Klotz, Michael

Working Paper

ISO/IEC 3850x - Die Normenreihe zur IT-Governance

SIMAT Arbeitspapiere, No. 08-16-030

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

Suggested Citation: Klotz, Michael (2016) : ISO/IEC 3850x - Die Normenreihe zur IT-Governance, SIMAT Arbeitspapiere, No. 08-16-030, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund

This Version is available at:
https://hdl.handle.net/10419/144834

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 08-16-030

ISO/IEC 3850x – Die Normenreihe zur IT-Governance

Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

August 2016

ISSN 1868-064X

Klotz, Michael: ISO/IEC 3850x – Die Normenreihe zur IT-Governance. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2016 (SIMAT AP, 8 (2016), 29), ISSN 1868-064X

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
dokuteam-x
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“.

ISO/IEC 3850x – Die Normenreihe zur IT-Governance

Prof. Dr. Michael Klotz[1]

Zusammenfassung: In diesem Arbeitspapier wird die Norm „ISO/IEC 38500“ beschrieben und analysiert. Die erste Ausgabe der Norm wurde im Juni 2008 als "ISO/IEC 38500:2008 Corporate governance of information technology“ veröffentlicht. Die zweite Ausgabe folgte im Februar 2015 als „ISO/IEC 38500:2015 Information technology – Governance of IT for the organization“. Im Folgenden wird auf die institutionellen Hintergründe, die wesentlichen Bestandteile der ISO/IEC 38500:2015, das grundlegende Modell und die Prinzipien zur IT-Governance sowie auf die aus der Verbindung von Prinzipien und Governance-Funktionen resultierenden Leitlinien zur Ausgestaltung der IT-Governance eingegangen. Auch werden die Entwicklung zur Normenreihe und die Zusammenhänge der einzelnen Dokumente dieser Reihe verdeutlicht. Die Bedeutung der ISO/IEC 38500: 2015 wird vor allem in der Trennung zwischen IT-Governance und IT-Management sowie dem damit verbundenen Modell der IT-Governance gesehen. Dieses Modell hat die drei Governance-Funktionen „Evaluate – Direct – Monitor“ eingeführt, die auch in COBIT® 5 Eingang gefunden haben. Neben der ISO/IEC 38500:2015 werden auch die technische Spezifikation „ISO/IEC TS 38501:2015“ und der technische Report „ISO/IEC TR 38502:2014“ behandelt. Die ISO/IEC TS 38501:2015 beschreibt als Implementierungsleitfaden einen zyklischen Implementierungsansatz mit drei Phasen, die jeweils detailliert dargestellt werden. Der ISO/IEC TR 38502:2014 beinhaltet im Wesentlichen die in die ISO/IEC 38500:2015 weitgehend identisch übernommenen Begriffsdefinitionen sowie das Modell der IT-Governance. Daneben werden Vertiefungen zur Unterscheidung zwischen Governance und Management sowie ein Framework für die IT-Governance behandelt. Im Vergleich der verschiedenen Dokumente (Norm, Report, Spezifikation) sind Unstimmigkeiten i. S. einer mangelnden Bezugnahme zu entdecken. Insbesondere die in der ISO/IEC 38500:2015 etablierte Struktur der Verbindung von Governance-Funktionen mit Prinzipien der IT-Governance wird im Report und in der Spezifikation nicht weiter als Analyse- und Bewertungsraster verwendet. Trotzdem stellen die Norm und die ergänzenden Dokumente ein Hilfsmittel für die Praxis in der Ausgestaltung und ständigen Verbesserung

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

der IT-Governance dar. Standards zur Steuerung und Überwachung der Unternehmens-IT, allen voran COBIT®, werden in ihrer Weiterentwicklung die ISO/IEC 3850x berücksichtigen müssen.

Gliederung

Schlüsselwörter: COBIT® 5 – Corporate Governance – DIN – IEC – ISO – ISO/IEC 38500 – IT – IT-Governance – IT-Management – Norm – Unternehmen

JEL-Klassifikation: L21, L22, M10, M14, M21

Vorwort

Normung auf dem Gebiet des Managements spielt auch in der IT mittlerweile eine große Rolle. Auf internationaler Ebene kommt den beiden Normungsorganisationen ISO und IEC hier eine wichtige Rolle zu. Man denke nur an die Normenreihe ISO/IEC 270xx zur Informationssicherheit oder die Norm ISO/ IEC 20000-x zum IT-Servicemanagement. Dass der Bereich der IT-Governance ebenso Gegenstand der Normung – und zwar bereits 2008 – war, verwundert insofern nicht. Dennoch hat die ISO/IEC 38500:2008 sowohl in der Fachdiskussion als auch in der praktischen Anwendung bisher keine ähnliche Bedeutung erlangt, wie andere IT-Normen bzw. -Normenreihen. Die Gründe dafür mögen vielfältig sein. Dennoch hatte die ISO/IEC 38500:2008 eine nicht unbeträchtliche Ausstrahlung, ging doch die in der Norm enthaltene grundlegende Unterscheidung zwischen IT-Governance und IT-Management vor allem in das Framework COBIT® 5 und über diesen Weg dann eben indirekt doch in die Arbeit der IT-Verantwortlichen ein. Grund genug, mit der zweiten Ausgabe der Norm, der ISO/IEC 38500:2015, einen Blick auf die Weiterentwicklung der Norm selbst, aber auch auf ergänzende Normen sowie technische Reports und Spezifikationen – und damit den Weg von der Norm ISO/IEC 38500 zur Normenreihe ISO/IEC 3850x – zu werfen.

Prof. Dr. Michael Klotz

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AS	Australian Standard
AWI	Approved work item
CD	Committee draft
CMS	Compliance-Managementsystem
COBIT®	Control Objectives for Information and Related Technology
DIN	Deutsches Institut für Normung e. V.
DIS	Draft International Standard
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
e. V.	eingetragener Verein
FDIS	Final Draft International Standard
GEIT	Governance of Enterprise IT
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnik
ISACA	Information Systems Audit and Control Association
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
ISO/IEC JTC1	ISO/IEC Joint Technical Committee 1
IT	Informationstechnik / Informationstechnologie
ITGI	IT Governance Institute
ITSM	IT-Servicemanagementsystem
ITIL®	IT Infrastructure Library®
NIA	Normenausschuss Informationstechnik und Anwendungen
OECD	Organisation for Economic Co-operation and Development
PD	Proposed Draft
PRF	Proof
RMS	Risikomanagementsystem
SC	Sub Committee
TC	Technical Committee
TR	Technical Report
USA	United States of America
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VW	Volkswagen
WD	Working draft

1 Einleitung

Die "ISO/IEC 38500:2008 Corporate governance of information technology“ wurde im Juni 2008 veröffentlicht. Die Norm resultierte seinerzeit aus der im Januar 2005 veröffentlichten australischen Norm „AS8015:2005 Corporate governance of information and communication technology“[2], die im sog. „Fast-track“-Verfahren[3] übernommen wurde.[4]

Verbreitung in der Praxis

In der dem „Global Status Report on the Governance of Enterprise IT (GEIT) – 2011” der Information Systems Audit and Control Association (ISACA) zugrunde liegenden Umfrage antworteten 8,2 % der Befragten, dass die ISO/IEC 38500 in ihrem Unternehmen als externes Framework für die Gestaltung der IT-Governance verwendet wird. Damit lag die ISO/IEC 38500 zwar weit hinter den führenden Standards ITIL®[5] bzw. ISO/IEC 20000 (28 %) und ISO/IEC 27000 (21,1 %), aber selbst COBIT®[6] kam damals auf lediglich 12,9 %.[7] Für eine Norm, die zu diesem Zeitpunkt erst ca. drei Jahre „auf dem Markt war“, konnte dies als eine bis dahin erfolgreiche Verbreitung und Anwendung betrachtet werden.

Verbreitung im Schrifttum

Nach ihrer Publikation fand die ISO/IEC 38500 Eingang in die Fachdiskussion und entsprechende Publikationen.[8] Schon bald zählte sie zum Kanon der relevanten Frameworks für IT-Governance[9]. Auch im öffentlichen

---

[2] Zur Entstehung des AS8015:2005 siehe *da Cruz 2007*, S. 138f.

[3] Mittels des „Fast-track“-Verfahrens soll es ermöglicht werden, bestehende Normen außerhalb der ISO, also beispielsweise nationale Normen, innerhalb eines kurzen Zeitraums von ca. sechs Monaten als ISO-Norm verabschieden zu können. In diesen Fällen startet das Verfahren sofort mit der Prüfungsphase. Insbesondere das ISO/IEC JTC 1 sieht die Möglichkeit dieses „Fast-track“-Verfahrens für seine Normungsarbeit vor (vgl. *ISO/IEC 2015*, S. 78ff.).

[4] Dafür, dass – wie in *Lang/Wimmer 2014* ohne weitere Begründung behauptet wird – die ISO/IEC 38500:2008 auf dem Governance-Framework von *WEIL/ROSS* aus dem Jahre 2008 basiert (vgl. *Lang/Wimmer 2014*, S. 18), lassen sich Belege bzw. Bezüge weder in den von der Norm angegeben Referenzen (vgl. *ISO/IEC 38500:2008*, S. 3), noch im Text (insb. in den Beschreibungen des IT-Governance-Modells und der Prinzipien) finden. Auch die zeitliche Abfolge spricht gegen diese Auffassung, stammt die AS8015:2005 Corporate governance of information and communication technology“ doch bereits aus dem Jahr 2005.

[5] ITIL® is a registered trademark of AXELOS Limited. IT Infrastructure Library® is a registered trademark of AXELOS Limited.

[6] COBIT® is a registered trademark of ISACA.

[7] Nach *ITGI 2011*, S. 29.

[8] Vgl. z. B. *Calder 2008, Klotz 2008*; *Böhm/Goeken/Johannsen 2009*, S. 10; *Quack 2009*; *Rath/Sponholz 2009*, S. 29; *Strecker 2009*, S. 8; *Racz/ Weippl/Seufert 2010*; *Ayat/Masrom/ Sahibuddin 2011*, *Rath/Sponholz 2014*, S. 31ff.; *Gaulke 2014*, S. 180ff.; *Ahuja/Chan 2015*.

[9] Vgl. z. B. *Huber 2009*, S. 211ff.; *Johannsen/Goeken 2011*, S. 189ff.; *Klotz 2013*, S. 41f.; *Knolmayer/Aspirion 2014*.

Bereich erfuhr die ISO/IEC 38500 Berücksichtigung.[10] Mitunter wurde aber auch nur darauf verwiesen, dass die ISO/IEC 38500 Eingang in COBIT® gefunden habe.[11]

Künftige Bedeutung

Dass die Norm bis heute nicht in einem Zuge mit der ISO/IEC 27000 oder der ISO/IEC 20000 genannt wird, mag daran liegen, dass sie als „high level"-Norm nicht unmittelbar handlungsorientiert[12] ist und es für sie auch keine Zertifizierungsmöglichkeit gibt. Dieses mag sich aber in Zukunft ändern, wenn die ISO/IEC 38500 nach ihrer Überarbeitung in 2015 durch weitere Normen und technische Reports ergänzt wird, so dass letztlich eine neue Normenreihe entsteht. Der Bedarf an praxistauglichen Konzepten und Modellen für die Gestaltung der IT-Governance wird sicherlich nicht geringer. Die Steuerung und Überwachung der Unternehmens-IT muss – nicht zuletzt durch den 2015 publik gewordenen VW-Skandal um eine die Pkw-Abgaswerte manipulierende Software – auf der obersten Etage der Unternehmenshierarchie thematisiert werden. Die Orientierung an weltweit eingesetzten und bewährten Normen kann nicht nur die Analyse- und Konzeptionsphase unterstützen, sondern dokumentiert auch die Erfüllung von Sorgfaltspflichten in diesem Verantwortungsbereich.

2 Institutioneller Hintergrund

Der institutionelle Hintergrund der ISO/IEC 38500:2015 wird durch verschiedene Organisationen gebildet, allen voran die International Standardization Organization (ISO) und die International Electrotechnical Commission (IEC).

ISO / DIN

- Die ISO mit Sitz in Genf ist eine 1947 gegründete, private Organisation. Mitglieder der ISO sind nationale Normungsorganisationen, derzeit 163.[13] Das Deutschland vertretende Mitglied ist das Deutsche Institut für Normung e. V. (DIN).

IEC / DKE

- Die IEC, Genf, ist eine 1906 gegründete Organisation in den Bereichen Elektrotechnik und Elektronik. Die Mitglieder sind so genannte nationale Komitees. Für Deutschland ist dies die Deutsche Kommission

[10] Vgl. z. B. *Bundesrechnungshof 2001*, Anhang, S. 4; *Schwertsik 2013*, S. 56ff.,
[11] Vgl. z. B. *Konrad/Puchnan/Gann 2012*, S. 11.
[12] So spricht GAULKE von einem „hohen Abstraktionsgrad", vgl. *Gaulke 2014*, S. 180.
[13] Zahlenangabe nach *ISO 2016a*.

Elektrotechnik Elektronik Informationstechnik im DIN und VDE (DKE).[14]

ISO/IEC JTC 1

Für die Normungsarbeit im Bereich der Informationstechnologie unterhalten ISO und IEC seit 1987 ein gemeinsames Gremium, das „ISO/IEC Joint Technical Committee 1“ (JTC 1). Dieser Einrichtung gehören derzeit 32 Länder an (unter ihnen Deutschland), weitere 63 Ländern sind „observing countries“, d. h. sie haben einen Beobachtungsstatus.[15] Aus der Arbeit des JTC 1 resultierende Normen erhalten eine ISO/IEC-Kennung, so wie dies auch bei der ISO/IEC 38500 der Fall ist.

SC 40

Verantwortlich für die Norm ISO/IEC 38500:2015 zeichnet im „ISO/IEC JTC 1“ der 2013 eingerichtete Unterausschuss „SC 40 IT Service Management and IT Governance“.[16] Allein die Bildung dieses Unterausschusses sowie die explizite Nennung des Begriffs „IT-Governance“ in der Bezeichnung des Unterausschusses demonstriert die gesteigerte Bedeutung von IT-Governance in der Normungsarbeit von ISO/IEC. Zudem ist innerhalb des Unterausschusses eine spezielle Arbeitsgruppe „Governance of information technology“ eingerichtet.

Australische Akteure

Stand der 2008 noch zuständige Unterausschuss „SC 7 Software and Systems Engineering“ unter der Leitung von Professor Dr. François Coallier, Universität Québec,[17] so waren auch bei der Überarbeitung der Norm australische Akteure führend. Dies zeigt sich vor allem darin, dass das Sekretariat des Unterausschusses SC 40 von der australischen Normungsorganisation „Standards Australia“ gestellt und dementsprechend der Vorsitz des Unterausschuss von einem der Chief Technology Officer der australischen Regierung, John Sheridan, ausgeübt wird.[18]

Rechtzeitiges Review

Da ISO-Normen üblicherweise nach Ablauf von fünf Jahren nach ihrer Verabschiedung einem Review unterliegen und die Überarbeitung der ISO/IEC 38500:2008 bei einer Beteiligung von Mitgliedern aus 28 Nationen zwei Jahre in Anspruch nahm,[19] kann die zweite Ausgabe in 2015 als plangemäß bezeichnet werden. Nach ihrer Veröffentlichung befindet sich die Norm im ISO nun im Stage code 60.60, der für „International Standard

[14] Vgl. *IEC 2016*.
[15] Vgl. *ISO 2016b*, Stand der Zahlenangabe: 04.07.2016.
[16] Vgl. *ISO 2016c*, Stand der Zahlenangabe: 04.07.2016,
[17] Vgl. *ISO 2008*.
[18] Vgl. *ISO 2016c*.
[19] Vgl. *Standards Australia 2015*.

published“ steht.[20]

DIN – NIA

In der internationalen Normungsarbeit stellt der „Normenausschuss Informationstechnik und Anwendungen“ (NIA) des DIN Deutsches Institut für Normung e. V. das deutsche Spiegelgremium zur ISO/IEC JTC 1 dar. Der NIA agiert als nationales Gremium für die Normung in der Informationstechnik und in ausgewählten Anwendungsbereichen der Informationstechnik.[21] In seinem Jahresbericht für das Jahr 2015 verweist der NIA auf seine intensive Teilnahme an der Ausarbeitung verschiedener internationaler Dokumente und das Einbringen der deutschen Expertenmeinung in die Arbeit des ISO/IEC JTC 1/SC 40. Als eines dieser Dokumente listet der NIA auch die ISO/IEC 38500 auf.[22]

3 Entwicklung zur Normenreihe

Titel der Norm

Im Vergleich zum Titel der ersten Ausgabe der Norm fällt ins Auge, dass die ISO/IEC 38500:2015 nunmehr den erweiterten Titel „Information technology – Governance of IT for the organization“ trägt. Mit der Erweiterung um das Sachgebiet „Information technology“ wird die Eingliederung der Norm in die Normen des JTC 1, speziell des Unterausschusses SC 40, dokumentiert. Damit weist der Titel jetzt die gleiche Struktur auf wie beispielsweise die Normenreihen ISO/IEC 270xx und ISO/IEC 20000-x. Hiermit wird gleichzeitig die Grundlage gelegt für die Erweiterung zur Normenfamilie.

Neben die eigentliche Norm „ISO/IEC 38500:2015“ treten nunmehr ein Implementierungsleitfaden als technische Spezifikation, die ISO/IEC TS 38501:2015, und detaillierte Beschreibungen des in der ISO/IEC 38500 verwendeten Frameworks und Modells für IT-Governance im Rahmen des bereits Anfang 2014 erschienenen technischen Reports ISO/IEC TR 38502: 2014, siehe Tabelle 1.[23]

---

[20] Vgl. *ISO 2016d*.
[21] Vgl. *Klotz 2013*, S. 12.
[22] Vgl. *DIN/NIA 2015*, S. 65.
[23] Die ISO/IEC 38500:2008 umfasst insgesamt 15 Seiten. Dass sich die zweite Ausgabe der Norm über nurmehr 12 Seiten erstreckt, ist dem im Vergleich der beiden Ausgaben kompakteren Layout zuzuschreiben, das an das übliche Standardlayout der ISO-Normen angepasst wurde. Hinsichtlich der Textmenge ist die ISO/IEC 38500:2015 sogar etwas umfangreicher als die ISO/IEC 38500:2008.

Tabelle 1
Die Normenreihe ISO/IEC 3850x

Nr.	Dokument	Titel	Art	Status[1] (stage)	Status-Datum	Umfang[2]
1	ISO/IEC 38500	Information technology – Governance of IT for the organization	Norm	60.60	15.02. 2015	12
2	ISO/IEC TS 38501	Information technology – Governance of IT – Implementation guide	Technische Spezifikation	60.60	01.04. 2015	15
3	ISO/IEC TR 38502	Information technology – Governance of IT – Framework and model	Technischer Report	60.60	01.02. 2014	14
4	ISO/IEC PDTR 38503	Information technology – Governance of IT – Assessment of the governance of IT	Technischer Report	30.92	30.10. 2015	k. A.
5	ISO/IEC PRF TR 38504	Information technology – The structure of principles-based standards in the governance of IT	Technischer Report	50.00	23.06. 2016	k. A.
6	ISO/IEC DIS 38505-1	Information Technology – Governance of IT – Part 1: The application of ISO/ IEC 38500 to the governance of data	Norm	40.00	30.05. 2016	19
7	ISO/IEC WD TR 38505-2	Information Technology – Governance of IT – Part 2: Implications of 38505-1 for data management	Technischer Report	20.20	22.04. 2016	k. A.
8	ISO/IEC AWI 38506	Information technology – Governance of IT – Governance of IT enabled investments	Norm	20.00	07.06. 2016	k. A.

[1] 20.00 = New project registered in TC/SC work programme; 20.20 = Working draft (WD) study initiated; 30.92 = Committee draft (CD) referred back to Working Group; 40.00 = Draft International Standard (DIS) registered; 50.00 = Final text received or Final Draft International Standard (FDIS) registered for formal approval; 60.60 = International Standard published;
[2] Angabe in Seiten
Stand aller Angaben: 29.06.2016

- Die Norm „ISO 38500:2015“ beinhaltet in fünf Abschnitten Ausführungen zum Anwendungsbereich, zu Begriffsdefinitionen und zum Nutzen von IT-Governance. Den Kern der Norm bilden ein Überblick zu den Prinzipien und dem Modell der IT-Governance sowie eine detailliertere Beschreibung der sechs Prinzipien der IT-Governance, indem diese auf die Governance-Funktionen bezogen werden.[24] ISO/IEC 38500:2015

- Die technische Spezifikation „ISO/IEC TS 38501:2015“ umfasst in sechs Abschnitten Ausführungen zum Anwendungsbereich und Verweisungen zu den beiden anderen Normen der Normenreihe. Im Sinne eines Implementierungsleitfadens verfolgt die Spezifikation einen zyklischen Implementierungsansatz mit drei Phasen, die jeweils detailliert beschrieben werden. Den Kern bildet hierbei die Darstellung der drei Hauptaufgaben des Governance-Modells der ISO/IEC 38550. Die Anhänge beinhalten ein allgemeines Bewertungsschema und beispielhafte Bewertungskriterien für die einzelnen Prinzipien der IT-Governance.[25] ISO/IEC TS 38501:2015

- Im technischen Report „ISO/IEC TR 38502:2014“ finden sich nach Ausführungen zum Anwendungsbereich insgesamt 28 aufeinander bezogene Begriffsdefinitionen, die die Begrifflichkeit der ISO/IEC 38550:2008 – auch im Sinne einer Konsistenz mit anderen Normen der ISO/IEC[26] – verbessern, vgl. die Beispiele in Abbildung 1. Die Definitionen des Reports wurden weitgehend in die ISO/IEC 38550:2015 übernommen. Es folgt die Darstellung des gegenüber der ISO/IEC 38550:2008 vor allem bezüglich der Trennung zwischen Governance und Management weiterentwickelten Modells der IT-Governance, das ebenfalls in die ISO/IEC 38550:2015 übernommen wurde. Dieses Modell wird ergänzt durch ein generisches IT-Governance-Framework. Ergänzend werden Empfehlungen für die Anwendung des IT-Governance-Modells gegeben, die sich auf die Verantwortlichkeit von Unternehmensleitung und weiterem Management, die Strategieformulierung, die Delegation von Verantwortlichkeiten und das interne Steuerungs- und Überwachungssystem richten. Der Anhang enthält die Prinzipien der IT-Governance entsprechend der ISO/IEC 38500:2008.[27] ISO/IEC TR 38502:2014

[24] Vgl. *ISO/IEC 38500:2015*.
[25] Vgl. *ISO/IEC TS 38501:2015*.
[26] So betont FISCHLIN die nunmehr bessere Übereinstimmung mit dem Management-Begriff der ISO 9000; vgl. *Fischlin 2015*.
[27] Vgl. *ISO/IEC TR 38502:2014*.

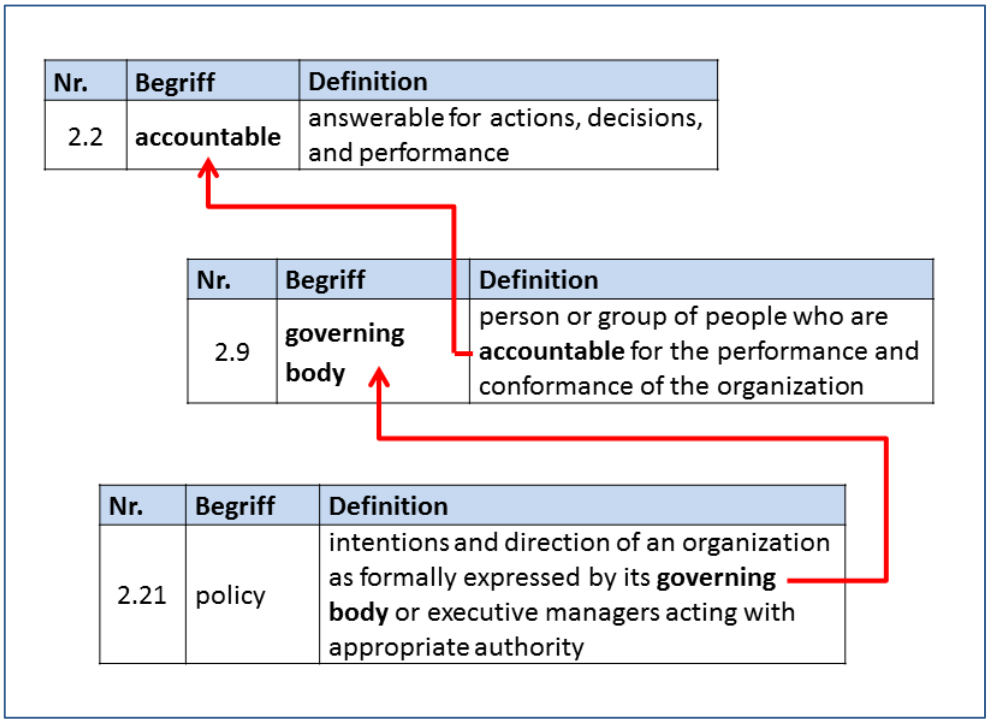

Abbildung 1
Zusammenhänge der Definitionen[28]

Hinzu kommen fünf weitere, im Entwicklungsprozess befindliche Dokumente, die meisten davon mit aktuellen Zwischenständen aus 2016:

Aktuelle Erweiterungen

- Der seit Oktober 2015 als Entwurfsvorschlag (Proposed Draft – PD) vorliegende technische Report ISO/IEC PDTR 38503 hat die Bewertung der IT-Governance zum Inhalt.

  ISO/IEC PDTR 38503

- Der unmittelbar vor der Publikationsphase befindliche technische Report ISO/IEC PRF TR 38504 befasst sich mit den Strukturen der Normen zu IT-Governance.

  ISO/IEC PRF TR 38504

- Eine Norm, mit der die Unterscheidung von Governance und Management auf die Ressource „Daten“ angewendet wird, befindet sich derzeit in der frühen Prüfungsphase. Seit Ende Mai 2016 liegt ein im Komitee abgestimmter Entwurf (Draft International Standard), die ISO/IEC DIS 38505-1, vor. Die Norm richtet sich auf Data Governance, während der zweite Teil, der derzeit als Arbeitsentwurf vorliegende technische Report ISO/IEC WD TR 38505-2, die Auswirkungen auf das Datenmanagement zum Thema hat.

  ISO/IEC DIS 38505-1 und ISO/IEC WD TR 38505-2

[28] Nach *ISO/IEC 38500:2015*, S. 1ff.; eigene Darstellung.

- Die ISO/IEC AWI 38506, die derzeit lediglich ein „Approved work item“ (AWI) darstellt, wird die Governance von IT-Investitionen behandeln.

ISO/IEC AWI 38506

4 Governance-Begriff der ISO/IEC 38500

Der in der ISO/IEC 38500 vertretene Begriff der (IT-)Governance beruht ausdrücklich zum einen auf dem Cadbury Report, zum anderen auf den Corporate-Governance-Grundsätzen der OECD[29], vgl. Abbildung 2.

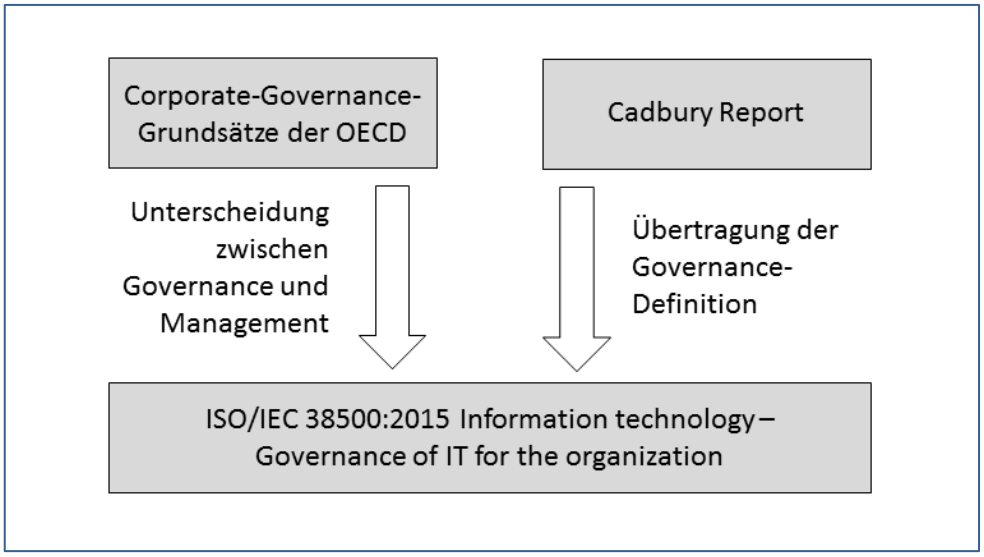

Abbildung 2
Quellen des Governance-Verständnisses der ISO/IEC 38500[30]

- Der gewöhnlich als “Cadbury Report” bezeichnete Bericht des im Mai 1991 von der Londoner Börse eingesetzten und nach dem Leiter des Komitees, Sir Adrian Cadbury, benannten Cadbury-Komitees (der offizielle Name lautete "The Committee on the Financial Aspects of Corporate Governance“) wurde im Dezember 1992 publiziert. Seine Empfehlungen zur Corporate Governance haben entsprechende Regularien weltweit, u. a. in den USA und Europa, maßgeblich beeinflusst. Insbesondere seine grundlegende Definition für Corporate Governance wird bis heute häufig zitiert: „Corporate governance is the system by which companies are directed and controlled“[31]. Dies wird von der ISO/IEC

Cadbury Report

[29] Vgl. *ISO/IEC 38500:2015*, S. V.
[30] Eigene Darstellung.
[31] *Committee on the Financial Aspects 2015*, S. 14.

38500 – teilweise wörtlich – überführt in ein Verständnis von IT-Governance als

> „governance of IT“ = “system by which the current and future use of IT is directed and controlled”[32].

- Aus den OECD-Grundsätzen zur Corporate Governance übernimmt die ISO/IEC 38500 die auf dem allgemeinen Konzept von Kontrolle und Gegenkontrolle beruhende Trennung zwischen Governance und Management.[33] Diese bildet in den OECD-Grundsätzen ein durchgängiges Prinzip, das sich in der Unterscheidung zwischen der von der Unternehmensleitung ausgeübten Managementfunktion einerseits und der diesbezüglichen Überwachung durch Aufsichtsgremium und Eigentümer andererseits ausprägt.

OECD-Grundsätze zur Corporate Governance

Bereits in der ersten Ausgabe der ISO/IEC 38500 wurde nicht der Begriff „IT-Governance“, sondern „Corporate governance of IT“ verwendet.[34] In der zweiten Ausgabe findet sich nunmehr der Begriff „Governance of IT“, unter dem die Begriffe „corporate“, „enterprise“ und „organizational governance of IT“ subsumiert werden.[35] Von STANDARDS AUSTRALIA wird die begriffliche Neufassung als eine wichtige Änderung angesehen, kommt doch darin nach Ansicht dieser Organisation die umfassende Anwendung der Norm zum Ausdruck.[36] Damit dürfte gemeint sein, dass die ISO/IEC 38500 nicht nur privatwirtschaftliche Umgebungen, sondern Organisationen aller Art adressiert – was allerdings bereits in der ersten Ausgabe der Norm ausdrücklich intendiert war.[37]

Begrifflichkeit

5 Zielgruppe und Anwendungsbereich

Die ISO/IEC 38500:2015 richtet sich an Stakeholder, die die Steuerung und Überwachung der Unternehmens-IT verantworten. Diese werden als „Go-

Zielgruppe

[32] *ISO/IEC 38500:2015*, S. 2.
[33] Vgl. *OECD 2004*, S. 12.
[34] *ISO/IEC 38500:2008*, S. 3.
[35] Vgl. *ISO/IEC 38500:2015*, S. 2.
[36] Nach *Standards Australia 2015*.
[37] Im Folgenden wird primär auf Unternehmen Bezug genommen, was aber den Geltungsbereich derAusführungen i. S. der Norm nicht einschränken soll.

verning body“ bezeichnet und stellen denjenigen Personenkreis dar, der formal die Unternehmensleistungen nach außen verantwortet[38], mithin Eigentümer, Einzelpersonen oder Mitglieder der Leitungsorgane (z. B. Geschäftsführung, Vorstand oder Aufsichtsrat). Welche Personen oder Gruppen im realen Einzelfall zum Governing body zählen, hängt somit insbesondere von der jeweiligen Struktur der Leitungsorgane (monistisches oder dualistisches Führungssystem) ab.[39]

Weiterhin richtet sich die Norm an diejenigen Stellen, die den Leitungsorganen[40] assistieren, ihnen prüfend oder beratend zur Seite stehen oder auf die im Rahmen der Delegation Verantwortung für spezielle Funktions- oder Aufgabenbereiche übertragen wird. Explizit genannt werden:

- das der Unternehmensleitung nachgelagerte Management,
- Auditoren, unternehmensexterne und -interne Berater bzw. Dienstleister,
- externe Spezialisten, z. B. in den Bereichen Recht oder Rechnungslegung.
- Experten von Wirtschaftsvereinigungen, Fachverbänden o. Ä.[41]

Die in der ersten Ausgabe der ISO/IEC 38500 noch aufgeführten Lieferanten von Hard- und Software, Kommunikationstechnik und sonstigen IT-Produkten werden in der ISO/IEC 38500:2015 nicht mehr adressiert, was im Hinblick auf notwendige strategische Partnerschaften bei IT-Outsourcing (zumindest wenn es in größerem Umfange betrieben wird) bzw. dem weiteren Vordringen der Inanspruchnahme von IT-Leistungen mittels Cloud Computing überrascht.

Anwendungsbereich

Für den Anwendungsbereich werden keinerlei Beschränkungen getroffen: Hinsichtlich der Unternehmensgröße gelten keine Einschränkungen, genauso wie für die Art der betreffenden Institution (Unternehmen, öffentliche

[38] Vgl. *ISO/IEC 38500:2015*, S. 2.
[39] Der Begriff „governing body“ wird in der ersten Ausgabe der ISO/IEC 38500 nicht verwendet; hier ist lediglich von „directors“ die Rede. Gerade hinsichtlich der für eine allgemeine Norm notwendigen Unabhängigkeit von den realen Ausprägungen der Organstrukturen einer Organisation stellt sich der Begriff „governing body“ als bessere Wahl dar.
[40] In den folgenden Ausführungen wird der Begriff der Leitungsorgane bzw. der Mitglieder des Leitungsorgans verwendet, wenn die Norm von „governing body“ spricht. Damit soll der Bezug auf die formale Verantwortung betont werden. In der Regel richten sich die Ausführungen jedoch an die Unternehmensleitung, weniger an einen Aufsichtsrat oder Inhaber (bspw. Aktionäre).
[41] Nach *ISO/IEC 38500:2015*, S. 1.

Verwaltung, Non-Profit-Organisation etc.). Ebenso wird kein spezifischer Unternehmensaufbau oder eine bestimmte Eigentümer- bzw. Organstruktur vorausgesetzt. Auch der Umfang des IT-Einsatzes spielt keine Rolle.[42] Weiterhin wird in der Norm klargestellt, dass IT-Governance eine Funktionsspezialisierung von Organizational bzw. Corporate Governance für IT-Belange darstellt.[43]

6 Zielsetzung der Norm

Zielsetzung

Die (gegenüber der ersten Ausgabe der Norm unveränderte) Zielsetzung der ISO/IEC 38500:2015 besteht darin, einen effektiven, effizienten und den Erwartungen der Stakeholder entsprechenden Einsatz der IT zu bewirken. Vor allem soll mit der Umsetzung der Norm das Vertrauen der Stakeholder in die Governance der IT gestärkt werden. Für die Unternehmensleitung soll die Norm als Anleitung dienen, damit diese ihrer Governance-Verantwortung für IT gerecht wird. Und schließlich soll mit der Norm ein Vokabular für IT-Governance etabliert werden.[44]

Nutzen von IT

Letztlich soll aus der Anwendung der Norm eine gute IT-Governance resultieren. Diese zeigt sich darin, dass die Nutzung von IT positiv zur Unternehmensleistung beiträgt, indem

- Geschäfts-, Markt- oder Serviceinnovationen ermöglicht werden;
- Business/IT-Alignment gewährleistet wird;
- IT-Systeme und -Komponenten adäquat implementiert und betrieben werden;
- Verantwortlichkeiten und Rechenschaftspflichten für IT-Angebot und IT-Nachfrage im Hinblick auf die Erreichung der Unternehmensziele geklärt sind;
- Nachhaltigkeit und Kontinuität der Geschäftstätigkeit sichergestellt werden;
- die IT-Ressourcen effizient eingesetzt werden;
- erfolgreiches Stakeholder-Management betrieben wird;
- der geplante Nutzen aus IT-Investitionen realisiert wird;

[42] Vgl. *ISO/IEC 38500:2015*, S. V, 1.
[43] Vgl. *ISO/IEC 38500:2015*, S. 1.
[44] Vgl. *ISO/IEC 38500:2015*, S. 1.

- Compliance mit gesetzlichen, regulativen und vertraglichen Vorgaben erreicht wird;
- aus Non-Compliance resultierende Haftungsrisiken für die verantwortlichen Führungskräfte vermieden werden.[45]

7 Prinzipien der IT-Governance

6 Prinzipien

Die beschriebene Zielsetzung bzw. der intendierte Nutzen von IT-Governance wird durch die Anwendung von sechs grundlegenden Prinzipien[46] erreicht, vgl. Tabelle 2.

Tabelle 2
Prinzipien der IT-Governance nach der ISO/IEC 38500:2015[47]

Nr.	Prinzip	Inhalt
1	Verantwortlichkeit (responsibility)	• Kenntnis und Akzeptanz der Verantwortlichkeiten für IT-Nachfrage und -Angebot • Verteilung verantwortungsadäquater Befugnisse
2	Strategie (strategy)	• Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung • Ausrichtung des IT-Einsatzes an der Unternehmensstrategie
3	Beschaffung (acquisition)	• Transparenz und Fundierung von IT-Beschaffungen • Kurz- und langfristige Ausgewogenheit von Nutzen und Kosten, Chancen und Risiken von IT-Beschaffungen
4	Performanz (performance)	• Verfügbarkeit von IT-Services entsprechend den aktuellen und künftigen Leistungs- und Qualitätsanforderungen der Geschäftsbereiche
5	Konformität (conformance)[48]	• Konformität der IT mit verpflichtenden gesetzlichen und regulativen Vorgaben • Definierte, implementierte und durchgesetzt Richtlinien und Verfahren
6	Verhalten (human behaviour)	• IT-Richtlinien, -Verfahren und -Entscheidungen berücksichtigen Verhaltensweisen sowie aktuelle und künftige Bedürfnisse aller Personen, die in die IT-Nutzung involviert sind

[45] Nach *ISO/IEC 38500:2015*, S. 4f.
[46] Gegenüber der ersten Ausgabe der Norm sind die Ausformulierungen der Prinzipien weitgehend wortwörtlich unverändert.
[47] Nach *Klotz 2008*, S. 21; *ISO/IEC 38500:2015*, S. 5f.
[48] Wie in der ersten Ausgabe ist in der ISO 38500:2015 weiterhin von „Conformance“ statt von „Compliance“ die Rede.

Diese Prinzipien beschreiben das „Was“, aber nicht das „Wie“. Es liegt in der Verantwortung der Unternehmensleitung, dass diese Prinzipien umgesetzt und befolgt werden.

Dass diese sechs Prinzipien als wichtiges, wenn nicht gar zentrales Element der ISO/IEC 38500:2015 angesehen werden, zeigt sich darin, dass die gesamte Norm als „principles-based advisory Standard“, der eine allgemeine Anleitung bieten soll, bezeichnet wird.[49]

8 Modell der IT-Governance

3 Governance-Funktionen

Neben den Prinzipien bietet die ISO 38500:2015 ein Modell für die IT-Governance, das vor allem auf einer Unterscheidung zwischen drei grundsätzlichen Governance-Funktionen (Direct, Monitor, Evaluate) und Management-Funktionen (die jedoch nicht weiter entfaltet werden) beruht. Die Verantwortung der Leitungsorgane des Unternehmens richtet sich auf die

- Bewertung des aktuellen und künftigen IT-Einsatzes (Evalate);
- Leitung der Erstellung und Umsetzung von IT-Richtlinien und -Strategien, mittels derer sichergestellt werden soll, dass der IT-Einsatz den Geschäftsanforderungen entspricht (Direct);
- Überwachung der Einhaltung von Richtlinien und der Leistung der IT hinsichtlich der festgelegten Strategien (Monitor).[50]

Bezug zu COBIT® 5

Die drei Governance-Funktionen sind als vielleicht wichtigster originärer Beitrag der ISO/IEC 38500 zu betrachten, hat diese Struktur doch Eingang in das führende IT-Governance und -Management-Framework „COBIT® 5“ gefunden. Diese Version von COBIT® wurde 2012 publiziert und führte die „Unterscheidung zwischen Governance und Management“ als eines der grundlegenden Prinzipien für die Governance und das Management der Unternehmens-IT ein. Der wesentliche Beweggrund wird darin gesehen, dass beide Disziplinen „mit unterschiedlichen Arten von Aktivitäten verbunden“ sind, unterschiedliche Organisationsstrukturen erfordern und unterschiedlichen Zwecken dienen.[51] Im Prozessreferenzmodell von COBIT® 5 wirkt sich die Anwendung des Prinzips in der Unterscheidung zwischen Go-

[49] *ISO/IEC 38500:2015*, S. V. Verstärkend kommt hinzu, dass sich die ISO/IEC PRF TR 38504 speziell auf diese Form von Standards richten wird.
[50] Nach *ISO/IEC 38500:2015*, S. 6.
[51] *ISACA 2012a*, S. 16.

vernance- und Managementprozessen aus. Mit ausdrücklicher und erkennbarer Anlehnung an die Konzepte der ISO/IEC 38500:2008 bestehen die Governance-Prozesse nach COBIT® 5 „aus Praktiken und Aktivitäten, die darauf ausgelegt sind, strategische Optionen zu evaluieren, die IT-Richtung vorzugeben (die IT zu steuern) und Ergebnisse zu überwachen“.[52] Auch COBIT® 5 verwendet für die Benennung der Governance-Domäne bzw. der zugehörigen IT-Prozesse die drei Begriffe „Evaluate, Direct, Monitor“ (abgekürzt „EDM“).[53]

Die Unterscheidung der beiden Ebenen und ihre Schnittstelle wird in der ISO38500:2015 graphisch wie in Abbildung 3 gezeigt dargestellt.[54] Die drei Governance-Funktionen beschreiben die Verantwortung des „Governing Body“ als zentralem Stakeholder.[55]

- Evaluate: Evaluate
  Die Bewertung des aktuellen und künftigen IT-Einsatzes richtet sich einerseits auf die Ergebnisse der Überwachung, andererseits auf die seitens der Management-Ebene erstellten und eingereichten Planungen und Vorschläge sowie interne und/oder externe Liefervereinbarungen. Um welche Planungen, Vorschläge[56] und Liefervereinbarungen es sich handelt, wird in der ISO/IEC 38500:2015 nicht näher beschrieben. Es ist jedoch evident, dass die Liefervereinbarungen i. S. von internen oder externen Service-Level-Agreements oder ähnlichen Servicevereinbarungen (insb. für Outsourcing-Dienstleistungen), die Pläne als generellere, auf die gesamte IT-Funktion bezogener Entwicklungsplan oder als

[52] *ISACA 2012b*, S. 25
[53] In der deutschen Übersetzung von „COBIT® 5 Enabling Processes“ werden die Begriffe „Evaluieren, Richtung vorgeben, Überwachen“ verwendet. Diese Begrifflichkeit wird hier übernommen.
[54] Gegenüber der ISO/IEC 38500:2008 ist das Modell in seiner Grundstruktur unverändert. Erweitert wurden die auf die Governance-Ebene wirkenden Einflussfaktoren um Erwartungen der Stakeholder, Compliance-Verpflichtungen und die Grundlage der Machtverteilung. Die Management-Ebene wurde in der der ISO/IEC 38500:2008 noch mittels der Geschäftsprozesse und den beiden IT-Bereichen der IKT-Projekte und des IKT-Betriebs dargestellt. In der ISO/IEC 38500:2015 wird diese Ebene nunmehr von den Führungskräften und den von ihnen verwendeten Managementsystemen repräsentiert. Dies korrespondiert besser mit der Governance-Ebene, die in der Abbildung die Mitglieder der Leitungsorgane beinhaltet.
[55] Im Folgenden nach *ISO/IEC 38500:2015*, S. 7f.
[56] Die in der ISO/IEC 38500:2015 enthaltene Abbildung zum Modell der IT-Governance enthält nur den Singular „Proposal“ (siehe *ISO/IEC 38500:2015*, S. 7), während in der entsprechenden Abbildung im ISO/IEC TR 38502 der Plural „Proposals“ verwendet wird (siehe *ISO/IEC TR 38502:2014*, S. 5). Da der Singular nicht als sinnvoll erscheint, handelt es sich offenbar um einen Übertragungsfehler.

IT-bezogene Einzelpläne (z. B. IT-Investitionsplan, IT-Projektportfolioplan, IT-Finanzplan, IT-Risikoplan, IT-Ressoucenplan) interpretiert werden können.

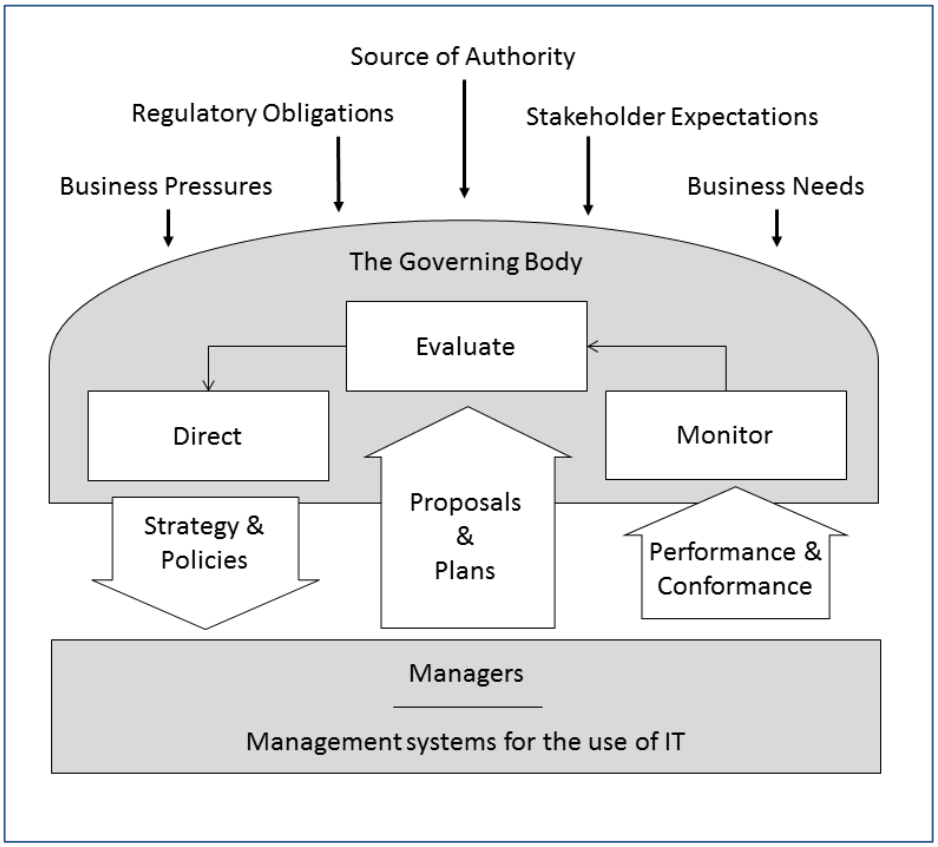

Abbildung 3
Modell der IT-Governance nach ISO/IEC 38500:2015[57]

Hinsichtlich der Vorschläge, die im Rahmen einer Governance geprüft, bewertet, genehmigt und in ihrer Umsetzung überwacht werden müssen, erweist sich ein Blick in COBIT® 5 als hilfreich. Dort ist beispielsweise von Vorschlägen für IT-Innovationen (APO 04.04), Investitionsvorschlägen (APO05.03), Vorschlägen zur Verbesserung der Lieferantenbeziehungen (APO10.03) oder Vorschlägen zur Reduzierung von Risiken (12.04) die Rede[58]. Im Rahmen der Bewertung sind einerseits Triebkräfte des Umfelds zu beachten, die zu spezifischen Herausforderungen auch für den IT-Einsatz im Unternehmen führen. Als Beispiele werden von der ISO 38500:2015 technologischer Wandel, soziale Entwicklungen, regulatorische Verpflichtungen, Erwartungen der Stakehol-

[57] Quelle: *ISO/IEC 38500:2015*, S. 7; eigene Darstellung.
[58] Vgl. *ISACA 2012b*, S. 73, 77, 101, 11].

der oder politische Einflüsse genannt. Andererseits sind geschäftliche Anforderungen zu berücksichtigen, insbesondere die Unternehmensziele, wie beispielsweise die Aufrechterhaltung von Wettbewerbsvorteilen.

Direct

- Direct:
  Zur Umsetzung der bewerteten, ausgewählten und verabschiedeten Strategien und Richtlinien haben die Leitungsorgane (insb. die Unternehmensleitung) entsprechende Verantwortlichkeiten an die Management-Ebene zu delegieren und den Prozess der Umsetzung zu steuern. Mittels der Strategien sind insbesondere die durch IT-Investitionen zu erreichenden Ziele festzulegen, während die Richtlinien eine korrekte Nutzung der IT durch die Mitarbeiter sicherstellen sollen. Für im Rahmen der Bewertung identifizierte Bedarfe ist durch die Leitungsorgane die Entwicklung entsprechender Vorschläge zu initiieren. Im Hinblick auf eine gute Governance-Kultur sind die Führungskräfte der Management-Ebene durch die Leitungsorgane zu transparenter Information sowie zum Einhalten aller Regelungen zur Steuerung der IT und der sechs Prinzipien der IT-Governance anzuhalten.

Monitor

- Monitor:
  Die Überwachungsverantwortung der Leitungsorgane bezieht sich auf die Leistungsüberwachung der IT. Diese erfolgt auf der Basis entsprechender Rückmeldungen aus der Managementebene unter Nutzung geeigneter Messsysteme. Die Überwachung hat sich zu richten auf die Erreichung der Unternehmensziele, die Übereinstimmung mit den verfolgten Strategien und die Konformität mit Compliance-Verpflichtungen aus gesetzlichen, behördlichen und vertraglichen Vorgaben sowie unternehmensinternen Regelungen.

Management und Managementsysteme

Die Schnittstelle zwischen Governance und Management wird in erster Linie durch die Zusammenarbeit der Mitglieder der Leitungsorgane mit den Führungskräften der nachgelagerten Hierarchieebenen gebildet. Zur Erfüllung der ihm delegierten Aufgaben bedienen sich die Führungskräfte der Fachabteilungen genauso wie der IT-Abteilung verschiedener, für die Steuerung und Überwachung der IT relevanter Managementsysteme. Beispiele hierfür sind

- Risikomanagementsysteme (RMS),
- interne Kontrollsysteme (IKS) oder
- Compliance-Managementsysteme (CMS),

die auch IT-Belange adressieren, aber auch spezielle IT-Managementsysteme, wie beispielsweise

- IT-Servicemanagementsysteme (ITSM) oder
- Informationssicherheitsmanagementsysteme (ISMS).

Auf der Grundlage der erfolgten Diskussion soll mit folgender Darstellung eine Übersetzung des Modells der IT-Governance versucht werden, vgl. Abbildung 4.

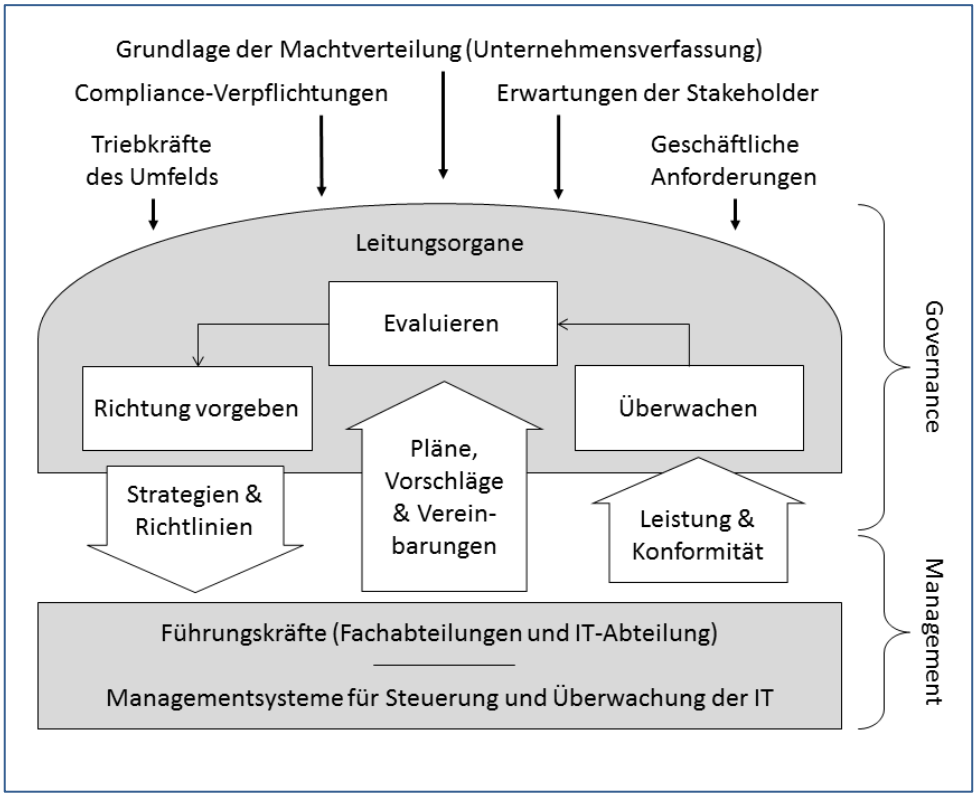

Abbildung 4
Modell der IT-Governance nach ISO/IEC 38500:2015 (Übersetzung)[59]

9 Leitlinien für die IT-Governance

47 normative Aussagen als Leitlinien

Die weitere Ausgestaltung des Modells der IT-Governance erfolgt in der ISO/IEC 38500: 2015 dadurch, dass die drei Governance-Funktionen für jedes der sechs Prinzipien expliziert werden. In der Summe werden 47 normative Aussagen als Leitlinien für das Führungshandeln der Leitungsorgane

[59] Quelle: *ISO/IEC 38500:2015*, S. 7; eigene Darstellung und Übersetzung.

im Rahmen der IT-Governance aufgelistet.[60] Die ISO/IEC 38500:2015 versteht diese Aussagen als Startpunkt für eine interne Diskussion darüber, wie die Governance-Verantwortung der Leitungsorgane unternehmensspezifisch auszugestalten ist.[61] Diese Darstellung stellt sowohl eine Systematisierung bisheriger Aussagen der ISO/IEC 38500:2015 als auch eine Erweiterung der Aussagen zum jeweiligen Prinzip bzw. der betreffenden Governance-Funktion dar. So werden beispielsweise dem Strategie-Prinzip insgesamt sieben Leitlinien zugeordnet, die alle die Verantwortung der Leitungsorgane umschreiben, vgl. Tabelle 3.

Tabelle 3
Kombination aus Prinzipien und Governance-Funktionen am Beispiel von Prinzip 9 [62]

Prinzip → **Governance-Funktion ↓**	Strategie (strategy) • Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung • Ausrichtung des IT-Einsatzes an der Unternehmensstrategie
Evaluieren	(1) Entwicklungen sowohl der IT als auch der Geschäftsprozesse sollten bewertet werden, um die Unterstützung der künftigen Geschäftsanforderungen durch die IT sicherzustellen. (2) Im Rahmen der Prüfung von Plänen und Richtlinien sollten IT-Nutzung und -Maßnahmen bewertet werden, um die Ausrichtung an den Unternehmenszielen und die Erfüllung der Anforderungen wichtiger Stakeholder zu gewährleisten. Hierbei sollten auch bewährte Verfahren berücksichtiget werden. (3) Der IT-Einsatz sollte Gegenstand eines geeigneten Risikomanagements sein.
Richtung vorgeben	(4) Die Erstellung und Verwendung von Strategien und Richtlinien sollte dahingehend gesteuert werden, dass das Unternehmen von den Entwicklungen der IT profitiert. (5) Vorschläge für innovativen IT-Einsatz sollten angeregt werden, damit das Unternehmen auf neue Chancen und Herausforderungen reagieren, neue Geschäftspotenziale erschließen oder Prozesse verbessern kann.
Überwachen	(6) Der Fortschritt in der Umsetzung genehmigter IT-Vorschläge sollte überwacht werden, um sicherzustellen, dass die Ziele mit den geplanten Ressourcen in der vorgesehenen Zeit erreicht werden. (7) Der IT-Einsatz sollte überwacht werden, um sicherzustellen, dass der beabsichtigte Nutzen realisiert wird.

[60] Im Vergleich mit der ersten Ausgabe der Norm ist in der IS 38500:2015 eine weitere normative Aussage hinzugekommen. Hierbei handelt es sich um die Forderung, dass für die Beschaffung ein gemeinsames Verständnis von Unternehmen und Lieferanten über die Beschaffungsziele hergestellt und aufrechterhalten werden soll (Prinzip 3 / Direct), vgl. *ISO/IEC 38500:2015*, S. 9.
[61] Vgl. *ISO/IEC 38500:2015*, S. 8.
[62] Nach *ISO/IEC 38500:2015*, S. 8f.

18-Felder-Matrix

Die Kombination von Governance-Funktionen (G) und Prinzipien (P) der IT-Governance lässt sich systematisch in einer 18-Felder-Matrix darstellen, vgl. Tabelle 4. Die in Tabelle 3 enthaltenen Leitlinien sind in der Matrix den Feldern 4 (Strategie / Bewertung), 5 (Strategie / Richtung vorgeben), und 6 (Strategie / Überwachung) zuzuordnen. Die Einordnung von IT-bezogenen Steuerungs- und Überwachungsmaßnahmen kann helfen, den eigenen Status festzustellen und Lücken zu identifizieren, indem analysiert wird, inwieweit die allgemeinen Leitlinien der ISO/IEC 38500:2015 im Unternehmen Anwendung finden. Auch für eine Abstimmung der verschiedenen, auf das eigene Unternehmen hin konkretisierten Leitlinien kann die Matrix herangezogen werden. Die "Summen" der Zeilen oder Spalten zeigen auf, ob und ggf. inwieweit Prinzipien oder Governance-Funktionen bisher vernachlässigt wurden.

Tabelle 4
Matrix der IT-Governance[63]

	Governance-Funktionen (F)		
Prinzip (P)	Bewertung	Richtung vorgeben	Überwachung
Verantwortlichkeit	< 1 >	< 2 >	< 3 >
Strategie	< 4 >	< 5 >	< 6 >
Beschaffung	< 7 >	< 8 >	< 9 >
Performanz	< 10 >	< 11 >	< 12 >
Konformität	< 13 >	< 14 >	< 15 >
Verhalten	< 16 >	< 17 >	< 18 >

10. Ergänzungen der ISO/IEC TS 38501:2015

Zyklischer Implementierungsansatz

Der zyklische Implementierungsansatz der ISO/IEC TS 38501:2015 mit drei Phasen richtet sich auf, vgl. Abbildung 5:

- das Etablieren und Pflegen eines förderlichen Umfelds;

[63] Nach *Klotz 2008*, S. 22.

- das Wahrnehmen der Governance-Verantwortung entsprechend dem IT-Governance-Modell;
- die kontinuierliche Bewertung und Verbesserung der etablierten IT-Governance.[64]

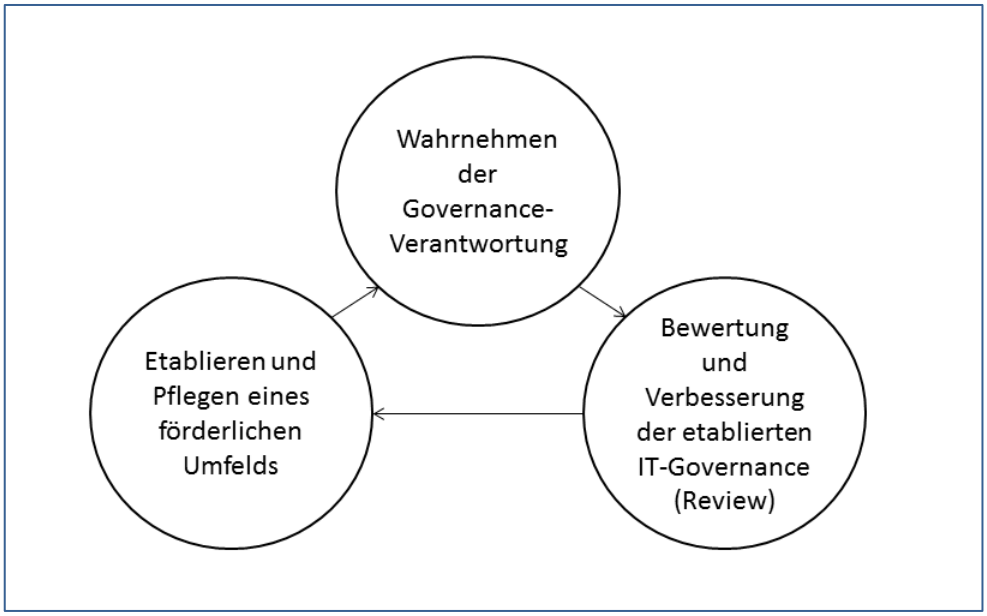

Abbildung 5
Implementierungszyklus für die ISO/IEC 38500 [65]

Etablieren und Pflegen des Umfelds

Entsprechend der Bedeutung der IT für das Unternehmen müssen sich die Leitungsorgane, insbesondere die Unternehmensleitung bei der Implementierung eines Governance-Systems für die IT engagieren, z. B. für einen kulturellen Wandel oder die Verbesserung von IT-Prozessen. Vor allem ein effektives und effizientes Stakeholdermanagement, das zu einem klaren Rollenverständnis (z. B. eines Sponsors) und einer klaren Verteilung der Verantwortlichkeiten führen soll, wird betont. Organisatorisch kann die Implementierung durch einen Governance-Steuerungsausschuss unterstützt werden.[66]

Wahrnehmen der Governance-Verantwortung

Das Wahrnehmen der Governance-Verantwortung besteht in der Anwendung der ISO 38500:2015. Die ISO/IEC TS 38501:2015 verweist darauf, dass das Ergebnis der Implementierung eines Governance-Systems für die IT klar formuliert sein sollte. Aus Sicht der Leitungsorgane soll der Schwer-

[64] Nach *ISO/IEC TS 38501:2015*, S. 1f.
[65] Nach *ISO/IEC 38500:2015*, S. 8f.; eigene Darstellung.
[66] Nach *ISO/IEC TS 38501:2015*, S. 2f.

punkt auf das „Was“ gelegt werden, nicht auf das „Wie“.[67] Im Einzelnen orientieren sich die Empfehlungen der Spezifikation an den drei Governance-Funktionen:

- Evaluate: Evaluate
  Für die Bewertung ist ein Verständnis des internen Umfelds, der Unternehmensziele und -strategien, des Risikobewusstseins, der Organisationskultur, der allgemeinen IT-Kompetenz, der Rolle der IT bei der Gewinnung von Wettbewerbsvorteilen, der wesentlichen IT-Services, die Unterstützung von wesentlichen Geschäftsprozessen durch IT u. a. m. erforderlich. Ebenso muss das externe Umfeld verstanden werden. Dieses besteht für die ISO/IEC TS 38501:2015 aus folgenden Faktoren:
  - regulatorisches Umfeld;
  - Entwicklung der Informationstechnologien;
  - gesellschaftliche Entwicklungen im kulturellen und sozialen Umfeld;
  - Verfügbarkeit von benötigten Fähigkeiten und Fertigkeiten;
  - IT-Nutzung der Wettbewerber;
  - Entwicklungen der Märkte mit Auswirkung auf die IT-Nutzung;
  - Einflüsse externer Stakeholder und
  - externe Bedrohungen für die Unternehmens-IT.

  Auf dieser Basis ist zu bestimmen, wie das Unternehmen aktuell durch die im Unternehmen eingesetzte IT unterstützt wird. Die Bewertung kann sich hierbei an den Prinzipien der IT-Governance nach der ISO/IEC 38500:2015 richten. Als Bewertungskriterium wird von der ISO/IEC TS 38501:2015 eine Unterscheidung nach Nutzen und Anhaltspunkten i. S. von Maßnahmen bzw. Verhaltensweisen, durch die sich der jeweilige Nutzen einstellt, vorgeschlagen. Für jedes Prinzip werden zwei bis drei Nutzen bzw. Anhaltspunkte angeben. Tabelle 5 zeigt die Bewertungskriterien für das Prinzip “Strategie”. Für den ersten Zyklus der Implementierung eines IT-Governance-Systems kann diese Bewertung als „Baseline“ dienen. In den folgenden Zyklen ist die Bewertung auf Basis der angepassten, auf das Unternehmen konkret ausgerichteten Bewertungskriterien zu wiederholen.[68]

[67] Nach *ISO/IEC TS 38501:2015*, S. 3.
[68] Nach *ISO/IEC TS 38501:2015*, S. 4f.

Tabelle 5
Bewertungskriterien für das Prinzip "Strategie"[69]

Nutzen	Anhaltspunkte
Die Geschäftsaktivitäten werden effektiv durch die IT unterstützt und der strategische Wandel wird durch die IT angemessen ermöglicht.	Die IT ist an den Unternehmenszielen und der Architektur ausgerichtet.
Die Entscheidungsunterstützungssysteme des Unternehmens bieten hochwertige und zeitgerechte Informationen.	Die Geschäftsanforderungen an die Nutzbarkeit, die Vertraulichkeit, die Integrität und die Verfügbarkeit von entscheidungsrelevanten Daten sind identifiziert und werden erfüllt.
Das Erreichen der Unternehmensziele wird durch IT-Innovationen ermöglicht.	IT wird genutzt, um Geschäftsmodelle zu ermöglichen oder sie evolutionär oder disruptiv zu verändern.

Direct

- Direct:
  Die Leitungsorgane haben die Richtung des IT-Einsatzes vorzugeben. Hierfür sind von ihnen notwendige Veränderungen zu initiieren und Maßnahmen zur Implementierung eines IT-Governance-Systems zu ergreifen. Hierzu gehört eine adäquate Kultur, z. B. bezüglich Risiken und Compliance. Die Formulierung von Zielvorgaben kann sich wieder an den für die Prinzipien verwendeten Bewertungskriterien orientieren. Ergibt sich im Rahmen einer Lückenanalyse Handlungsbedarf, so sind entsprechende Maßnahmen im Rahmen eines Veränderungsprogramms festzulegen. Hierfür sind nach der ISO/IEC TS 38501:2015 zu bestimmen:
  - benötigte Ressourcen und Fähigkeiten/Fertigkeiten;
  - Einbeziehung von Stakeholdern und Zuordnung von Verantwortlichkeiten;
  - Budget und Zeitplanung;
  - Abhängigkeiten zu anderen Projekten;
  - Prioritäten basierend auf den Erfordernissen des Unternehmens;
  - Potenziale für schnelle Erfolge (sog. „Quick-wins").

  Die Leitungsorgane haben das Veränderungsprogramm zu prüfen, ggf.

[69] Nach *ISO/IEC TS 38501:2015*, S. 12; eigene Übersetzung.

freizugeben und für Managementunterstützung der Implementierung zu sorgen. Insbesondere sind Aufgaben und Verantwortlichkeiten festzulegen und zu delegieren. Neben dem Governance-Steuerungsausschuss sind ggf. weitere Gremien zu bestimmen, z. B. für Risikomanagement oder Revision.[70]

- Monitor:
  Die Überwachung Implementierung eines IT-Governance-Systems muss beantworten können, ob die richtigen Maßnahmen ergriffen werden, welcher Fortschritt erzielt wird und ob der intendierte Zielzustand erreicht ist. Auch diese Überwachung soll sich wieder an den vorgegebenen Bewertungskriterien orientieren. Allerdings sollen die hierfür notwendigen Informationen aus vorhandenen Managementsystemen zugeliefert werden.[71]

Monitor

Kontinuierliche Bewertung und Verbesserung

Mit der initialen Implementierung des IT-Governance-Systems ist eine Baseline vorhanden, auf der die weiteren Implementierungszyklen aufbauen und diese verbessern. Die Ergebnisse gehen dann wiederum kontinuierlich in eine Bewertung und Beurteilung der Zielerreichung ein. Das Review hat sich insbesondere darauf zu richten, ob

- sich die Einschätzung der Leitungsorgane in Bezug auf den potenziellen Wertbeitrag der IT verändert;
- sich die geschäftlichen Anforderungen der Führungskräfte in Bezug auf die IT-Nutzung verändern;
- aus besserer IT-Governance ein höherer Wertbeitrag der IT resultiert;
- die Risiken der IT-Nutzung umfassend verstanden und im Rahmen der Governance-Strukturen gemanagt werden.

Neuer Implementierungszyklus

Wird durch das Review ein Handlungsbedarf deutlich, hat der Governance-Steuerungsausschuss einen neuen Implementierungszyklus anzustoßen, um eine kontinuierliche Verbesserung des IT-Governance-Systems sicherzustellen.[72]

[70] Nach *ISO/IEC TS 38501:2015*, S. 5ff.
[71] Nach *ISO/IEC TS 38501:2015*, S. 7f.
[72] Nach *ISO/IEC TS 38501:2015*, S. 8f.

11. Ergänzungen der ISO/IEC TR 38502:2014

Wie bereits erwähnt, beinhaltet der ISO/IEC TR 38502:2014 die in die ISO/IEC 38500:2015 weitgehend identisch übernommenen Begriffsdefinitionen sowie das Modell der IT-Governance. Die Ergänzungen des Reports beziehen sich zum einen auf eine Erörterung der Abgrenzung zwischen Governance und Management, zum anderen auf die Konzeption eines allgemeinen Governance-Framework für die Unternehmens-IT, aus dem verschiedene Empfehlungen abgeleitet werden.

Unterscheidung Governance vs. Management

In Bezug auf das Modell der IT-Governance, vgl. Abbildung 4, wird die Unterscheidung zwischen Governance und Management in folgenden fünf Aspekten gesehen:

- Governance-Verantwortung:
  Die Mitglieder der Leitungsorgane sind verantwortlich für IT-Governance und den effektiven, effizienten und den Erwartungen der Stakeholder entsprechenden IT-Einsatz im Unternehmen.
- Strategievorgabe und Überwachung:
  Governance stellt sich als Mittel dar, durch welches die Leitungsorgane die Richtung in Bezug auf den IT-Einsatz vorgeben sowie die Erreichung der Unternehmensziele und die Leistungserbringung des Managements überwachen.
- Delegation:
  Das Management wird – ggf. auch im Rahmen von Governance-Aufgaben – tätig, indem ihm von den Leitungsorganen adäquate Verantwortlichkeiten und Befugnisse übertragen werden.
- Management-Verantwortung:
  Führungskräfte sind verantwortlich für das Erreichen von Zielen im Rahmen von Strategien und Richtlinien, die von den Leitungsorganen für den IT-Einsatz vorgegeben werden.
- Governance sowie interne Steuerung und Überwachung:
  Eine effektive IT-Governance bedarf effektiver interner Kontrollsysteme (IKS) als Teil der Management- und Überwachungssysteme des Unternehmens.[73]

[73] Nach *ISO/IEC TR 38502:2014*, S. 6.

Governance-Referenzmodell

Der ISO/IEC TR 38502:2014 beschreibt sieben Kernelemente eines Governance-Framework für die Unternehmens-IT, vgl. Abbildung 6.

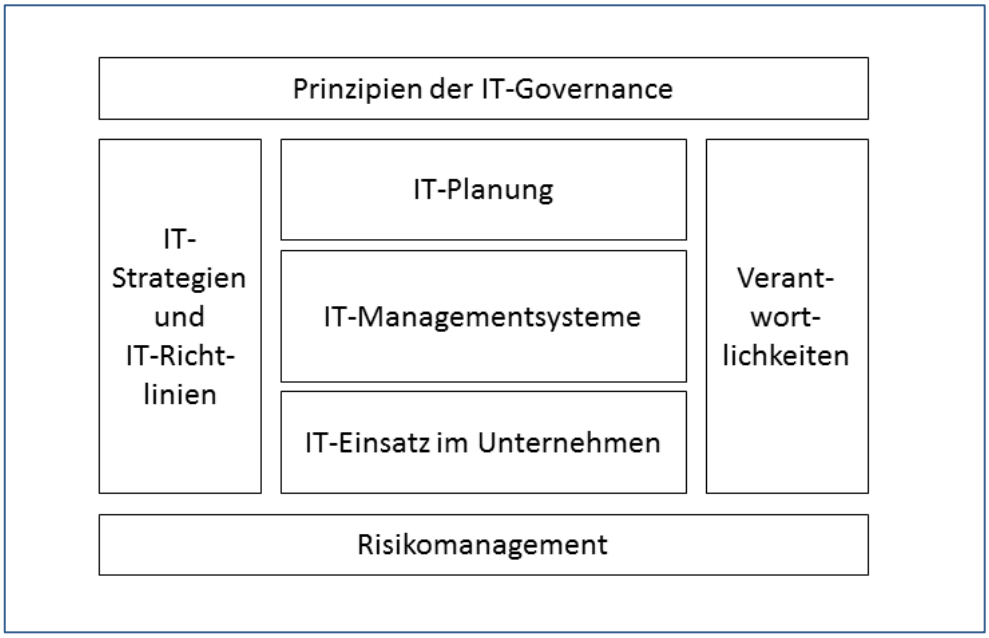

Abbildung 6
IT-Governance-Framework des ISO/IEC TR 38502[74]

Bezug zum Modell und den Prinzipien der IT-Governance

Während das Modell der IT-Governance eine Kombination aus Prozess- und Rollenmodell darstellt, lässt sich das Framework für die IT-Governance als Strukturmodell verstehen. Es bestehen jedoch Übereinstimmungen. Die IT-Strategien und -Richtlinien des Framework resultieren im Governance-Modell aus der Governance-Funktion „Direct“. Die Managementsyteme sind im Governance-Modell Bestandteil der Management-Ebene und die IT-Planung nimmt im Governance-Modell von der Managementebene ihren Ausgang und unterliegt in der Governance-Ebene der Bewertung durch die Leitungsorgane. Neben den Elementen des Modells der IT-Governance sind zudem die Prinzipien der IT-Governance in das Framework integriert.

Empfehlungen

Im Anschluss an die Darstellung von Modell und Framework formuliert die ISO/IEC TR 38502:2014 verschiedene, insbesondere an die Leitungsorgane gerichtete Empfehlungen. Diese greifen verschiedene Aspekte des Modells bzw. des Framework auf, orientieren sich jedoch nicht strikt an der einen oder der anderen Struktur. Beispielsweise werden für die Formulierung einer IT-Strategie sechs Handlungsempfehlungen für die Leitungsorgane getroffen, vgl. Tabelle 6.

[74] Quelle: *ISO/IEC TR 38502:2014*, S. 7; eigene Darstellung und Übersetzung.

Tabelle 6
Handlungsempfehlungen des ISO/IEC TR 38502:2014 für die Strategieformulierung[75]

Nr.	Handlungsempfehlung – Die Leitungsorgane sollen ...
1	durch aktive Führung sicherstellen, dass aus der Entwicklung von Strategien ein Wertbeitrag der IT generiert wird.
2	die IT-Strategie des Unternehmens genehmigen, wobei der Beitrag dieser Strategie zur Erreichung der Geschäftsziele, aber auch die damit verbundenen Risiken zu berücksichtigen sind.
3	sicherstellen, dass das interne und externe IT-Umfeld regelmäßig überwacht wird. IT-Strategie und IT-Richtlinien sind ggf. an geänderte Umfeldbedingungen anzupassen.
4	sicherstellen, dass das Verhalten der Organisationsmitglieder durch entsprechende Richtlinien (z. B. hinsichtlich Compliance, Risikomanagement, Erreichung der Unternehmensziele) gesteuert wird.
5	sicherstellen, dass bei neuen geschäftlichen Herausforderungen Ziele, Strategien und Richtlinien geklärt und ggf. angepasst werden.
6	die entsprechend der IT-Strategie notwendige Veränderungsbereitschaft im Unternehmen einschätzen können. Es ist sicherzustellen, dass die hierfür erforderliche Zustimmung sowie das notwendige Leistungsvermögen vorhanden sind.

12. Fazit

Entwicklung der ISO/IEC 38500

Die ISO/IEC 38500:2015 weist gegenüber der ersten Ausgabe keine grundsätzlichen Änderungen auf. Sie übernimmt im Wesentlichen die Weiterentwicklungen des ISO/IEC TR 38502:2014, insbesondere in Bezug auf die Begrifflichkeit und das Modell der IT-Governance. Mit den bisher publizierten und den in Arbeit befindlichen Dokumenten ist die Grundlage der Entwicklung der ISO/IEC 38500 zur Normenreihe gelegt, was ihr und den weiteren Dokumenten eine verstärkte Beachtung in der Praxis sichern wird. Auch Standards, allen voran COBIT®, werden in ihrer Weiterentwicklung die ISO/IEC 3850x berücksichtigen müssen.

Konsistenz von Norm, TR und TS

Im Moment erweist sich das Zusammenspiel der bisherigen drei Dokumente (Norm, Report, Spezifikation) als zumindest teilweise problematisch. Mit der in der Norm etablierten Struktur der Verbindung von Governance-Funktionen mit Prinzipien der IT-Governance ist ein Analyse- und Bewertungsraster – versinnbildlicht durch die in Tabelle 4 dargestellte Matrix – vorge-

[75] Nach *ISO/IEC TR 38502:2014*, S. 9.

geben, das in seiner Gesamtheit die Komplexität der Gestaltung von IT-Governance abzubilden in der Lage scheint. Trotzdem wird diese Struktur in den weiteren Dokumenten nicht genutzt. Sie findet sich weder im Implementierungsansatz noch in den Bewertungskriterien der ISO/IEC TS 38501: 2015 wieder. Gleiches gilt für die ISO/IEC TR 38502:2014. Der Zusammenhang zwischen dem Modell und dem Framework für die IT-Governance wird nicht einmal thematisiert. Die verschiedenen Handlungsempfehlungen können sicherlich allgemein als sinnvoll betrachtet werden, in einem systematischen Zusammenhang mit den 47 Leitlinien aus der Norm stehen sie jedoch nicht.

Anwendung

Für die Entwicklung der Normenreihe wäre eine bessere Abstimmung wünschenswert. Allerdings ist zu berücksichtigen, dass gerade ein technischer Report rein informativen Charakter hat und mitunter nur einzelne inhaltliche Elemente der zugehörigen Norm adressiert. Insofern bleibt es den die Norm anwendenden Organisationen selbst überlassen, ob und inwieweit sie die verschiedenen Modelle, Konzepte, Leitlinien und Empfehlungen für die Gestaltung ihrer IT-Governance nutzen. Stehen Prozessorientierung und Systematik im Vordergrund, sind Unternehmen mit den Governance-Prozessen von COBIT® 5 sicherlich besser aufgehoben. Allerdings bieten sich die ISO/IEC 38500:2015 und die ergänzenden Dokumente durchaus als Mittel einer kritischen Reflexion der COBIT®-Inhalte an. Die Normenreihe ISO/IEC 3850x gehört damit zur Arbeitsausstattung eines jeden IT-Governance-Managers bzw. aller IT-Verantwortlichen, die mit der Ausgestaltung und ständigen Verbesserung ihrer IT-Governance befasst sind.

Quellenangaben

Ahuja/Chan 2015: Ahuja, Suchit; Chan, Yolande E., "IT Security Governance: A Framework based on ISO 38500" (2015), CONF-IRM 2015, Proceedings. Paper 27, online unter: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1020&context=confirm2015 (Abruf am 10.08.2016)

Ayat/Masrom/Sahibuddin 2011: Ayat, Masarat; Masrom, Maslin, Sahibuddin, Shamsul: IT Governance and Small Medium Enterprises. 2011 International Conference on Software and Computer Applications, IPCSIT Vol. 9 (2011) IACSIT Press, Singapore 2011, S. 167-173, online unter: http://www.ipcsit.com/vol9/32-B042.pdf (Abruf am 10.08.2016)

Böhm/Goeken/Johannsen 2009: Böhm, Markus; Goeken, Matthias; Johannsen, Wolfgang: Compliance und Alignment: Vorgabenkonformität und Strategieabgleich als Erfolgsfaktoren für eine wettbewerbsfähige IT, in: HMD - Praxis der Wirtschaftsinformatik, Volume 269, Heft 269, 46. Jg (2009), S. 7-17

Bundesrechnungshof 2001: Bundesrechnungshof (Hg.) Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik – Leitlinien und gemeinsame Maßstäbe für IuK-Prüfungen – (IuK-Mindestanforderungen 2011), Stand: November 2011, online unter: https://www.bundesrechnungshof.de/de/veroeffentlichungen/broschueren/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik/at_download/file (Abruf am 10.08.2016)

Calder 2008: Calder, Alan: ISO/IEC 38500 – The IT-Governance Standard, IT Governance Publishing, Ely 2008

Committee on the Financial Aspects 2015: The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd. (Ed.): Report of the Committee on the Financial Aspects of Corporate Governance vom 1. Dez. 1992, online unter: http://www.ecgi.org/codes/documents/cadbury.pdf (Abruf am 10.08.2016)

da Cruz 2007: da Cruz, Marghanita: AS 8015-2005 – Australian Standard for Corporate Governance of IT, in: The IT Service Management Forum (itSMF) (Hg.): Frameworks für das IT-Management – Die führenden 24, ITSM Library, Van Haren Publishing 2007, S. 137-144

DIN/NIA 2015: DIN Deutsches Institut für Normung e. V. Normenausschuss Informationstechnik und Anwendungen (NIA): Jahresbericht 2015 DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN e. V., Berlin 2015, online unter: http://www.din.de/blob/72142/53a915f6e815a8b6834be208d7dfacd3/nia-jahresbericht-2015-data.pdf (Abruf am 10.08.2016)

Fischlin 2015: Fischlin, Roger: Neue Fassung der ISO/IEC 38500 "Governance of IT for the organization", XING-Gruppe IT-Governance, Forum IT Governance - Entwicklungen, Chancen, Risiken, Beitrag vom 14.02.2015, online unter: https://www.xing.com/communities/posts/neue-fassung-der-iso-strich-iec-38500-governance-of-it-for-the-organization-1009267047 (Abruf am 10.08.2016)

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

Huber 2009: Huber, Bernhard: Managementsysteme für IT-Serviceorganisationen – Entwicklung und Umsetzung mit EFQM, COBIT, ISO 20000, ITIL, dpunkt, Heidelberg 2009

IEC 2016: International Electrotechnical Commission (IEC): Germany IEC Full Member, online unter: http://www.iec.ch/dyn/www/f?p=103:16:0::::FSP_ORG_ID:1007 (Abruf am 10.08.2016)

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

ISACA 2012b: Information Systems Audit and Control Association (ISACA): COBIT 5 – Enabling Processee, Deutsche Ausgabe, Rolling Meadows: ISACA 2012

ISO 2008: International Organization for Standardization (ISO) (Ed.): ISO/IEC standard for corporate governance of information technology, News, 5 June 2008, online unter: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1135 (Abruf 10.08.2016)

ISO 2016a: International Organization for Standardization (ISO): About ISO, online unter: http://www.iso.org/iso/home/about.htm, (Abruf am 10.08.2016)

ISO2016b: International Organization for Standardization (ISO): ISO/IEC JTC 1 Information technology, online unter: http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020 (Abruf am 10.08.2016)

ISO2016c: International Organization for Standardization (ISO): ISO/IEC JTC 1/SC 40 IT Service Management and IT Governance, online unter: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=5013818 (Abruf am 10.08.2016)

ISO2016d: International Organization for Standardization (ISO): ISO/IEC 38500:2015 – Information technology – Governance of IT for the organizatiom, online unter: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62816 (Abruf am 10.08.2016)

ISO/IEC 2015: International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) (Ed.): ISO/IEC Directives, Part 1, Consolidated JTC 1 Supplement 2015 – Procedures specific to JTC 1, online unter: http://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/9482942/JTC_1_Supplement_%28pdf_version%29.pdf?nodeid=9484244&vernum=-2 (Abruf am 10.08.2016)

ISO/IEC 38500:2008: ISO/IEC: Corporate governance of information technology, International Standard ISO/IEC 38500:2008, first edition 2008-06-01

ISO/IEC 38500:2015: ISO/IEC: Information technology – Governance of IT for the organization, International Standard ISO/IEC 38500:2015, second edition 2015-02-15

ISO/IEC JTC 1/SC 40: International Organization for Standardization (ISO): ISO/IEC JTC 1/SC 40 IT Service Management and IT Governance – About, online unter: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=5013818 (Abruf am 10.08.2016)

ISO/IEC TR 38502:2014: ISO/IEC: Information technology – Governance of IT – Framework and model, International Standard ISO/IEC 38502:2014, first edition 2014-02-01

ISO/IEC TS 38501:2015: ISO/IEC: Information technology – Governance of IT – Implementation guide, International Standard ISO/IEC 38501:2015, first edition 2015-04-01

ITGI 2015: IT Governance Institute® (ITGI®): Global Status Report on the Governance of Enterprise It (GEIT) – 2011, Rolling Meadows, ITGI 2011, online unter: http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-2011_res_Eng_0111.pdf (Abruf am 10.08.2016)

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

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

Klotz 2013: Klotz, Michael: 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, SIMAT AP Nr. 24, Jg. 5 (2013), online unter: https://www.econstor.eu/dspace/bitstream/10419/88419/1/773961380.pdf (Abruf am 10.08.2016)

Knolmayer/Aspirion/Loosli 2014: Knolmayer, Gerhard; Aspirion, Patra Maria; Loosli, Gabriela: IT-Governance. in: Gronau, Norbert u. a. (Hg.): Enzyklopädie der Wirtschaftsinformatik, Beitrag vom 17.11.2014, online unter: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/daten-wissen/Grundlagen-der-Informationsversorgung/IT-Governance (Abruf am 10.08.2016)

Konrad/Puchnan/Gann 2012: Konrad, Thomas; Puchan, Jörg & Gann, Thomas; (2012): Referenzprozessmodelle: Bestandsaufnahme, Synopse und Entwicklungspotentiale. In: e-Journal of Practical Business Research, Sonderausgabe: Business Process Benchmarking – Band I Grundlagen (Hrsg. Puchan/Gann) (07/2012), online unter: http://www.e-journal-of-pbr.info/downloads/2_BusinessProcessBenchmarking_I_Referenzprozessmodelle.pdf (Abruf am 10.08.2016)

Lang/Wimmer 2014: Lang, Ulrich; Wimmer, Martin (Hrsg.): CIOs und IT-Governance an deutschen Hochschulen, Ergebnisse einer von Markus von der Heyde durchgeführten Studie, Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI), Heilbronn 2014, online unter: https://www.zki.de/fileadmin/zki/Publikationen/ZKI_CIO-Studie_final.pdf (Abruf am 10.08.2016)

OECD 2004: Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD): OECD-Grundsätze der Corporate Governance, Neufassung 2004,

OECD Publications, Paris, online unter: https://www.oecd.org/corporate/ca/corporategovernanceprinciples/32159487.pdf (Abruf am 10.08.2016)

Quack 2009: Quack, Karin: ISO/IEC 38500 stärkt die IT-Position im Unternehmen, Computerwoche, Beitrag vom 22.05.2009, online unter: http://www.computerwoche.de/a/iso-iec-38500-staerkt-die-it-position-im-unternehmen,1896505 (Abruf am 10.08.2016)

Racz/Weippl/Seufert 2010: Racz, Nicolas; Weippl, Edgar; Seufert, Andreas: A process model for integrated IT governance, risk, and compliance management, in: "Proceedings of the Ninth Baltic Conference on Databases and Information Systems 2010 (DB&IS 2010)", S. 155-170, online unter: http://www.grc-resource.com/resources/racz_al_grc_process_model_balticdbis2010.pdf (Abruf am 10.08.2016)

Rath/Sponholz 2009: Rath, Michael; Sponholz, Rainer: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen. Erich Schmidt, Berlin 2009

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

Schwertsik 2013: Schwertsik, Andreas Roland: IT-Governance als Teil der organisatorischen Governance – Ausgestaltung der IT-Entscheidungsrechts am Beispiel der öffentlichen Verwaltung. Springer Gabler, Wiesbaden 2013

Standards Australia 2015: Standards Australia (Ed.): 2015 Edition of ISO/IEC 38500 Published, Media Release, 23 March 2015, online unter: http://www.standards.org.au/OurOrganisation/News/Documents/SA%20Media%20Release%20March%202015%20-%20%20ISO%20IEC%2038500-2015.pdf (Abruf am 10.08.2016)

Strecker 2009: Strecker, Stefan: Ein Kommentar zur Diskussion um Begriff und Verständnis der IT-Governance: Anregungen zu einer kritischen Reflexion, Universität Duisburg-Essen, ICB-Research Report No. 36, Dezember 2009, online unter: https://www.econstor.eu/bitstream/10419/58157/1/716008440.pdf (Abruf am 10.08.2016)

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 Informationsmanagements
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 Projektmanagementsoftware – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.

04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	02.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen
06-14-025	01.2014	M. Klotz	IT-Compliance nach COBIT® – Gegenüberstellung von COBIT® 4.0 und COBIT® 5
06-14-026	04.2014	L. von Blumröder	Projektpriorisierung im Rahmen eines ganzheitlichen Projektportfoliomanagements
06-14-027	06.2014	S. Press	Automatisierte Kontrollen in der Beschaffung – Exemplarische Konzeption und Umsetzung
06-14-028	07.2014	M. Klotz	IT-Compliance – Begrifflichkeit und Grundlagen
07-15-029	09.2015	M. Klotz	Projektmanagement-Normen und –Standards
08-16-030	08.2016	M. Klotz	ISO/IEC 3850x – Die Normenreihe zur IT-Governance