entsprechende Anforderungen an die (nicht nur elektronische) Dokumentation und Archivierung. Gemäß § 427 ZPO kann die Nichtvorlage dazu führen, dass der Beweis durch den Gegner als geführt gilt, insbesondere wenn, z. B. auf Grund der handelsrechtlichen Regelungen, eine Pflicht zur Aufbewahrung besteht. Zivilprozessordnung

4.1.4 Deutsche Verordnungen

Rechts-verordnungen

Anders als Gesetze unterliegen Rechtsverordnungen als untergesetzliche Rechtsnormen keinem förmlichen Gesetzgebungsverfahren. Stattdessen werden sie durch die Bundesregierung, eine Landesregierung oder ein Ministerium erlassen, wobei hierfür eine in einem Bundes- oder Landesgesetz geregelte Ermächtigung vorliegen muss. Ein Beispiel ist die Bildschirmarbeitsverordnung, die nach den Verordnungsermächtigungen des Arbeitsschutzgesetzes von der Bundesregierung mit Zustimmung des Bundesrates erlassen wurde.

Folgende Bundesrechtsverordnungen sind im Rahmen der IT-Compliance zu beachten:[46]

- Bildschirmarbeitsverordnung

  Die Bildschirmarbeitsverordnung (BildscharbV) enthält Vorgaben für die Arbeit an Bildschirmen; sie dient insbesondere der Sicherheit und dem Gesundheitsschutz der IT-Nutzer. In einem Anhang sind insgesamt 25 Einzelpunkte enthalten, mit denen Anforderungen an Bildschirmarbeitsplätze, z. B. hinsichtlich Geräten und Arbeitsumgebung, aber auch in Bezug auf die softwareergonomische Gestaltung, gestellt werden.

- Barrierefreie Informationstechnik-Verordnung

  Die Barrierefreie Informationstechnik-Verordnung (BITV 2.0) trifft Regelungen, um behinderten Menschen den Zugang und die Nutzung von Informationstechnik zu ermöglichen oder zu erleichtern. Sie betreffen vor allem die den IT-Nutzern angebotenen elektronischen Inhalte und Informationen. Entsprechende Anforderungen werden in einer Anlage getroffen.

- Preisangabenverordnung

  Die Preisangabenverordnung (PAngV) enthält Regelungen für den E-Commerce. In § 5 Abs. 1 wird bestimmt, dass der Ort eines Leistungsangebotes auch die Bildschirmanzeige sein kann. In § 4 Abs. 4 PAngV wird für diesen Fall den Ort der Preisauszeichnung festgelegt.

4.2 Verwaltungsvorschriften

Verwaltungs-vorschriften

Weitere für die IT relevante rechtliche Regelwerke stellen Verwaltungsvorschriften dar. Diese werden von Ministerien (z. B. dem Bundesfinanzministerium) oder Aufsichtsorganisationen (z. B. der Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) zur Interpretation der Rechtsnormen aufgestellt. „Diese Regelwerke bewirken rechtlich eine Selbstbindung der Ver-

[46] Im Folgenden nach *Klotz 2012*, S. 44ff.

waltung, indem sie die Anwendung der Rechtsnormen durch die Verwaltung bestimmen. Zudem ist die Entwicklung zu beobachten, dass es zunehmend ergänzende Informationsschreiben gibt, in denen dargelegt wird, wie spezielle Fragen zur Nutzung von IT aus Sicht der Verwaltung handzuhaben sind".[47] Die für die IT relevanten Verwaltungsvorschriften haben in der Regel die Form eines vom Bundesministerium für Finanzen (BMF) verfassten Schreibens. Insofern sind diese Verwaltungsvorschriften zumeist steuerlichen Inhalts.[48]

E-Bilanz

- In dem BMF-Schreiben vom 5. Juni 2012 zur E-Bilanz verweist das Bundesfinanzministerium darauf, dass für die Übermittlung der Bilanz sowie der Gewinn- und Verlustrechnung durch Datenfernübertragung die für das betreffende Wirtschaftsjahr jeweils geltende Taxonomie verwendet werden muss.

Übermittlung von Bilanz und GuV

- Im BMF-Schreiben vom 28. September 2011 zur „Elektronische Übermittlung von Bilanzen sowie Gewinn- und Verlustrechnungen" stellt das Bundesfinanzministerium klar, dass nicht beanstandet wird, wenn Unternehmen für das Wirtschaftsjahr 2012 ihre Bilanz sowie die Gewinn- und Verlustrechnung noch nicht durch Datenfernübertragung übermitteln. Erstmals verbindlich ist die elektronische Übermittlung von Bilanz und GuV somit in 2014 für den Jahresabschluss 2013.

GDPdU

- Das BMF-Schreiben vom 16. Juli 2001 beinhaltet die vieldiskutierten „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU). Die GDPdU regeln die Aufbewahrung digitaler Unterlagen und die Mitwirkungspflicht der Steuerpflichtigen bei Betriebsprüfungen. Die zentrale Mitwirkungspflicht besteht darin, dass ein Unternehmen im Falle der Erstellung steuerrelevanter Aufzeichnungen mit Hilfe eines IT-Systems nicht nur die Einsichtnahme in diese Daten zu ermöglichen, sondern nach Vorgabe der Finanzbehörde die Daten selbst auszuwerten oder auf einem lesbaren Datenträger zur Verfügung zu stellen hat. Weiterhin werden Unternehmen durch die GDPdU dazu verpflichtet, steuerrelevante Daten über einen Zeitraum von mindestens zehn Jahren unveränderbar sowie maschinell les- und auswertbar vorzuhalten. Das BMF-Schreiben zu den GDPdU wird durch einen Frage- und Antwortenkatalog sowie durch eine Information zum XML-basier-

[47] *Klotz 2012*, S. 50.
[48] Im Folgenden nach *ebd.*, S. 50ff.

ten Beschreibungsstandard, der für die Zugriffsart der Datenträgerüberlassung (sog. Z3-Zugriff) verpflichtend ist, ergänzt.

- Die im BMF-Schreiben vom 7. November 1995 publizierten „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) regeln die ordnungsmäßige Behandlung elektronischer Dokumente, insbesondere deren Aufbewahrung und Archivierung. Auch eine Verpflichtung zur Datensicherheit ist enthalten. Zudem für jedes DV-gestützte Buchführungssystem eine so genannte Verfahrensdokumentation zu erstellen.[49] GoBS

- Mit dem Schreiben vom 2. Juli 2012 zur Vereinfachung der elektronischen Rechnungsstellung erläutert das BMF, wie elektronische Rechnungen steuerlich korrekt zu nutzen sind, insbesondere hinsichtlich des Vorsteuerabzuges nach dem Umsatzsteuergesetz. Elektronische Rechnungen

4.3 Referenzierte Regelwerke

Unter „referenzierten Regelwerken“ sollen hier solche Regelwerke verstanden werden, „auf die in Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften verwiesen wird oder die von der Rechtsprechung zur Auslegung herangezogen werden. In anderen Wirtschaftsbereichen wird hiervon regelmäßig Gebrauch gemacht, beispielsweise im Bauwesen, wo in Urteilen DIN-Normen umfangreich zur Begründung herangezogen werden. In der IT-Branche sind derartige Verweise bisher jedoch kaum zu finden. Insbesondere haben Gerichte bisher (noch) nicht in ihren Urteilen auf die gängigen IT-Normen und -Standards zurückgegriffen.“[50] Referenzierte Regelwerken

Das wohl am häufigsten zitierte Beispiel für ein referenziertes Regelwerk ist in den Mindestanforderungen an das Risikomanagement (MaRisk) zu finden. Hierbei handelt es sich um ein Rundschreiben der BaFin vom 15.12.2010. Die MaRisk konkretisieren das von Kreditinstituten nach dem Kreditwesengesetz (KWG) einzurichtende Risikomanagement. Die der MaRisk zugehörige Anlage 1 enthält im Allgemeinen Teil (AT) unter „AT 7.2 Technisch-organisatorische Ausstattung“ Vorgaben für den IT-Einsatz. Die Erläuterun- MaRisk

[49] Die GoBS, die GDPdU und die Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung werden zurzeit durch die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD) abgelöst. Diese liegen derzeit in einem überarbeiteten Entwurf vor. Eine Veröffentlichung der finalen GoBD wird noch in 2014 erwartet.
[50] *Klotz 2012*, S. 18.

gen zu diesem Punkt geben Hinweise für die operative Umsetzung. Hierin wird sowohl auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutzkataloge als auch auf die Normenreihe ISO/IEC 2700X hingewiesen, auf die als „bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich ... abzustellen“[51] sei.

4.4 Rechtsprechung

Bedeutung von Urteilen

Für die Auslegung von Gesetzen sind Gerichtsurteile von hoher praktischer Bedeutung. Gleichwohl ist dies ein Bereich der IT-Compliance, in dem ein einigermaßen vollständiger und aktueller Überblick ohne den Einsatz spezialisierter juristischer Ressourcen fast unmöglich sein dürfte.[52]

BGH-Urteil zum Compliance Officer

Für den Bereich der Compliance allgemein ist das Urteil der Bundesgerichtshofes (BGH) vom 17. Juli 2009 (Az. 5 StR 394/08) von grundlegender Bedeutung. Im entschiedenen Fall wurde der Leiter der Innenrevision eines öffentlichen Entsorgungsbetriebes verurteilt. Dieser hatte entgegen der ihm vom Gericht zuerkannten Garantenstellung nicht verhindert, dass der Betrieb seinen Kunden überhöhte Gebühren in Gesamthöhe von 23 Mio. € in Rechnung gestellt hatte. Die Ausführungen des BGH sind insofern für die Compliance-Thematik relevant, da explizit auf die Position und Verantwortung eines „Compliance Officer“ eingegangen wird. Im Ergebnis kommt der BGH zu der Auffassung, dass dem Compliance Officer regelmäßig eine Garantenpflicht zukommt, die darauf abzielt, „im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern.“[53]

Schwächen in der IT als Verstoß gegen § 91 AktG

Speziell für die IT-Compliance liegt seit 2002 ein Urteil vor, das die Bedeutung der IT für alle Mitglieder eines Vorstands klarstellt. In dem vom Kammergericht Berlin am 27. September 2004 getroffenen Urteil (Az. 2 U 191/02) wird zwar die Kündigung des Vorstandsmitglieds letztinstanzlich als unwirksam erklärt, allerdings aus formalen Gründen (Fristüberschreitung). In der materiell-rechtlichen Argumentation des Landgerichts Berlin (Urteil vom 03.07.2002, Az. 2 O 358/01) wurde die Kündigung damit begründet, dass – basierend auf einer entsprechenden Feststellung im Jahresabschlussbericht

[51] *BAFIN 2012*, S. 24.
[52] Im Folgenden nach *Klotz 2012*, S. 57ff.
[53] *BGH 2009*, Rn. 27.

der beauftragten Wirtschaftsprüfungsgesellschaft – die vom Vorstand getroffenen Maßnahmen nicht die gesetzlichen Anforderungen an ein Risikofrüherkennungssystem nach § 91 Abs. 2 AktG und § 25a KWG erfüllt hätten. Hierbei wurde u. a. auch auf Schwächen in der IT Bezug genommen, insbesondere auf eine mangelhafte Datenqualität, die sich in einem veralteten und unvollständigen Datenbestand zeigte. Diesen Mangel befand das Gericht deswegen als „besonders gravierend, weil die Qualität und ständige Verfügbarkeit von EDV-Daten grundlegend ist für die Überwachung von Risiken und die Reaktion auf Risiken."[54] Zudem könne sich das gekündigte Vorstandsmitglied auch nicht darauf berufen, für die Datenverarbeitung nicht verantwortlich gewesen zu sein, da sie zum fraglichen Zeitpunkt „in den Verantwortungsbereich des Gesamtvorstands und damit auch in seine Verantwortung fiel"[55]

Urteile im Hinblick auf GDPdU

Für die IT-Compliance-Verantwortlichen im Unternehmen ergibt sich die Herausforderung, in Zusammenarbeit mit der Rechtsabteilung die für IT-Compliance relevanten Urteile zu identifizieren, ihre Auswirkung für das Unternehmen abzuschätzen und gegebenenfalls entsprechend notwendige Maßnahmen umzusetzen. Ein Bereich, in dem zahlreiche Urteile mit praktischen Folgen zu finden sind, betrifft die Anwendung der GDPdU. Beispielsweise hat das Finanzgericht Rheinland-Pfalz in seinem Urteil vom 20. Januar 2005 (Az. 4 K 2167/04) einen Fall entschieden, in dem eine Bank ihre Datenbestände für die Betriebsprüfung nicht so organisiert hat, dass das Bankgeheimnis nach § 30a AO bei einer Betriebsprüfung gewahrt bleiben konnte. Das Finanzgericht bestätigte jedoch die Pflicht des Geprüften, die Buchhaltungsdaten derart abzugrenzen, dass für steuerlich nicht relevante Daten anderweitige gesetzliche Vorgaben, wie Datenschutz, Berufsgeheimnis oder wie in diesem Fall das Bankgeheimnis, eingehalten werden.[56] In einem anderen Urteil zur Anwendung der GDPdU betonte das Finanzgericht Schleswig-Holstein in seinem Urteil vom 3. Februar 2010 (Az. 3 V 243/09) den repressiven und präventiven Charakter des Verzögerungsgeldes nach § 146 Abs. 2b AO. In dem entschiedenen Fall wurde durch die Finanzverwaltung ein Verzögerungsgeld verhängt, da das betreffende Unternehmen der Aufforderung zur Datenträgerüberlassung nach mehrmaligen Anforderungen nicht nachkam. Nachdem das Unternehmen dem Verlangen genügte, be-

[54] *LG Berlin 2002*, Rn. 29.
[55] *Ebd.*, Rn 29.
[56] Vgl. *Kaminski 2010*, S. 22f.

harrte die Finanzverwaltung – nach dem Gericht zu Recht – auf der Forderung des Verzögerungsgeldes.[57]

Urteile im Hinblick auf Software

Auch Urteile, die sich mit der Entwicklung und Einführung von Software befassen, finden sich in großem Umfang. So hat das Oberlandesgericht Köln in seinem Urteil vom 29. Juli 2005 (Az. 19 U 4/05) zum Anforderungsprofil einer Individualsoftware entschieden, dass es grundsätzlich die Aufgabe des Auftraggebers ist, das für die Softwareentwicklung erforderliche Anforderungsprofil zu erstellen. Der Auftragnehmer muss hieran jedoch in geeigneter Weise mitwirken. Hinsichtlich der Lieferung einer Standard-Software ist nach dem Urteil des Landgerichtes Landshut vom 20. August 2003 (Az. 2 HK O 2392/02) Kaufrecht zu Grunde zu legen. Eine Anwendung des Werkvertragsrechts käme nur dann in Frage, wenn die Standard-Software den individuellen Bedürfnissen des Kunden in einem Umfang angepasst werden muss, dass im Ergebnis eine Individual-Software vorliegt. Weiterhin hat das Gericht entschieden, dass ein Handbuch auch als CD-ROM übergeben werden darf. In Bezug auf die Übergabe eines Handbuches liegt weiterhin ein Urteil des Landgerichtes Stuttgart vom 24. Januar 2002 vor (Az. 8 O 274/99) vor. Hierin wird klargestellt, dass die Übergabe eines Handbuches beim Verkauf von Hard- und Software eine Hauptleistungspflicht darstellt.

Urteil zur Datensicherungspflicht

Ein weiterer Bereich der IT, zu dem verschiedene Urteile getroffen wurden, ist die Datensicherung. So hat beispielsweise das Landgericht Stuttgart in seinem Urteil vom 30. Januar 2002 (Az. 38 O 149/00 KfH) klargestellt, dass jeder Softwareanwender eine regelmäßige Datensicherung vorzunehmen habe. Hierzu gehöre auch die Überprüfung der Vollständigkeit und Wiederherstellbarkeit. Ein weiteres, vielzitiertes Urteil stammt vom Oberlandesgericht Hamm (Urteil vom 01. Dezember 2003, Az. 13 U 133/03). Das Gericht hat eine unterlassene Datensicherung bei Schäden, die durch Datenverlust entstehen, als Mitverschulden gewertet. Deswegen wurde in dem entschiedenen Fall die Haftung einer beauftragten IT-Firma für Datenverluste verneint. Das beauftragende Unternehmen hatte die Datensicherung lediglich auf monatlicher Basis durchgeführt, was das Gericht als nicht ausreichend erachtete und deshalb dem Unternehmen anlastete, die Datenverluste selbst fahrlässig verursacht zu haben. Das Gericht stellte fest, dass eine Datensicherung täglich, eine Vollsicherung mindestens einmal wöchentlich zu erfolgen habe.

[57] Vgl. *ebd.*, S. 28f.

Urteile im Hinblick auf die Nutzung von Social Media

Auch aus der Nutzung der IT und insbesondere von Internet und Social Media ergeben sich zahlreiche Rechtsstreitigkeiten mit entsprechend für die IT-Compliance relevanten Urteilen. In einem vom Landesarbeitsgericht Hessen entschiedenen Fall (Urteil vom 24. Januar 2012, Az. 19 SaGa 1480/11) erließ das Gericht mit Bezugnahme auf das Kunsturhebergesetz eine einstweilige Verfügung. Die beklagte Organisation hatte nach Ausscheiden einer Mitarbeiterin deren Daten (Bild, Name, Profil) zu Unrecht nicht aus dem auf der Internetseite des Unternehmens befindlichen News-Blog entfernt. Dass gezieltes Netzwerken mitunter einen Verstoß gegen das Wettbewerbsrecht darstellen kann, zeigt das Urteil des Landgerichts Heidelberg vom 23. Mai 2012 (Az. 1 S 58/11). Hier ging es um einen Versuch der Mitarbeiterabwerbung von Wettbewerbern durch gezielte Zusendung von Nachrichten über die Social Media-Plattform „XING“. Das Gericht beurteilte die Kontaktaufnahme in Verbindung mit herabsetzenden Äußerungen über den Arbeitgeber der angemailten Mitarbeiter als eine nach UWG wettbewerbswidrige Abwerbung.

Handlungsbedarf

Diese wenigen Beispiele zeigen, dass aus Gerichtsurteilen vielfältige Vorgaben für die IT-Compliance resultieren können. Natürlich ist jeder Fall individuell zu beurteilen. Trotzdem ergibt sich für die IT-Compliance die Herausforderung, die IT-bezogene Rechtsprechung zu verfolgen und aus den Urteilen Folgerungen für eigene Compliance-Maßnahmen abzuleiten. Diese Analyse muss kontinuierlich und systematisch ausgeführt werden. Hierzu ist es erforderlich, die entsprechende Verantwortlichkeit im Unternehmen zu verankern (z. B. innerhalb der Rechtsabteilung), die Ergebnisse auszuwerten und an die Betroffenen (IT-Abteilung, Personalmanagement, Revision etc.) zu kommunizieren.

4.5 IT-Verträge

IT-Verträge

Verträge, die ein Unternehmen mit Kunden, Hard- und Software-Lieferanten und sonstigen Marktpartnern (z. B. IT-Beratern, Versicherungen) abschließt und die IT-relevante Vereinbarungen enthalten, ergänzen die Gruppe der rechtlichen Regelwerke. Im Gegensatz zu den bisher genannten rechtlichen Regelwerken besitzen Verträge jedoch keine allgemeine Verbindlichkeit, sondern verpflichten lediglich die jeweiligen Vertragspartner. Im Mittelpunkt stehen hier die zahlreichen Möglichkeiten des IT-Outsourcings, z. B. durch Vergabe von Entwicklungs- und Wartungsaufträgen oder des Betriebs kompletter Anwendungen an spezialisierte IT-Dienstleistungsunternehmen.

In allen Fällen der Inanspruchnahme externer Dienste sowie beim Erwerb von informationstechnischem Anlagevermögen und Software-Lizenzen entstehen für Unternehmen vertragliche Bindungen, die wegen ihrer Vielzahl, ihres Umfanges, ihrer Spezifität sowie ihrer inhaltlichen und rechtlichen Komplexität Gegenstand von Compliance-Maßnahmen sein müssen.[58]

Verantwortung

Auf IT-Verträge bezogene Compliance-Maßnahmen werden wohl eher selten bei einem „IT-Compliance Manager“ angesiedelt sein. Eher dürften diesbezügliche Aufgaben von der IT-Beschaffung, der Rechtsabteilung oder im Rahmen von IT-Projekten, bei deren Durchführung externe Beauftragungen erfolgen, wahrgenommen werden. Die Notwendigkeit steht jedoch außer Frage, insbesondere wenn die Vielzahl unterschiedlicher Vertragsarten berücksichtigt wird, vgl. Tabelle 4.

Risiken aus mangelnder Vertrags-Compliance

Ohne eine vertragsbezogene Compliance drohen das Verfehlen der Zielsetzung, die mit der Inanspruchnahme externer Leistungen erreicht werden soll, ggf. materielle oder immaterielle Verluste, eine Gefährdung eigener Rechtspositionen und daraus resultierender Ansprüche, eine Überschreitung geplanter Kosten, Friktionen im IT-Betrieb oder bei der Durchführung von IT-Projekten.[59] Um derartige Risiken zu vermeiden, hat eine auf die Einhaltung von IT-Verträgen zielende Compliance inhaltliche, terminliche, organisatorische und rechtliche Maßnahmen zu ergreifen.[60]

Inhaltliches Vertragsmanagement

Die inhaltsorientierten Maßnahmen richten sich auf die

- Kontrolle der Übereinstimmung von tatsächlichen und vereinbarten Produkteigenschaften und Leistungen;
- Kontrolle der Regelungen zur nachhaltigen Nutzbarkeit (z. B. das Nachhalten von Softwarehinterlegungsvereinbarungen);
- Aufnahme von Leistungsstörungen.

Terminliches Vertragsmanagement

Die terminlichen Maßnahmen umfassen die

- Überwachung der Einhaltung von Terminen (bzgl. Lieferung, Leistungserbringung, Abnahme etc.);
- Überwachung von Reaktionszeiten (z. B. Rückmeldezeiten bei einer externen Hotline oder Reparaturzeiten bei einem Servicevertrag);

[58] Nach *Klotz/Dorn 2005*, S. 97.
[59] Vgl. *Klotz/Dorn 2005*, S. 98.
[60] Vgl. im Folgenden *ebd.*, S. 102f.

Tabelle 4
IT-Vertragsarten

Gegenstand	Vertrag
Dienstleistung	- IT-Planungsvertrag - IT-Beratungsvertrag - IT-Rahmen- und Einzelvertrag - Generalunternehmer- und Subunternehmervertrag - IT-Schulungsvertrag - IT-Body-Leasing-Vertrag - IT-Projektvertrag
Hardware	- Kaufvertrag für Hardware - Mietvertrag für Hardware - Leasingvertrag für Hardware - Wartungsvertrag für Hardware
Software	- Softwareerstellungsvertrag - Standardsoftware-Überlassung nach Kaufrecht - Standardsoftware-Überlassung nach Mietrecht - Softwarepflegevertrag - Supportvertrag (Hotlinie-/Helpdeskverträge)
Infrastruktur	- Rechenzentrumsvertrag - Backup-Vertrag - Softwarehinterlegungsvertrag
Internet	- Providervertrag - Access-Providing-Vertrag - Webhosting-Vertrag - Werbevertrag
Versicherung	- Datenverlustvertrag - Betriebsausfall-Vertrag - IT-Haftpflichtvertrag
Quelle: Eigene Darstellung	

- Überwachung der Einhaltung von Laufzeiten und Fristen (Vertragsdauer, Kündigungsfrist, Prüffrist, Gewährleistungsfrist etc.).

Organisatorisches Vertragsmanagement

Die organisatorischen Maßnahmen betreffen die Kontrolle der Erfüllung von

- Berichtspflichten;
- Dokumentationspflichten;
- Mitwirkungspflichten.

Rechtliches Vertragsmanagement

Die rechtlichen Maßnahmen umfassen die

- Kontrolle der Voraussetzungen für die Geltendmachung des Anspruches auf Zahlung einer Vertragsstrafe und ggf. die Initiierung der Anspruchserhebung;

- Kontrolle der notwendigen und übertragenen Nutzungsrechte zur Vermeidung von Verstößen gegen Rechte Dritter (Urheber-, Nutzungs- und Schutzrechte).
- Kontrolle der Voraussetzungen für die Geltendmachung von Durchsetzbarkeit von Minderungsansprüchen und ggf. die Initiierung der Anspruchserhebung;
- Kontrolle der Voraussetzungen für die Geltendmachung von Schadenersatzansprüchen und ggf. die Initiierung der Anspruchserhebung;

Beziehungen zwischen Verträgen

Bei der Vielzahl der IT-Verträge ist außerdem eine Kontrolle von Abhängigkeiten und Überschneidungen zwischen den verschiedenen Verträgen erforderlich. So bedürfen beispielsweise im Rahmen von IT-Projekten die Lieferfristen von Software- und Hardwarebeschaffungen einer Abstimmung genauso wie die Koordination von Mitwirkungspflichten gegenüber mehreren Vertragspartnern. Auch in der Vorbereitung von IT-Outsourcing-Verträgen sind anderweitig bestehende IT-Verträge entsprechend Art und Umfang der auszulagernden Aufgaben zu prüfen und ggf. anzupassen oder zu kündigen, um eine überlappende oder doppelte Leistungsinanspruchnahme zu verhindern.

5 Für IT-Compliance relevante IT-Normen und -Standards

5.1 Abgrenzung Normen vs. Standards

Standard

IT-bezogene Normen und Standards stellen die wesentlichen unternehmensexternen Regelwerke dar. Da die Begriffe „Normen“ und „Standards“ oft in einem Zuge genannt werden, stellt sich die Frage nach der Abgrenzung der beiden Begriffe.[61] Ein Standard beschreibt die Art und Weise der Ausführung einer Aufgabe, der Lösung eines Problems oder der Handhabung einer Technik oder eines Instruments. Allerdings stellt nicht jede Zusammenfassung von Begriffen, Zielen, Konzepten, Methoden, Empfehlungen u. Ä. einen Standard dar. Zur Verschriftung eines Regelwerkes muss hinzukommen, dass die im Standard enthaltenen Regelungen breit akzeptiert und angewendet werden. „Der Akzeptanzbereich kann dabei geografisch (z. B. auf einen Staat oder eine Staatengemeinschaft) oder auf eine nationale, internationale oder globale Anwendergruppe (z. B. Ingenieure, Projektmanager) beschränkt sein. Die Anwendergruppe muss zudem den Standard nicht nur kennen und akzeptieren, sondern auch wirklich praktisch nutzen. Aus dieser Nutzung muss sich außerdem eine Rückkopplung für die Weiterentwicklung des Standards ergeben.“[62]

Norm

Ähnlich wie ein Standard beschreiben Normen „wissenschaftlich begründete Arbeitsmethoden zur Bewältigung rationeller, meist wiederholbarer Arbeitsprozesse … bzw. Qualitäts- und Sicherheitsanforderungen.“[63] Eine Norm ist das Ergebnis eines systematischen, definierten Normungsverfahrens. Eine Norm ist damit ein „Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird.“[64] Eine Norm erhält einen offiziellen Charakter dadurch, dass die Normungsorganisation die Norm in ihrem Geltungsbereich fachlich durchsetzen kann. Aus diesem Grund werden Normen auch als „de-jure-Standard“ bezeichnet.

Verbindlichkeit von Normen

Aufgrund des formalisierten Erstellungsprozesses beinhalten Normen für gewöhnlich nicht den innovativsten Stand eines Anwendungsgebietes, sondern

[61] im Folgenden nach *Klotz 2013b*, S. 739.
[62] *Ebd.*
[63] *VOI 2008*, S. 18.
[64] *DIN 2007*, S. 25.

fixieren vielmehr die durch praktische Bewährung allgemein anerkannten Regeln eines (technischen) Anwendungsbereiches. Insofern werden Normen häufig – z. B. von externen Gutachtern in Gerichtsverfahren – herangezogen um festzustellen, ob Sorgfaltspflichten eingehalten wurden. Mitunter werden Normen in nationalen und internationalen Vorschriften, d. h. vor allem in Gesetzen und Verordnungen, verbindlich vorgeschrieben. In diesen Fällen erlangt eine Norm eine unmittelbare rechtliche Bindungswirkung.[65]

Normungsorganisationen

Eine Norm wird im Gegensatz zu einem Standard von einer offiziellen Normungsorganisation entwickelt, beschlossen und veröffentlicht. Eine Normungsorganisation ist eine Institution, „die auf nationaler, regionaler oder internationaler Ebene anerkannt ist und als wesentliche Funktion, dank ihrer Statuten, die Erstellung, Anerkennung oder Annahme von Normen hat, welche der Öffentlichkeit zugänglich sind".[66] Für das Management der IT relevante Normungsorganisationen sind

- in Deutschland das „DIN Deutsches Institut für Normung e. V." (DIN);
- auf internationaler Ebene die „International Standardization Organization" (ISO) und die „International Electrotechnical Commission" (IEC);
- auf europäischer Ebene das Europäische Komitee für Normung (Comité Européen de Normalisation – CEN).

ISO/IEC Joint Technical Committee 1

Der Großteil der für die IT relevanten Normen wird gemeinsam von der ISO und der IEC als ISO/IEC-Norm veröffentlicht. Das ISO/IEC Joint Technical Committee 1 stellt das von der ISO und der IEC gemeinsame gebildete Gremium für die Normung im Bereich der Informationstechnik dar. Für die operative Normungsarbeit ist dieses in weitere Sub-Komitees gegliedert, beispielsweise das Subcommittee SC 7, Software and systems engineering, das für die ISO/IEC 38500 verantwortlich zeichnet. Innerhalb des Deutschen Instituts für Normung (DIN) agiert der Normenausschuss Informationstechnik und Anwendungen (NIA) als nationales Gremium für die Normung in der IT und in ausgewählten Anwendungsbereichen der Informationstechnik. In der internationalen Normungsarbeit stellt der NIA das deutsche Spiegelgremium zur ISO/IEC JTC1 dar.[67]

---

[65] Nach *VOI 2008*, S. 18.
[66] *DIN EN 45020*, S. 33.
[67] Nach *Klotz 2013a*, S. 12f.

5.2 IT-Normen

DIN 66271 und DIN 66399

Normen im Bereich der Informations- und Kommunikationstechnologie („IT-Normen“) gibt es viele. Für die IT-Compliance sind jedoch prinzipiell nur solche Normen relevant, die das Management des IT-Einsatzes im Unternehmen adressieren. In diesem Bereich gibt es nur wenige allein vom DIN erarbeitete und verabschiedete Normen:

- So behandelt die DIN 66271 Softwarefehler und ihre Beurteilung. Sie fordert insbesondere eine transparente Fehlerklassifizierung.
- Die aus zwei Teilen bestehende DIN 66399 regelt die Vernichtung von Datenträgern mit schutzbedürftigen Informationen. Es werden im Einzelnen Gruppen von Datenträgern, Schutzklassen und Sicherheitsstufen definiert.

DIN ISO 15489-1

Als einzig relevante, allein von der ISO übernommene Norm liegt derzeit lediglich die DIN ISO 15489-1 vor. Sie beschreibt grundlegende Anforderungen an die rechtssichere Dokumenten- und Aktenverwaltung.[68]

ISO/IEC-Normen

In der Gruppe der ISO/IEC-Normen findet sich eine größere Anzahl relevanter IT-Normen. [69]

- Die ISO/IEC 12207 beinhaltet „einen Prozessstandard für die Entwicklung und das Management von Software. Hierfür beschreibt sie eine Architektur für den Lebenszyklus von Software, beginnend mit der ersten Bedarfs- und Anforderungsanalyse über Projektmanagement und Akquisition, Implementierung, Betrieb und Support bis hin zur Ablösung/ Außerbetriebnahme.“[70]
- Die ISO/IEC 18043 beinhaltet Regelungen in Bezug auf die Auswahl, den Einsatz und den Betrieb von Intrusion Detection Systemen (IDS).
- Die Normenreihe „ISO/IEC 20000-x“ beschreibt Anforderungen an ein IT-Servicemanagement (ITSM). Hierbei enthält die ISO/IEC 20000-1 Mindestanforderungen an ein professionelles IT-Service-Management, die ISO/IEC 20000-2 gibt Leitlinien für die Gestaltung von ITSM-Systemen vor und die ISO/IEC 20000-3 beinhaltet allgemeine praktische Anleitungen für die Umfangsdefinition.

---

[68] Nach *Klotz 2013a*, S. 18ff.
[69] Nach *Klotz 2013a*, S. 28ff.
[70] *Ebd.*, S. 28f.

- Die ISO/IEC 24762 beschreibt Anforderungen an interne und externe Dienste zur Wiederherstellung (Disaster recovery) von Informations- und Kommunikationstechnologien.
- Die ersten drei Normen der ISO/IEC 270xx-Normenreihe sind bereits vom DIN übernommen worden (s. u.). Weitere ISO/IEC-Normen richten sich u. a. auf ein Informationssicherheits-Risikomanagement (ISO/IEC 27005), eine IT Security Governance (ISO/IEC 27014), die Rolle der IT im Rahmen des unternehmensweiten Kontinuitätsmanagements (ISO/IEC 27031), die Cybersecurity (ISO/IEC 27032) oder ein Incident-Management für die Informationssicherheit (ISO/IEC 27035).
- In die Gruppe der ISO/IEC-Normen fällt auch die bereits erwähnte ISO/IEC 38500 zur Corporate governance of information technology.
- Zudem unterstützt die ISO/IEC 90003 Unternehmen bei der Anwendung der Qualitätsnorm ISO 9001 (Quality management systems – Requirements) in Bezug auf den Softwareeinsatz.

DIN ISO/IEC-Normen

Die ISO/IEC-Normen werden vom DIN kontinuierlich daraufhin geprüft, ob sie als deutsche Norm übernommen werden sollen. In diesem Fall erhalten sie eine „DIN ISO/IEC“-Kennung, wie dies bereits für folgende Normen erfolgt ist.[71]

- Allen vier DIN ISO/IEC-Normen sind Teil der Normenreihe „DIN ISO/IEC 15504-x“ (die ISO/IEC 15504-5 und ISO/IEC 15504-6 liegen bisher nur als ISO/IEC-Normen vor). Die Normen beschreiben ein Modell zur Bewertung von Prozessen, das in der Fachdiskussion unter dem Namen „SPICE“ (Software Process Improvement and Capability Determination) bekannt ist. Dieses Modell unterstützt durch einen strukturierten Ansatz zur Verbesserung der Entwicklungsprozesse das Management der Softwareentwicklung.
- Die DIN ISO/IEC 19770-1 trifft Regelungen für das Software Asset Management (SAM). Die Norm behandelt die SAM-Prozesse zur Verwaltung der genutzten Software-Ressourcen, insbesondere der Lizenzen.
- Die DIN ISO/IEC 270xx-Normenreihe enthält Richtlinien und Empfehlungen für ein Informationssicherheits-Managementsystems (ISMS). Die ersten drei Normen der Reihe wurden vom DIN übernommen. Die

[71] Nach *ebd.*, S. 21ff.

DIN ISO/IEC 27000 gibt einen Überblick über Informationssicherheits-Managementsysteme (ISMS) und ist der konzeptionelle Rahmen für die weiteren Normen der Reihe. Die DIN ISO/IEC 27001 beinhaltet Anforderungen an eine systematische Erstellung, Umsetzung, Dokumentation, Ausführung, Überwachung und Weiterentwicklung eines ISMS. Insbesondere wird hierbei die Verantwortung des Managements, z. B. für eine grundlegende Verpflichtung auf Informationssicherheit oder für die Bereitstellung von Ressourcen, herausgestellt. Die ISO/IEC 27002 enthält „einen umfangreichen Maßnahmenkatalog zur Umsetzung der DIN ISO/IEC 27001. Behandelt werden die Einschätzung von und der Umgang mit Sicherheitsrisiken, die Nutzung einer Sicherheitsrichtlinie, die Organisation der Informationssicherheit und das Asset Management, hier insbesondere die Klassifizierung von Information. Weitere Themen sind personelle Aspekte der Sicherheit, die physische Sicherheit, das Betriebs- und Kommunikationsmanagement, Zugangskontrolle, die Beschaffung, Entwicklung und Wartung von Informationssystemen, der Umgang mit Informationssicherheitsvorfällen,“[72] das IT-Kontinuitätsmanagement und Compliance als Einhaltung von Vorgaben.

5.2 IT-Standards

IT-Standards

Noch unübersichtlicher als bei den Normen ist die Situation bei den IT-Standards, die es von zahlreichen Organisationen (Berufs- und Branchenverbänden, Fachorganisationen, Vereinen, Behörden, Agenturen etc.) zu den verschiedensten IT-Handlungsbereichen (z. B. IT-Governance, IT-Sicherheit oder IT-Servicemanagement) gibt. Oftmals ist es der Sinn derartiger Regelwerke, Mindeststandards zu definieren, die dem Adressatenkreis des Standards als Orientierung in dem betreffenden Handlungsbereich dienen sollen. Wegen der mangelnden allgemeinen Verbindlichkeit von Standards kann ihre Entwicklung und Verbreitung als Form der Selbstregulierung angesehen werden. Durch im Standard enthaltene Richtlinien, Empfehlungen, Vorgehensmodelle etc. sollen Best Practices im Sinne von auf kaufmännischer Sorgfalt basierenden Verfahrensweisen zur Verfügung gestellt werden.[73] In Tabelle 5 sind einige der in der Unternehmenspraxis international genutzten IT-Standards aufgelistet.[74]

[72] *Klotz 2013a*, S. 27.
[73] Nach *Rath/Sponholz 2009*, S. 78f.
[74] Vgl. *Johannsen/Goeken 2011*, S. 26.

Abkürzung	Standard
CMMI®	Capability Maturity Model Integration[75]
COBIT® 5	Control Objectives for Information and Related Technology[76]
ISAE 3402	International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a Service Organization
ITIL®	IT Infrastructure Library®[77]
PRINCE 2®	Projects in controlled environments[78]
Risk IT	The Risk IT Framework
TOGAF®	The Open Group Architecture Framework[79]
Val IT	Val IT Framework 2.0
Eigene Darstellung	

Tabelle 5
International verbreitete IT-Standards

IDW-Standards

Für die IT-Compliance sind vor allem Standards von hoher Relevanz, auf deren Basis Testierungen oder Zertifizierungen vorgenommen werden. Hierzu zählen auf nationaler Ebene vor allem die Prüfungs- und Rechnungslegungsstandards des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW), siehe Tabelle 6.

ISAE-Standards

Für Provider von IT-Infrastruktur und -Services und ihre Kunden ist der Standard ISAE 3402 von geschäftskritischer Bedeutung. In der Nachfolge des US-amerikanischen Audit-Standards "Statement on Auditing Standards (SAS) No. 70 Service Organizations" wurde mit dem "International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a Service Organization" ein internationaler Standard geschaffen, nach dem bei einer Auslagerung von IT-Leistungen diejenigen Kontrollen beim Provider geprüft werden, die für das rechnungslegungsbezogene interne Kontrollsystem (IKS) des jeweiligen Kunden relevant sind. Bei der Anwendung des Standards werden zwei Berichtstypen unterschieden. Typ-1 Berichte beurteilen Kontrollen dahingehend, ob und inwiefern sie geeignet sind, die Kontrollziele zu erreichen. Typ-2 Berichte treffen zusätzlich Aussagen zur Wirksamkeit der eingerichteten Kontrollen.

[75] CMMI® is a registered mark of Carnegie Mellon University.
[76] COBIT® is a registered trademark of ISACA.
[77] ITIL® is a registered trademark of AXELOS Limited; IT Infrastructure Library® is a registered trademark of AXELOS Limited.
[78] PRINCE® is a registered trademark of AXELOS Limited.
[79] TOGAF® is a registered trademark of The Open Group.

Nr.	Titel
IDW PS 261 n. F.	Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken
IDW PS 330	Abschlussprüfung bei Einsatz von Informationstechnologie
IDW PS 331	Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen
IDW PS 850	Projektbegleitende Prüfung bei Einsatz von Informationstechnologie
IDW PS 880	Die Prüfung von Softwareprodukten
IDW PS 951	Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen
IDW PS 980	Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen
IDW RS FAIT 1	Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie
IDW RS FAIT 2	Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce
IDW RS FAIT 3	Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren
IDW RS FAIT 4	Anforderungen an die Ordnungsmäßigkeit und Sicherheit IT-gestützter Konsolidierungsprozesse
Eigene Darstellung	

Tabelle 6
Standards des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW)

COBIT

Aus Sicht sowohl der IT-Governance und der IT-Compliance als auch der Wirtschaftsprüfung und des IT-Auditing stellt COBIT (Control Objectives for Information and Related Technology) den zentralen IT-Standard dar. COBIT wurde von dem in den USA ansässigen Prüfungsverband ISACA (Information Systems Audit and Control Association) entwickelt und erstmals im April 1996 veröffentlicht.[80] Die erste Version formulierte Anforderungen an die IT – bezeichnet als „Control Objectives“ – und richtete sich damit in erster Linie an Wirtschaftsprüfer. Durch das Erreichen dieser Control Objectives sollte ein effizienter und effektiver Einsatz von IT-Ressourcen in Unternehmen gewährleistet werden. In den Folgejahren entwickelte sich COBIT zu einem umfassenden Framework für das IT-Management, mit

[80] Im Folgenden nach *Gaulke 2014*, S. 9ff.; *Klotz 2013b*, S. 722ff.

dem die IT-Prozesse nicht nur geprüft, sondern proaktiv gestaltet werden können. Das Prozessmodell von COBIT wurde über die Zeit durch zwei weitere ISACA-Frameworks (Val IT und Risk IT) ergänzt. Außerdem berücksichtigt COBIT auch wichtige IT-Normen, wie ISO/IEC 20000, ISO/IEC 27005 oder ISO/IEC 38500, und Standards, z. B. die „Information Technology Infrastructure Library" (ITIL) oder den Architektur-Standard "The Open Group Architecture Framework" (TOGAF). Die aktuelle fünfte Version von COBIT wurde 2012 veröffentlicht. COBIT 5 integriert nunmehr die beiden anderen ISACA-Frameworks „Val IT 2.0" und „Risk IT", wobei sich vier Domänen auf das IT-Management richten und eine Domäne die IT-Governance adressiert. Durch die Erweiterung besteht das Prozessmodell jetzt aus fünf Domänen mit insgesamt 37 Prozessen:[81]

5 COBIT-Domänen

- Evaluieren, Vorgeben und Überwachen (Evaluate, Direct and Monitor – EDM);
- Anpassen, Planen und Organisieren (Align, Plan and Organise – APO);
- Aufbauen, Beschaffen und Implementieren (Build, Acquire and Implement – BAI);
- Bereitstellen, Betreiben und Unterstützen (Deliver, Service and Support – DSS);
- Überwachen, Evaluieren und Beurteilen (Monitor, Evaluate and Assess – MEA).

COBIT-Struktur

Für jeden Prozess werden in Aktivitäten untergliederte Governance- bzw. Managementpraktiken beschrieben, mit denen die prozess- und IT-bezogenen Ziele erreicht werden können. Zur Messung der Zielerreichung werden exemplarische Metriken vorgeschlagen. Weiterhin sind die an den IT-Prozessen beteiligten Stellen und Rollen verzeichnet. Die Beteiligungsformen richten sich auch in COBIT 5 nach dem RACI-Rollenmodell (R = responsible, A = accountable, C = consulted, I = informed). Im RACI-Diagramm werden für jeden IT-Prozess die Organisationsstrukturen bzw. Rollen mit den einzelnen Managementpraktiken des betreffenden Prozesses verbunden.[82]

ITIL

Der wohl am weitesten verbreitete IT-Standard dürfte die „Information Technology Infrastructure Library" (ITIL) sein. Sie richtet sich auf Planung, Betrieb und Steuerung von IT-Services und bildet insofern den zentralen

[81] Vgl. *ITGI 2012a*, S. 26.
[82] Nach *Klotz 2013c*, S. 28.

Standard für das IT-Servicemanagement (ITSM). Entwickelt wurde der Standard 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 übertragen. In der aktuellen dritten Version besteht die „Library“ aus fünf Büchern zu

- Servicestrategie (Service Strategy),
- Serviceentwurf (Service Design),
- Serviceüberführung (Service Transition),
- Servicebetrieb (Service Operation) und
- zur kontinuierlichen Serviceverbesserung (Continual Service Improvement).

Zertifizierung

Eine Zertifizierungsmöglichkeit nach ITIL auf der institutionellen Ebene gibt es nicht, diese muss für das IT-Servicemanagement nach der ISO/IEC 20000 erfolgen.[83] Lediglich auf der persönlichen Ebene können verschiedene ITIL-Zertifikate als Qualifikationsnachweise erlangt werden.

BSI-Standards

Auf nationaler Ebene gibt es neben den IDW-Standards weitere verbreitete IT-Standards, insbesondere im Bereich der Informations- bzw. IT-Sicherheit. Von Bedeutung sind hier vor allem die IT-Grundschutz-Standards, die vom „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) herausgegeben werden, siehe Tabelle 7.

Tabelle 7
IT-Grundschutz-Standards des BSI

Nummer	Titel
BSI-Standard 100-1	Managementsysteme für Informationssicherheit (ISMS)
BSI-Standard 100-2	IT-Grundschutz-Vorgehensweise
BSI-Standard 100-3	Risikoanalyse auf der Basis von IT-Grundschutz
BSI-Standard 100-4	Notfallmanagement
Eigene Darstellung	

Weitere IT-Standards

Neben den allgemeinen Standards, die sich grundsätzlich an Unternehmen aller Branchen richten, liegen auch branchenspezifische Standards vor. Ein Beispiel hierfür ist der Prozess-Standard „Enhanced Telecom Operations

[83] Nach *Klotz 2013b*, S. 740.

Map“ (eTom), der in der Telekommunikationsbranche weit verbreitet ist. Ein weiteres Beispiel ist der „Payment Card Industry Data Security Standard” (PCI DSS), der für alle Handelsunternehmen maßgeblich ist, deren Geschäftsprozesse Kreditkarten-Transaktionen beinhalten. Für Kreditinstitute ist nach wie vor Basel II ein relevantes Regelwerk, indem es im Rahmen der Auflistung operationeller Risiken in fast allen Kategorien potenzielle Bedrohungen benennt, die zu Gefährdungen der IT führen können.[84]

Überblick als Herausforderung

Insgesamt wird deutlich, dass zahlreiche Normen und Standards für das IT-Management und damit für die IT-Compliance in unterschiedlichem Ausmaß von Bedeutung sind. Für Unternehmen allgemein und die IT-Compliance speziell gilt es somit, im Bereich der IT-Normen und -Standards insoweit einen Überblick zu erhalten und zu bewahren, dass eine fundierte Entscheidung darüber möglich ist, welche Standards für die Unternehmens-IT relevant sind und – ganz im Sinne der Definition von IT-Compliance – als verbindlich erachtet werden.

[84] Vgl. *Klotz 2007b*, S. 97f.

6 Unternehmensinterne Regelwerke

Unternehmens-interne Regelwerke

Unternehmensinterne Regelwerke dienen in Unternehmen seit jeher als Instrumente der Steuerung und Überwachung von Prozessen, der Koordination der Aufgabenausführung im Rahmen der Arbeitsteilung und der Verhaltensteuerung der Belegschaft. Dies gilt auch für die unternehmensweite Nutzung der IT und die IT-Funktion des Unternehmens. Durch die mit dem IT-Einsatz notwendig verbundene Strukturierung und Formalisierung von Arbeitsabläufen stellt die IT zweifelsfrei einen der am umfangreichsten durch unternehmensinterne Regelwerke „regulierten" Unternehmensbereiche dar.

QM- Strukturierung

Eine Strukturierung der unternehmensinterne Regelwerke ist schwierig, da begriffliche Abgrenzungen je nach fachlicher Orientierung variieren. So trifft beispielsweise die DIN EN ISO 9000 für das Qualitätsmanagement (QM) eine Unterscheidung von Dokumenten nach Spezifikationen, QM-Handbüchern, QM-Plänen und Aufzeichnungen für den Nachweis von ausgeführten Tätigkeiten und erreichten Ergebnissen.[85] Diese Bezeichnungen lassen sich durchaus auch auf Regelwerke der IT anwenden. So dürften in nahezu jedem Unternehmen Handbücher für die Nutzung von Anwendungen, IT-Pläne vielfältiger Art, Spezifikationen für die Programmentwicklung, Leitfäden und Verfahrensbeschreibungen im Rahmen von IT-Prozessen, Anleitungen für die Gewährleistung der IT-Sicherheit oder Aufzeichnungen über die Durchführung von IT-Kontrollen vorhanden sein. An dieser Stelle soll jedoch eine IT-affine Klassifizierung mit fünf Gruppen verwendet werden[86], deren Begriffe in der Praxis eine breitere Verwendung finden, s. Abbildung 4.

- IT Policy

  IT Policy

  Eine „Policy" beschreibt aus Sicht des verantwortlichen Managements „grundsätzliche Werte, Vorstellungen oder Ziele zum Einsatz der IT insgesamt oder zu einzelnen Themen".[87] Hierzu können Leitbilder zählen, die in Bezug auf die IT übergeordnete Aussagen zum Stellenwert des Produktionsfaktors „Information", zur Verantwortung der Unternehmensmitglieder für einen effektiven und effizienten Einsatz dieses Produktionsfaktors und die gewünschte Art und Weise des Umgangs mit

[85] Nach *DIN EN ISO 9000*, S. 29f.
[86] Vgl. im Folgenden nach *Böhm 2009*, S. 16f., *Peltier 2004*, S. 10f.
[87] *Böhm 2009*, S. 16.

IT und IT-Ressourcen beinhalten.[88] Aber auch IT-Richtlinien zählen zu dieser Gruppe. Richtlinien dienen der Steuerung der Unternehmensprozesse. In ihnen ist zwar nicht jeder einzelne Prozessschritt festgelegt, aber als generelle Vorgaben sichern sie transparente und kontrollierbare Problemlösungswege und die Zuweisung von Verantwortlichkeiten.[89] Beispiele sind leicht für die IT-Sicherheit zu finden. So kann es eine generelle Richtlinie für die IT-Sicherheit insgesamt geben (wie sie als Leitlinie zur Informationssicherheit vom BSI empfohlen wird[90]) oder für einzelne sicherheitsrelevante Bereiche, beispielsweise eine E-Mail-Policy. Policies sind grundsätzlich verbindlich, allerdings bedürfen sie in der Regel zur ihrer Umsetzung und Überprüfung einer Konkretisierung. Hierzu dienen hausinterne IT-Standards.

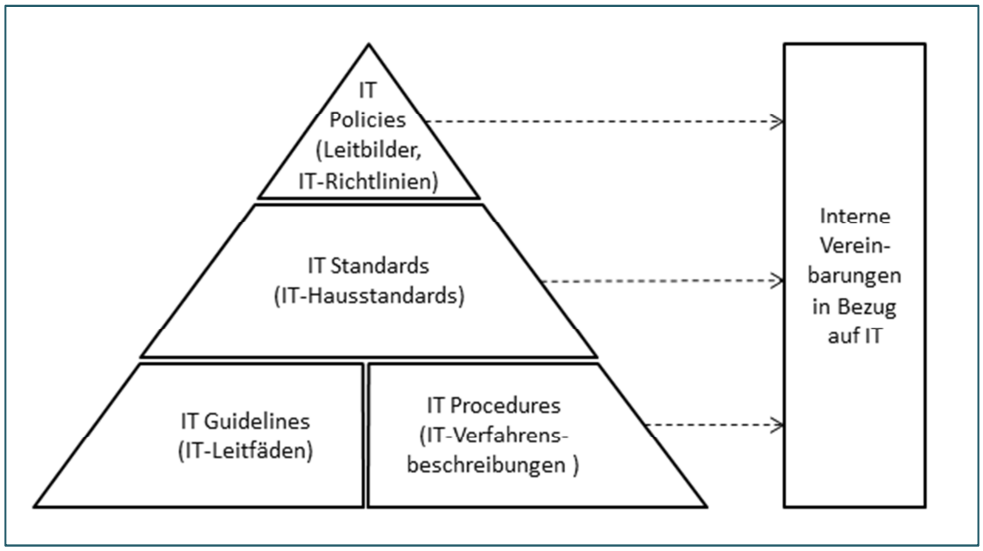

Abbildung 4
Unternehmensinterne Regelwerke der IT-Compliance

IT Standard

IT Standard

Ein „Standard“ i. S. eines unternehmensspezifischen IT-Hausstandards beinhaltet „Mindestanforderungen an Applikationen, IT-Services, Prozesse und sonstige Themen in der IT“.[91] Da Standards der Umsetzung von Policies dienen, sind sie ebenfalls verbindlich. So kann beispielsweise ein Hausstandard für die Nutzung von Passwörtern Regeln für die mindestens erforderliche Passwortkomplexität vorschreiben. IT-Haus-

[88] Vgl. *Pietsch/Martiny/Klotz 2004*, S. 277ff.
[89] Nach *Picot/Dietl/Franck 2008*, S. 257f.
[90] Vgl. *BSI 2008*, S. 24.
[91] *Böhm 2009*, S. 17.

standards sind so konkret, dass ihre Einhaltung anhand von Kontrollen überwacht werden kann (was für das Beispiel der Passwortkomplexität offensichtlich ist). Hausstandards können und sollen als verbindliche Mindestanforderungen jedoch nicht das gesamte Handeln der Unternehmensmitglieder in Bezug auf die Nutzung von Informationen und IT-Systemen regeln. In Fällen, wo es lediglich Vorgaben i. S. einer Orientierung geben kann, kommen Guidelines zum Einsatz. Im Gegensatz dazu finden dort, wo ein Standard durch eine Folge festgelegter Handlungen anzuwenden ist, Procedures Verwendung.

- IT Guidelines

IT Guidelines

„Guidelines“ geben als nicht verbindliche Leitfäden Hinweise zur Erfüllung einer IT Policy. Sie beinhalten häufig Best Practices, die mit Empfehlungen helfen, in einer konkreten Entscheidungssituation die grundsätzliche Vorgabe einer Policy zu erfüllen. So können in Bezug auf die IT-Sicherheit Leitfäden verwendet werden, die Hinweise für die IT-Sicherheitsverantwortlichen in den verschiedenen Organisationseinheiten des Unternehmens enthalten, z. B. zur Sensibilisierung der Mitarbeiter oder zur Analyse von Sicherheitslücken, die dieser situationsspezifisch auslegen und anwenden muss.

- IT Procedures

IT Procedures

„Procedures“ stellen als Verfahrensbeschreibungen häufig eine Schritt-für Schritt-Anweisung dar. Eine Verfahrensbeschreibung „ist immer durchführungsorientiert gestaltet, ob nun als Text, Checkliste, Ablaufdiagramm oder IT-gestützter Prozess (Workflow)“.[92] Ein Beispiel wäre eine IT-Verfahrensanweisung für die Nutzung von Passworten, in der im Einzelnen die Vergabe, der Gebrauch und die Änderung der Passworte in den jeweiligen notwendig durchzuführenden Schritten beschrieben sind.

- Interne Vereinbarungen

Interne Vereinbarungen

Interne Vereinbarungen in Bezug auf die IT regeln in vielen Bereichen das Zusammenwirken zwischen der IT-Funktion und den Fachabteilungen. Sie richten sich auf die Zusammenarbeit im Rahmen von IT-Prozessen oder der Nutzung von IT-Services und regeln verbindlich den

[92] *Böhm 2009*, S. 17.

Leistungsaustausch sowie die hierfür erforderliche Zuordnung von Verantwortung. Insofern können die internen Vereinbarungen auch zur Umsetzung einer IT-Policy dienen oder die Anwendung von IT-Hausstandards oder IT-Verfahrensanweisungen beinhalten. Beispiele sind Regelungen im Rahmen von Service-Level-Agreements (SLAs) oder eigenständige Vereinbarungen zur Verrechnung von IT-Leistungen.

Verwaltung der Regelwerke

In der Summe wird sich in einem Unternehmen eine große Anzahl an internen Regelwerken in Bezug auf die IT anfinden. Auch wenn die Erstellung und Verwaltung der verschiedenen Regelwerke höchst unterschiedlich sein dürfte, so ist doch ein allgemeines Management der Regelwerke in ihrer Form als (elektronische) Dokumente sinnvoll. Dies betrifft vor allem ihre Bezeichnung, Merkmalsbeschreibung inkl. Klassifizierung, das Zugriffs- und Änderungsmanagement sowie ihre Speicherung und Archivierung.

7 IT-Compliance und Unternehmensziele

Unternehmens-interne Regelwerke

Die Sicherstellung von IT-Compliance stellt zweifelsfrei ein Unternehmensziel dar. Unternehmen haben sich an geltendes Recht zu halten und Rechtsverstöße seitens der Unternehmensmitglieder gegenüber der Gesellschaft, öffentlichen Einrichtungen, Lieferanten und Kunden zu vermeiden. Diese Sichtweise findet sich auch in dem bereits erwähnten IT-Governance Framework „COBIT“ wieder. COBIT 5 beinhaltet 17 allgemeine Unternehmensziele, die den einzelnen Ebenen einer Balanced Scorecard (BSC) zugeordnet sind. Zwei Unternehmensziele beziehen sich auf Compliance:

- Unternehmensziel 4: Einhaltung externer Gesetze und Bestimmungen (Compliance);
- Unternehmensziel 15: Compliance mit internen Richtlinien.

Nachteile aus Non-Compliance

Hierbei ist das Ziel der Compliance mit internen Richtlinien der internen BSC-Perspektive zugeordnet, das Ziel der Einhaltung externer Gesetze und Bestimmungen (Compliance) dagegen der Finanzperspektive.[93] Eine Erklärung hierfür findet sich in COBIT 5 nicht. Allerdings lässt sich die Zuordnung leicht mit den mit Non-Compliance verbundenen finanziellen Nachteilen für Unternehmen, die gegen gesetzliche und behördliche Vorgaben verstoßen, begründen. So sollen Gefängnisstrafen, insbesondere Buß- und Zwangsgelder, Schadensersatzleistungen, Vertragsstrafen, aber auch erhöhte Steuerzahlungen aufgrund von Schätzungen des Finanzamts vermieden werden.[94] Dabei sind die Risiken aus mangelnder IT-Compliance nicht immer offensichtlich. So kann sich beispielsweise ein Schaden ergeben, wenn ein Unternehmen im Rahmen einer gerichtlichen Auseinandersetzung beweiserhebliche Daten und Dokumente nicht vorlegen und damit seine Beweispflicht nicht erfüllen kann. Wird in Bezug auf steuerrelevante Unterlagen gegen Archivierungspflichten verstoßen, können Strafzahlungen wegen Steuerverkürzung die Folge sein. Neben diese monetären Schäden kann ein Imageschaden für das Unternehmen treten, wenn etwa gegen Datenschutzvorschriften verstoßen wird. Hieraus können negative Nachrichten in den Medien, der Ausschluss bei der Vergabe öffentlicher Aufträge oder gar Kundenverluste resultieren. Ein weiteres Beispiel für negative Folgen von Non-Compliance in Bezug auf die IT liegt vor, wenn die Due-Dilligence-Prüfung

[93] Vgl. *ITGI 2012b*, S. 21.
[94] Im Folgenden nach *Klotz 2009*, S. 17ff.

im Rahmen einer Unternehmenstransaktion IT-Compliance-Risiken offenbart und sich hieraus Abschläge bei der Bestimmung des Unternehmenswertes ergeben.

Wertbeitrag

Die Vermeidung von Nachteilen ist somit als der wesentliche Wertbeitrag von IT-Compliance im Rahmen des „Value Delivery“ der IT insgesamt anzusehen. Neben dieser Schutzfunktion ergeben sich aus IT-Compliance jedoch zahlreiche weitere Vorteile[95], s. Abbildung 5.

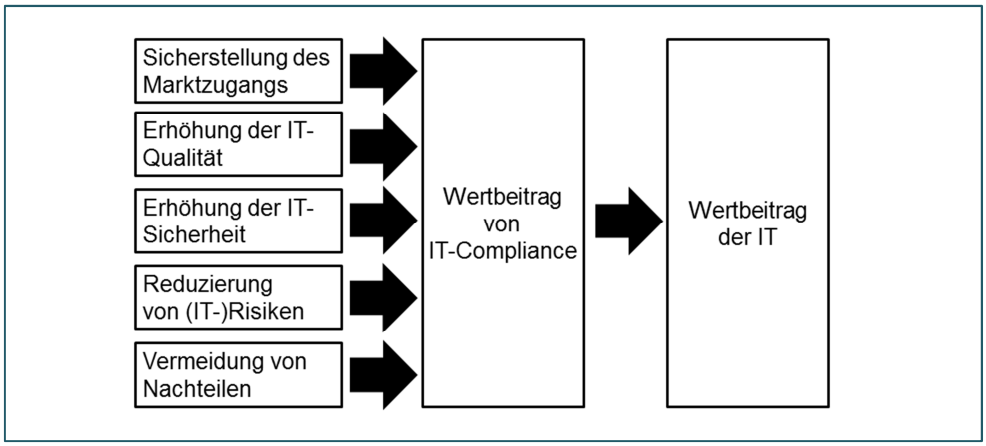

Abbildung 5
Wertbeitrag von IT-Compliance

- Marktzugang: Erweisen sich bestimmte unternehmensexterne IT-Standards (z. B. IT-Sicherheitszertifikate oder individuelle Qualifikationsnachweise) oder Anforderungen des Auftraggebers (z. B. hinsichtlich technischer und organisatorischer Schnittstellen zur überbetrieblichen Kopplung logistischer Systeme) als Markteintrittsbarrieren, so ist der Wertbeitrag offensichtlich. Ohne die Erfüllung derartiger externer Vorgaben können Aufträge nicht erlangt, Umsatzpotenziale nicht erschlossen werden.
- IT-Qualität: Viele Maßnahmen der IT-Compliance tragen zu einer höheren Qualität der Unternehmens-IT, insbesondere zu einer effizienten Organisation, zu Transparenz und Effektivität von IT-Prozessen und -Services, bei. Dies resultiert unmittelbar aus der Anwendung prozessbezogener Normen (wie z. B. ISO/IEC 12207 oder ISO/IEC 90003) und Standards (wie z. B. COBIT). IT-Richtlinien zu internen Hard- und Softwarestandards führen zu einer Homogenisierung und damit verbunden zu einer Reduzierung der Komplexität der IT-Infrastruktur.

[95] Vgl. *Böhm 2008*, S. 26f.

- IT-Sicherheit: Ein direkter Zusammenhang ergibt sich auch hier aus der Konformität mit IT-Sicherheitsnormen (insbesondere der Normenreihe DIN ISO/IEC 27000ff.) und -standards (z. B. den IT-Sicherheitsstandards des BSI). Aber auch Maßnahmen der IT-Compliance, die gesetzliche Vorgaben des IT-Betriebs sicherstellen, adressieren zu einem hohen Anteil die Sicherheit der IT. Gerade beim Bundesdatenschutzgesetz ist dieser Zusammenhang über die in der Anlage zu § 9 BDSG aufgeführten technischen und organisatorischen Kontrollmaßnahmen deutlich und kann als Compliance-Verpflichtung zu IT-Sicherheit aufgefasst werden.[96]
- IT-Risiken: Die Reduzierung von IT-Risiken folgt auf der einen Seite ebenso wie für die IT-Sicherheit aus der Anwendung entsprechend spezialisierter Normen (vor allem der ISO/IEC 27005) und Standards (z. B. Risk IT der ISACA). Auf der anderen Seite ergibt sich die Reduzierung von IT-Compliance-Risiken aus der Erfüllung insbesondere der rechtlichen Compliance-Anforderungen.

Kosten und ROI

Hinsichtlich der IT-Kosten stellt sich die Situation differenziert dar. So verursachen die verschiedenen Maßnahmen der IT-Compliance selbstverständlich Kosten. Da die Maßnahmen aber auch aus Gründen der Erhöhung der IT-Qualität, der Reduzierung von IT-Risiken und der Erhöhung der IT-Sicherheit erfolgen, lassen sich die damit verbundenen Kosten in der Regel nicht eindeutig der IT-Compliance zurechnen. „Dies gilt natürlich auch umgekehrt für die Kosteneinsparungen, die sich u. a. aus der Automatisierung manueller Arbeitsabläufe (beispielsweise 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 – somit nur in einem größeren Zusammenhang ermittelt werden. Trotzdem gilt, dass IT-Compliance zwar Investitionen erfordert, aber auch zur Reduzierung von IT-Kosten beiträgt.“[97]

[96] Vgl. *Schmidl 2009*, S. 709.
[97] *Klotz 2009*, S. 19.

8 IT-Compliance-Managementsystem

IT-Compliance-Managementsystem

Um IT-Compliance als Unternehmensziel zu erreichen, bedarf es systematischer Aktivitäten im Rahmen einer effektiven und effizienten Struktur. Mit anderen Worten bedarf es eines speziellen Managementsystems, dessen oberstes Ziel die Sicherstellung von IT-Compliance ist. In Übertragung der Definition des IDW lassen sich unter einem IT-Compliance-Managementsystem (IT-CMS) Grundsätze und Maßnahmen verstehen, die ein regelkonformes Verhalten – d. h. das Einhalten von Regeln und das Verhindern von wesentlichen Regelverstößen – der Unternehmensmitglieder und ggf. beteiligter Dritter sicherstellen.[98] Hierzu müssen die Elemente eines IT-Compliance-Managementsystems, siehe Abbildung 6, aufeinander abgestimmt sein und im betrieblichen Alltag operativ zusammenwirken.

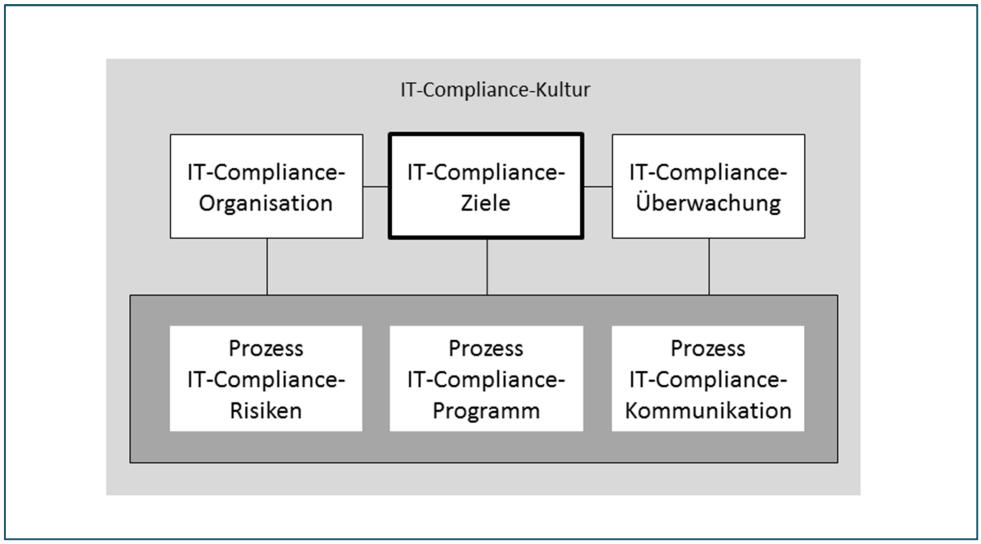

Abbildung 6
IT-Compliance-Managementsystem nach IDW

Die Konzeption eines IT-Compliance-Managementsystems beinhaltet[99]

- die Förderung einer IT-Compliance-Kultur;
- die Festlegung der IT-Compliance-Ziele;
- den Prozess der Feststellung und Analyse der IT-Compliance-Risiken;
- den Prozess zur Erstellung des IT-Compliance-Programms;
- den Aufbau der IT-Compliance-Organisation;

[98] Nach *IDW 2011*, Tz. 6.
[99] Nach *ebd.*, Tz. 10.

- die Entwicklung eines Kommunikationsprozesses und
- die Entwicklung von Verfahren zur Überwachung und Verbesserung des IT-Compliance-Managementsystems.

IT-Compliance-Kultur

Die im Unternehmen herrschende Compliance-Kultur stellt die Grundlage für die Angemessenheit und Wirksamkeit des IT-Compliance-Managementsystems dar. Die IT-Compliance-Kultur wird zwar wesentlich von der allgemeinen Compliance-Kultur beeinflusst werden, weist aber eben auch IT-spezifische Ausprägungen auf. Dies gilt beispielsweise hinsichtlich des Umgangs mit personenbezogenen Daten oder geschäftlich sensiblen Dokumenten, vor allem dann, wenn mobile Endgeräte zum Einsatz gelangen. Für die einzelnen Mitarbeiter spielt die Vorbildfunktion des Managements bis hin zur Unternehmensleitung (sog. „tone at the top“) eine wichtige Rolle für ihre Bereitschaft, die Vorgaben der IT-Regelwerke einzuhalten.[100] Eine wichtige Funktion können hierbei IT-bezogene Leitbilder und Verhaltenskodizes einnehmen. Ein IT-Leitbild kann eine wichtige Orientierung für den Stellenwert des „Produktionsfaktors“ Information für das Unternehmen und darauf aufbauend hinsichtlich der Verantwortung der Mitarbeiter für einen effektiven und effizienten Einsatz dieses Produktionsfaktors bieten. Verhaltenskodizes können ergänzend die vom Unternehmen gewünschte Art und Weise der Informationsnutzung verdeutlichen.[101]

IT-Compliance-Ziele

Die Ziele für die IT-Compliance sind aus den Compliance-Zielen des Unternehmens abzuleiten bzw. werden mit diesen in einer hierarchischen Zielpyramide verknüpft sein. Hieraus ergeben sich Prioritäten und Gewichtungen für die IT-Compliance-Ziele. In Unternehmen, wo das operative Unternehmensgeschäft in hohem Maß von der Funktionsfähigkeit der IT abhängt, werden die Ziele für die IT-Compliance eine wesentlich höhere Bedeutung haben als in Unternehmen, wo dies nicht der Fall ist. Bei der Festlegung der IT-Compliance-Ziele sind die Anforderungen der Konsistenz, der Verständlichkeit und Praktikabilität, der Messbarkeit und der Erreichbarkeit durch die vorhandenen Ressourcen zu beachten.[102] Aus den IT-Compliance-Zielen leitet sich dann auch der Umfang der Ausgestaltung der anderen Elemente des IT-Compliance-Managementsystems ab, insbesondere der Umgang mit IT-Compliance-Risiken.

---

[100] Nach *ebd.*, Tz. 23.
[101] Vgl. *Pietsch/Martiny/Klotz 2004*, S. 278f.
[102] Nach *IDW 2011*, A 15.

IT-Compliance-Risiken

Die IT-Compliance-Risiken sind – idealerweise im Rahmen des unternehmensweiten Risikomanagements – zu managen. Hierzu bedarf es vor allem einer systematischen Erkennung, Analyse der IT-Compliance-Risiken sowie einer adäquaten Berichterstattung. Bei der Erkennung von IT-Compliance-Risiken sind neben den Entwicklungen im rechtlichen Umfeld insbesondere personelle Veränderungen und die Nutzung neuer Informationstechnologien, beispielsweise Cloud Computing oder Big Data, relevant. Auch der Ort der Geschäftstätigkeit ist vor dem Hintergrund des Einsatzes mobiler Technologien und damit zusammenhängender Entwicklungen, wie Mobile Office-Technologien oder BYOD (Bring Your Own Device), von Bedeutung.[103] Für die Ausgestaltung eines entsprechenden Prozesses kann auf den COBIT-Prozess „APO12, Managen des Risikos“ zurückgegriffen werden. Dieser adressiert in den ersten beiden von insgesamt sechs Managementpraktiken das Erfassen von risikobezogenen Daten und das Analysieren des Risikos.[104]

IT-Compliance-Programm

Das IT-Compliance-Programm soll mittels Grundsätzen und Maßnahmen Non-Compliance soweit wie möglich vermeiden und damit die IT-Compliance-Risiken begrenzen. Unter Grundsätzen sind hier Reglungen zu verstehen, die i. S. der oben angesprochenen Verhaltenskodizes ein regelkonformes Verhalten der Unternehmensmitglieder sicherstellen sollen. Diese Regelungen müssen klare Festlegungen zur Zulässigkeit bzw. Unzulässigkeit von informationsbezogenen Verhaltensweisen sowie zu den Sanktionen im Falle von Non-Compliance umfassen. Die Maßnahmen des IT-Compliance-Programms richten sich auf das Erkennen von Compliance-Verstößen (z. B. mittels eines Hinweisgeber-Systems) und die Reaktion darauf. Wird Non-Compliance aufgedeckt, ist ggf. eine zeitnahe Kommunikation an externe Stellen vorzunehmen, so wie dies beispielsweise gemäß § 42a BDSG bei unrechtmäßiger Kenntniserlangung personenbezogener Daten der Fall ist. Auch die Einrichtung einzelner prozessintegrierter Kontrollen im Rahmen des internen Kontrollsystems (IKS) zählt zu den Maßnahmen des IT-Compliance-Programms.[105]

IT-Compliance-Organisation

Die Einrichtung der IT-Compliance-Organisation umfasst die Festlegung von Prozessen, Aufgaben und Verantwortlichkeiten. In aufbauorganisatorischer Hinsicht kann die Stelle eines IT-Compliance-Officer in Verbindung

[103] Vgl. *IDW 2011*, A 16.
[104] Vgl. *ITGI 2012*, S. 110ff.
[105] Nach *IDW 2011*, A 17.

mit der Einrichtung entsprechender IT-Compliance-Gremien bzw. ihre Integration in die Compliance-Organisation des Unternehmens sinnvoll sein. Aber auch die Zusammenarbeit mit der zentralen Compliance-Funktion des Unternehmens, dem Risikomanagement, der Revision und der Rechtsabteilung ist zu klären. Für die prozessuale Gestaltung kann eine Orientierung an COBIT 5 erfolgen. Der Standard beinhaltet einen speziellen Compliance-Prozess. Dies ist der Managementprozess „MEA03, Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen“. Er soll sicherstellen, dass alle externen Compliance-Anforderungen identifiziert und adäquat berücksichtigt werden. Der Prozess gliedert sich in vier Prozesspraktiken, die vor allem die extern orientierte IT-Compliance adressieren:

- Identifizieren externer Compliance-Anforderungen;
- Optimieren der Reaktion auf externe Anforderungen;
- Bestätigen der externen Compliance;
- Erhalten von Compliancebestätigungen.[106]

Zur Gestaltung der IT-Compliance-Organisation zählt auch die Integration der Maßnahmen und Managementsysteme der IT-Compliance in andere Managementsysteme des Unternehmens, insbesondere in das Risikomanagementsystem und das interne Kontrollsystem. Im Rahmen dieser Aufgabe wird regelmäßig auch die Frage der Tool-Nutzung zu klären sein, wobei auch hier eine Integration in vorhandene GRC- bzw- IKS-Tools angestrebt werden sollte.[107]

IT-Compliance-Kommunikation

Die Mitarbeiter des Unternehmens, ggf. auch Dritte, müssen zur Wahrnehmung ihrer IT-Compliance-Verantwortung ausreichend informiert sein. Hierzu umfasst die IT-Compliance-Kommunikation

- die Kommunikation der zu beachtenden IT-Regelwerke und ihrer einzelnen Vorgaben;
- die Kommunikation des IT-Compliance-Programms;
- die Festlegung von Berichtsanlässen und -wegen zur Kommunikation von IT-Compliance-Risiken und -Verstößen an die zuständigen Stellen;
- die Ergebniskommunikation der Überwachungsmaßnahmen.

[106] *ITGI2012a*, S. 215ff.
[107] Nach *IDW 2011*, A18.

Kommunikations-instrumente

Die IT-Compliance-Kommunikation bedient sich der üblichen Instrumente der internen Unternehmenskommunikation. Dies sind beispielsweise explizierte Leitlinien, Handbücher, Prozessbeschreibungen, Newsletter, aber natürlich auch Schulungsmaßnahmen. IT-Compliance muss zudem auch Gegenstand der Mitarbeiterführung sein. Hierbei ist vor allem die Bedeutung einer konsequenten, zeitnahen und vollständigen IT-Compliance-Kommunikation zu vermitteln.[108]

IT-Compliance-Überwachung

Die Überwachung der IT-Compliance erfolgt durch prozessunabhängige Stellen, z. B. die interne IT-Revision. Sie richtet sich auf die angemessene Ausgestaltung und die Wirksamkeit des IT-Compliance-Managementsystems, insbesondere der prozessintegrierten Kontrollen des IKS. Zeigen sich im Ergebnis der Überwachung Schwachstellen, so sind deren Ursachen zu ermitteln und Maßnahmen zur ihrer Beseitigung zu konzipieren und umzusetzen, beispielsweise eine Verstärkung der Kommunikationsmaßnahmen oder die Implementierung zusätzlicher Kontrollen. Werden Regelverstöße durch Unternehmensmitglieder bzw. Dritte aufgedeckt, sind personelle bzw. vertraglich vorgesehene Maßnahmen zu ergreifen. Bei schweren oder wiederholten Verstößen sind ggf. auch Verträge zu kündigen. Aber auch in diesen Fällen ist zu überlegen, wie diese Entwicklungen präventiv hätten verhindert werden können, so dass in der Summe aller Maßnahmen eine kontinuierliche Verbesserung des IT-Compliance-Managementsystems erreicht wird.[109]

Integration

Für die Wirksamkeit des IT-Compliance-Managementsystems ist es entscheidend, das IT-CMS in das unternehmensweite Compliance-Managementsystem zu integrieren, das grundsätzlich die gleiche Struktur aufweist. Dies verweist darauf, dass IT-Compliance als funktionsspezifische Ausprägung nicht losgelöst von der Corporate Compliance konzipiert, eingeführt, betrieben und weiterentwickelt werden kann. Dies betrifft die IT-Compliance im Allgemeinen und das IT-Compliance-Managementsystem in allen seinen Elementen im Besonderen.

[108] Nach *IDW 2011*, A19.
[109] Nach *ebd.*, A20.

Quellenangaben

BAFIN 2012: Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN): Anlage 1: Erläuterung zu den MaRisk in der Fassung vom 14.12.2012, online unter: http://www.bundesbank.de/Redaktion/DE/Downloads/Kerngeschaeftsfelder/Bankenaufsicht/Marisk/2012_12_14_erlaeuterungen.pdf?__blob=publicationFile (letzter Zugriff: 12.07.2014)

Benzler/Weber-Rey 2013: Compliance und Aufsichtsrecht. In: Inderst, C.; Bannenberg, B.; Poppe, S. (Hg.): Compliance, Aufbau – Management – Risikobereiche. 2. Aufl., C.F. Müller, Heidelberg 2013, S. 629-772

BGH 2009: Bundesgerichtshof (BGH): Urteil vom 17.07.2009 (Az. 5 StR 394/08), zitiert nach juris: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=48874&pos=0&anz=1 (letzter Zugriff: 12.07.2014)

BITKOM 2008: BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hg.): Die Nutzung von E-Mail und Internet im Unternehmen – Rechtliche Grundlagen und Handlungsoptionen, Version 1.5, Stand: 16.01.2008, Berlin 2008, online unter: http://www.bitkom.org/files/documents/BITKOM_Leitfaden_E-mail_und_Internet_im_Unternehmen_V.1.5_2008.pdf (letzter Zugriff: 12.07.2014)

Böhm 2008: Böhm, M.: IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT. In: HMD – Praxis der Wirtschaftsinformatik, Jg. 45 (2008), Nr. 263, S. 15-29

Böhm 2009: Böhm, M.: IT-Governance – Ein Überblick. dpunkt, Heidelberg 2009

BSI 2008: Bundesamt für Sicherheit in der Informationstechnik (Hg.): BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS), Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2008, online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile (letzter Zugriff: 12.07.2014)

DB AG 2014: Deutsche Bahn AG (Hg.): Corporate Governance – Begriffsklärung, online unter: http://www1.deutschebahn.com/ecm2-db-de/ir/cg/begriffserklaerung.html (letzter Zugriff: 12.07.2014)

DCGK 2013: Regierungskommission Deutscher Corporate Governance Kodex (Hg.): Deutscher Corporate Governance – Kodex in der Fassung vom 13. Mai 2013, online unter: http://www.dcgk.de/de/kodex/aktuelle-fassung/praeambel.html (letzter Zugriff: 12.07.2014)

Deutsche Bank 2014: Deutsche Bank AG (Hg.): Corporate Governance, online unter: https://www.deutsche-bank.de/ir/de/content/corporate_governance.htm (letzter Zugriff: 12.07.2014)

Deutscher Bundestag 1998: Deutscher Bundestag: Gesetzentwurf der Bundesregierung - Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), Drucksache 13/9712 vom 28.01.1998, Deutscher Bundestag, online unter: http://dipbt.bundestag.de/doc/btd/13/097/1309712.pdf (letzter Zugriff: 12.07.2014)

DIN EN ISO 9000: Qualitätsmanagementsysteme – Grundlagen und Begriffe. Deutsche Norm (ISO 9000:2005); dreisprach. Fassung, EN ISO 9000:2005 (2005), Beuth, Berlin 2005

DIN EN 45020: Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004); dreisprach. Fassung, EN 45020:2006 (2007), Beuth, Berlin 2007

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

Hauschka 2010: Hauschka, C.: § 1, Einführung. In: Hauschka, C. (Hg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 2. Aufl., Beck, München 2010, S. 1–25

Hilb 2013: Hilb, M.: Integrierte Corporate Governance: Ein neues Konzept zur wirksamen Führung und Aufsicht von Unternehmen. 5. Aufl. Springer, Berlin-Heidelberg 2013

IDW 2011: Institut der deutschen Wirtschaftsprüfer (IDW) (Hg.): IDW PS 980 – Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, Stand 11.03.2011, Institut der deutschen Wirtschaftsprüfer, Düsseldorf

ISO/IEC 38500: International Organization for Standardization (Hg.): International Standard ISO/IEC 38500:2008, Corporate Governance on Information Technology, First Edition 2008

ITGI 2001: IT Governance Institute (Hg.): Board Briefing on IT Governance. IT Governance Institute, Rolling Meadows 2001

ITGI 2003: IT Governance Institute (Hg.): Board Briefing on IT Governance. 2nd Ed., IT Governance Institute, Rolling Meadows 2003, online unter: http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf (letzter Zugriff am 12.07.2014)

ITGI 2012a: IT Governance Institute (Hg.): COBIT 5 – Enabling Processes, IT Governance Institute, Rolling Meadows 2012

ITGI 2012b: IT Governance Institute (Hg.): COBIT 5 – Rahmenwerk für Governance und Management der Unternehmens-IT, IT Governance Institute, Rolling Meadows 2012

Johannsen/Goeken 2011: Johannsen W., Goeken M.: Referenzmodelle für IT-Governance – Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co. dpunkt, Heidelberg 2011

Kaminski 2010: Kaminski, I.: Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, Jg. 2 (2010), Nr. 8, online unter: https://www.econstor.eu/dspace/bitstream/10419/60092/1/719806127.pdf (letzter Zugriff am 12.07.2014)

Klotz 2007a: Klotz, M.: IT-Compliance – auf den Kern reduziert. In: IT-Governance, Jg. 1 (2007), Heft 1, S. 14-18

Klotz 2007b: Klotz, M.: Basel II als Treiber des IT-Sicherheitsmanagements – Eine Klarstellung. In: HMD Praxis der Wirtschaftsinformatik, Jg. 44 (2007), Nr. 256, S. 93-104

Klotz 2008: Klotz, M.: IT-Governance genormt – die neue ISO/IEC 38500 In: IT-Governance, Jg. 2 (2008), Heft 4, S. 21-22

Klotz 2009: Klotz, Michael: IT-Compliance – Ein Überblick. dpunkt, Heidelberg 2009

Klotz 2012: Klotz, M.: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. 2. Aufl. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, Jg. 4 (2012), Nr. 20, online unter: http://www.econstor.eu/bitstream/10419/65374/1/726885614.pdf (letzter Zugriff am 12.07.2014)

Klotz 2013a: Klotz, M.: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, Jg. 5 (2013), Nr. 24, online unter : https://www.econstor.eu/dspace/bitstream/10419/88419/1/773961380.pdf (letzter Zugriff am 12.07.2014)

Klotz 2013b: Klotz, M.: IT-Compliance. In: Tiemeyer E. (Hg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 5. Aufl., Hanser, München 2013, S. 707-763

Klotz 2013c: IT-Compliance nach COBIT – Vergleich zwischen COBIT 4.0 und COBIT 5. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, Jg. 6 (2014), Nr. 25, online unter: http://www.econstor.eu/bitstream/10419/90163/1/775982954.pdf (letzter Zugriff am 12.07.2014)

Klotz/Dorn 2005: Klotz, M.; Dorn, D.-W. :Controlling von IV-Beschaffungsverträgen - Bedeutung, Ziele und Aufgaben. HMD Praxis der Wirtschaftsinformatik, Jg. 42 (2005), Nr. 241, S. 97-106

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

LG Berlin 2002: Landgericht Berlin Urteil vom 03.07.2002 (Az. 2 O 358/01), zitiert nach juris: http://www.juris.de/jportal/portal/t/ou2/page/jurisw.psml?doc.hl=1&doc.id=KORE558562002&documentnumber=1&numberofresults=2&showdoccase=1&doc.part=K&paramfromHL=true#focuspoint (letzter Zugriff: 12.07.2014)

Lufthansa 2014: Lufthansa AG (Hg.): Corporate Governance & Compliance, online unter: http://www.lufthansagroup.com/de/verantwortung/wirtschaftliche-nachhaltigkeit/corporate-governance-compliance.html (letzter Zugriff am 12.07.2014)

Meyer/Zarnekow/Kolbe 2003: Meyer, M.; Zarnekow R.; Kolbe, L.: IT Governance – Begriff, Status quo und Bedeutung. In: Wirtschaftsinformatik, Jg. 44 (2003), Nr. 4, S. 445-448

Noerr/Denton 2011: Noerr/Denton (Hg.): Der USA PATRIOT Act – Implikationen für das Cloud Computing, Noerr LLP, SNR Denton US LLP, 2011

OECD 2004: Organisation for Economic Co-operation and Development (OECD) (Hg.): OECD-Grundsätze der Corporate Governance, online unter: http://www.oecd.org/daf/ca/corporategovernanceprinciples/32159487.pdf (letzter Zugriff am 12.07.2014)

Peltier 2004: Peltier, T. R.: Information security policies and procedures: a practitioner´s reference. 2nd ed. Auerbach, Boca Raton u. a. 2004
Picot/Dietl/Franck 2008: Picot, A.; Dietl, H.; Franck, E.: Organisation – Eine ökonomische Perspektive. 5. Aufl. Schäffer-Poeschel, Stuttgart 2008
Pietsch/Martiny/Klotz 2004: Pietsch, T.; Martiny, L.; Klotz, M.: Strategisches Informationsmanagement – Bedeutung, Konzeption und Umsetzung. Erich Schmidt, Berlin 2004
Rath/Sponholz 2009: Rath, M.; Sponholz, R.: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen. Erich Schmidt, Berlin 2009
Redeker 2012: Redeker, H.: IT-Recht. 5. Aufl. Beck, München 2012
Schmidl 2009: Schmidl, M.: Recht der IT-Sicherheit. In: Hauschka, C. (Hg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 2. Aufl., Beck, München, 2009, S. 701-807
Siemens 2014: Siemens AG (Hg.): Corporate Governance, online unter: http://www.siemens.com/investor/de/corporate_governance.htm (letzter Zugriff am 12.07.2014)
Steckler 2007: Steckler, B.: Grundzüge des IT-Rechts: Das Recht der Datenverarbeitung und der Online-Dienste. 3. Aufl. Vahlen, München 2007
Stiglbauer 2010: Stiglbauer, M.: Corporate Governance: Führung und Kontrolle im InsiderSystem. Ventus Publishing ApS, Frederiksberg 2010
The Committee 1992: The Committee on the Financial Aspects of Corporate Governance (Hg.): Report of the Committee on the Financial Aspects of Corporate Governance, online unter: http://www.ecgi.org/codes/documents/cadbury.pdf (letzter Zugriff am 12.07.2014)
van Grembergen 2002: van Grembergen, W.: Introduction to the Minitrack "IT Governance and its Mechanisms". Proceedings of the 35th Hawaii International Conference on System Sciences 2002, online unter: http://www.computer.org/csdl/proceedings/hicss/2002/1435/08/14350240.pdf (letzter Zugriff am 12.07.2014)
VOI 2008: Verband Organisations- und Informationssysteme e. V. (VOI): Standards und Normen im Umfeld ECM – Leitfaden für organisatorische und technische Anforderungen. VOI Berlin 2008
Weill/Woodham 2002: Weill, P.; Woodham, R.: Don't Just Lead, Govern: Implementing Effective IT Governance, CISR WP No. 326, Massachusetts Institute of technology, Cambridge, April 2002, online unter: http://dspace.mit.edu/bitstream/handle/1721.1/1846/4237-02.pdf?sequence=2 (letzter Zugriff am 12.07.2014)
Welge/Eulerich 2012: Welge, M. K.; Eulerich, M.: Corporate-Governance-Management: Theorie und Praxis der guten Unternehmensführung. Gabler, Wiesbaden 2012

Das Stralsund Information Management Team (SIMAT)

Das von Prof. Dr. Michael Klotz geleitete „Stralsund Information Management Team“ (SIMAT) ist am Fachbereich Wirtschaft der FH Stralsund angesiedelt. Es bündelt akademische Lehre und Forschung, Weiterbildungsangebote und Projekte im Themenbereich des betrieblichen Informationsmanagements. Informationsmanagement richtet sich auf die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens. Diese Zielsetzung wird heute von verschiedenen spezialisierten Fachrichtungen in der Informatik, der Wirtschaftsinformatik und der Betriebswirtschaftslehre verfolgt. Das SIMAT arbeitet insofern interdisziplinär, wobei die inhaltlichen Schwerpunkte in Kompetenzzentren (Competence Center) fokussiert werden. Im Rahmen des RD&D-Ansatzes (Research, Development and Demonstration) dienen Labore, die mit aktuellen Tools des Informationsmanagements ausgestattet sind, sowohl der fachlichen Arbeit als auch zu Demonstrationszwecken. Eine intensive Kooperation mit ausgewiesenen Expertinnen und Experten sowie mit privatwirtschaftlichen Unternehmen und die Mitarbeit in anwendungsnahen Fachorganisationen gewährleisten eine praxis- und lösungsorientierte Vorgehensweise. Die Zusammenarbeit mit Lehrstühlen anderer Hochschulen, wissenschaftlichen Einrichtungen und eine umfangreiche Publikationstätigkeit stellen sicher, dass sich das SIMAT am State-of-the-Art des Informationsmanagements orientiert und diesen mitprägt. Auf diese Weise sind die Mitarbeiterinnen und Mitarbeiter des SIMAT in der Lage, anspruchsvolle Konzepte und Lösungen zu konzipieren und zu realisieren.

Das SIMAT versteht sich als Mittler zwischen akademischer Forschung und Lehre auf der einen, und der Wirtschaftspraxis auf der anderen Seite. Diese Transferaufgabe, verankert im Landeshochschulgesetz Mecklenburg-Vorpommerns, bildet den Schwerpunkt der Arbeit des SIMAT. Forschung und Lehre werden nicht als Selbstzweck begriffen, sondern führen zu handlungsrelevanten, innovativen Konzepten und Lösungen, die in die Unternehmenspraxis transferiert werden. Die berufliche Weiterbildung bildet hierbei ein wesentliches Element.

Die anwendungsnahe Forschung am SIMAT ist auf eine ökonomische Verwertung hin orientiert. Es sollen Innovationen entwickelt und in Kooperation mit anderen wissenschaftlichen Einrichtungen, Fach-Institutionen und Unternehmen in eine nachhaltige und profitable Praxis umgesetzt werden. Hierzu werden eigene F&E-Projekte auf dem Gebiet des Informationsmanagements und Innovationsprojekte mit Partnern durchgeführt. Zudem hat sich das SIMAT auf die betriebswirtschaftliche Begleitberatung bei IT-nahen Technologieprojekten spezialisiert. Studierenden und wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wird die Möglichkeit eröffnet, an

der Lösung praktischer Problemstellungen zu arbeiten und sich so optimal auf das spätere Berufsleben vorzubereiten.

Die studentischen Mitarbeiterinnen und Mitarbeiter erhalten im SIMAT Einblick in die Arbeitsmethodik sowohl auf wissenschaftlichem als auch auf wirtschaftlichem Gebiet. Aus den Projekten des SIMAT entstehen zahlreiche Abschlussarbeiten, die den Studierenden der FH Stralsund offen stehen. Das SIMAT bietet zudem eine berufliche Perspektive für Studierende, die sich als wissenschaftliche Mitarbeiter in der anwendungsnahen Forschung qualifizieren wollen.

Das SIMAT beteiligt sich zudem an der Diskussion der wissenschaftlichen Gemeinschaft. Hierzu werden regelmäßig Arbeitspapiere veröffentlicht, die den Stand der Arbeit des SIMAT in die Öffentlichkeit tragen und zur Diskussion anregen sollen. Das SIMAT lädt zudem andere Wissenschaftler, aber auch Referenten aus der Praxis als Vortragende ein. Auf diese Weise lernen die SIMAT-Mitarbeiterinnen und -Mitarbeiter sowie andere interessierte Studierende aktuelle Forschungsergebnisse und praktische Fragestellungen aus erster Hand kennen. Erkenntnisse aus diesen Aktivitäten sowie aus den verschiedenen F&E-Projekten werden systematisch in die Lehre überführt, so dass alle Studierenden von der Forschungsarbeit des SIMAT profitieren können.

Zum Zwecke des ökonomischen Transfers verfolgt das SIMAT den RD&D-Ansatz (Research, Development and Demonstration). Hierzu werden Labore als Demonstrationsbereiche unterhalten. In den Laboren werden Produkte und Lösungen von Kooperationspartnern des SIMAT in den Bereichen des Informations-, Projekt- und Prozessmanagements betrieben. Auf dieser technischen Grundlage werden im Rahmen von Projekten durch das SIMAT-Team prototypische Lösungen erarbeitet.

Kontakt

FH Stralsund • SIMAT • Zur Schwedenschanze 15 • 18435 Stralsund
Ansprechpartner: Prof. Dr. Michael Klotz (Wissenschaftlicher Leiter)
☎ +49 (0)3831 45-6946
✉ michael.klotz@fh-stralsund.de
www.simat-stralsund.de

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop-Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Karminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informations-managements
03-11-013	08.2011	H. Auerbach/ N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesundheitswirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutschsprachiger Museums-Apps
03-11-016	11.2011	S. J. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Mecklenburg-Vorpommern – Strom als Wettbewerbsfaktor und Gegenstand der Standortvermarktung
04-12-017	02.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagement-software – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.

04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	02.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen
06-14-025	01.2014	M. Klotz	IT-Compliance nach COBIT® – Gegenüberstellung von COBIT® 4.0 und COBIT® 5
06-14-026	04.2014	L. von Blumröder	Projektpriorisierung im Rahmen eines ganzheitlichen Projektportfoliomanagements
06-14-027	06.2014	S. Press	Automatisierte Kontrollen in der Beschaffung – Exemplarische Konzeption und Umsetzung
06-14-028	07.2014	M. Klotz	IT-Compliance – Begrifflichkeit und Grundlagen