

IT-Compliance

Erfolgreiches Management
regulatorischer Anforderungen

Von

Dr. Michael Rath
Rainer Sponholz

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet
über <http://dnb.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter

[ESV.info/978 3 503 11093 3](http://ESV.info/9783503110933)

ISBN: 978 3 503 11093 3

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co., Berlin 2009
www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen
der Deutschen Nationalbibliothek und der Gesellschaft für das Buch
bezüglich der Alterungsbeständigkeit und entspricht
sowohl den strengen Bestimmungen der US Norm Ansi/Niso
Z 39.48-1992 als auch der ISO-Norm 9706.

Druck und Bindung: Hubert & Co., Göttingen

Vorwort

Auf einer Konferenz zum Thema „IT-Governance“ wurde (unter Beteiligung der beiden Autoren) intensiv darüber diskutiert, wie man überhaupt die Vielzahl „regulatorischer Anforderungen“ an die im Unternehmen vorhandene Informationstechnologie (IT) erfüllen und damit „IT-Compliance“ gewährleisten könne.

Nach Ansicht einiger Teilnehmer dieser Diskussion sei es schon allein deshalb unmöglich, dauerhaft „100% IT-Compliance“ zu erreichen, da niemand in der Lage sei, alle diesbezüglichen Normen und Anforderungen überhaupt zu kennen: Die Anforderungen reichten von so trivialen Vorgaben wie der Bildschirmarbeitsplatzverordnung über steuerrechtliche Regelungen für die Anerkennung elektronischer Rechnungen bis hin zu den komplexen Bestimmungen in Bezug auf die Archivierung und Auswertung von (privaten und geschäftlichen) E-Mails. Darüber hinaus würde der Wirtschaftsprüfer jährlich anfragen, die Betriebsprüfer des Finanzamtes hätten sich neben der inzwischen etablierten Datenübernahme von steuerrelevanten Daten auch für die Sicherheitsmaßnahmen im Unternehmen interessiert gezeigt, und auch das Regierungspräsidium habe eine Datenschutzprüfung angekündigt.

Als Ergebnis der Diskussion wurde festgestellt, dass sich nicht nur staatlich beaufsichtigte Branchen, in denen die regulatorischen Anforderungen an die Datenverarbeitung besonders hoch sind, mit den vielfältigen Aspekten von IT-Compliance befassen müssen, sondern grundsätzlich alle Unternehmen, die Informationstechnologie in ihrer täglichen Arbeit anwenden. Die Unternehmensleitung muss demgemäß sicherstellen, dass ihre IT so betrieben wird, dass das Unternehmen auf der einen Seite (gerade wegen seiner Abhängigkeit von der Funktionstüchtigkeit der Datenverarbeitung) auch im Notfall weiterarbeiten kann, auf der anderen Seite aber schutzwürdige Belange wie etwa Daten-, Verbraucher-, Anleger- und Arbeitnehmerschutz gewährleistet sind.

Wie aber erhält man überhaupt Kenntnis von den zahlreichen Anforderungen an die IT? Bei dem Streben nach der im Unternehmen notwendigen IT-Compliance gilt es zunächst, den Überblick zu bewahren und die Systematik der relevanten Regelungen zu verstehen. Dabei muss man ein-

schätzen, wie „verbindlich“ diese Regeln sind, ob sie also als formelles Gesetz, behördliche Richtlinie oder „nur“ als Best Practice-Empfehlung zu betrachten sind. Diese Regularien werden in diesem Buch verallgemeinernd als „regulatorische Anforderungen“ bezeichnet, auch wenn eine Vielzahl der hier dargestellten Bestimmungen eben gerade nicht von einem mit Normsetzungsbefugnis ausgestatteten Normgeber stammen.

IT-Compliance bedeutet aber weit mehr als die bloße Einhaltung von IT-spezifischen Regularien. Dieses Werk will daher gerade nicht die unterschiedlichen regulatorischen Anforderungen aneinander reihen und schlicht deren stringente Beachtung postulieren. Vielmehr soll versucht werden, die Herkunft dieser Normen, deren unterschiedlichen Ziele sowie die unterschiedlichen Möglichkeiten der Umsetzung und des Management von IT-Compliance darzustellen. Wir sprechen daher in diesem Buch auch über das Wirkungsmodell von IT-Sicherheit, die Kosten von (IT)-Compliance, die Einführung entsprechender Prozesse und die passenden Werkzeuge, die sich hinter den Begriffen CobiT, ITIL und UCF verstecken. Dabei geht es uns auch darum, anhand von zunächst profan anmutenden Beispielen und der Darstellung einschlägiger Studien ein Gefühl für diese komplexe Materie zu vermitteln.

Unser Dank gilt insbesondere Frau Karin Thelemann, Präsidentin der ISACA Deutschland, und Frau Manuela Buck sowie Herrn Christian Kraft für ihre wertvollen Hinweise und Anregungen. Weiterhin möchten wir den Herren Dr. Detlef Zimmer und Benno Rieger von der SIZ GmbH für die Zurverfügungstellung ihres IT-Sicherheits-Modells, den Herren Jörg Asma und Carsten Schirp von der KPMG AG Wirtschaftsprüfungsgesellschaft für ihre Hinweise zum „Harmonised Shield“ und Herrn Markus Gaulke, ebenfalls von der KPMG, für das Praxisbeispiel zu den gemappten Standards danken. Ganz besondere Anerkennung verdient Herr Tobias Stähle für seine kritischen und zugleich konstruktiven Kommentare. Für die uns gegenüber geübte „familiäre Geduld“ danken wir auch unseren beiden Ehefrauen Ute Sponholz und Gudrun Rath.

Wir wünschen Ihnen viel Spaß bei der Lektüre und der anschließenden Umsetzung von IT-Compliance in der Praxis!

Die Autoren

Inhaltsverzeichnis

Vorwort.....	7
Inhaltsverzeichnis	9
Abkürzungsverzeichnis.....	13
Abbildungsverzeichnis	19
Kapitel 1: Einführung	21
1.1 Ursprung und Ziele von (IT)-Compliance	21
1.2 Governance.....	25
1.3 IT-Governance.....	28
1.4 Data Governance	31
1.5 Governance-Risk-Compliance (GRC)	32
1.6 Interdisziplinarität der IT-Compliance.....	32
1.7 Zusammenfassende Kapitelübersicht.....	35
Kapitel 2: Wirkungsmodell der IT-Sicherheit.....	37
2.1 Entwicklung der Computersicherheit und Wirkungsmodell der IT-Sicherheit.....	37
2.2 Allgemeines GRC-Wirkungsmodell und Anwendungsbeispiele.....	45
2.3 Pflichtschutzmaßnahmen als regulatorische Anforderungen der IT-Compliance.....	50
2.4 IT-Sicherheit als volkswirtschaftliche Aufgabe.....	52
2.5 Fazit zum Thema IT-Compliance als Pflichtschutzmaßnahme im GRC-Wirkungsmodell	54
Kapitel 3: Treiber von IT-Compliance	55
3.1 Überblick.....	55
3.2 Treiber der IT-Compliance im Detail.....	56
3.3 Fazit zum Thema Treiber der IT-Compliance.....	66
Kapitel 4: Rechtlicher Rahmen der IT-Compliance	67
4.1 Regulatorische Anforderungen an IT-Compliance	67
4.2 Normenhierarchie und Gültigkeit regulatorischer Anforderungen..	72
4.3 Regulatorische Institutionen der IT-Compliance und deren Ziele...	73
4.4 Diskussion der absoluten oder relativen Zielvorgaben für Pflichtschutzmaßnahmen der IT-Compliance.....	82
4.5 Fazit zum rechtlichen Rahmen der IT-Compliance	86

Kapitel 5: IT-Compliance unter Einsatz von CobiT	87
5.1 ISACA, ITGI und CobiT	87
5.2 Das CobiT-Referenzmodell im Detail.....	89
Kapitel 6: Kosten der IT-Compliance	97
6.1 Grundsätzliche Überlegungen zur Wirtschaftlichkeit von IT- Compliance.....	97
6.2 Anzahl der Anforderungen und Kostenwirkungen in der Praxis.....	100
6.3 Rentabilitätsanalyse.....	103
6.4 Fazit zur Wirtschaftlichkeits- und Nutzenbetrachtung der IT- Compliance.....	115
Kapitel 7: Management von IT-Compliance	117
7.1 Einleitung zum Management der IT-Compliance.....	117
7.2 IT-Compliance-Organisation (Aufbau- und Ablauforganisation)...	121
7.3 Weitere Elemente der IT-Compliance-Organisation	126
Kapitel 8: Der IT-Compliance-Prozess	135
8.1 Gesamtprozess IT-Compliance	135
8.2 Identifikation und Analyse von regulatorischen Anforderungen	136
8.3 Zuordnung und Behebung von Kontrollschwächen	141
8.4 Berichterstattung über Compliance.....	142
8.5 Vorgehensmodell Initialprojekt IT-Compliance	146
Kapitel 9: Werkzeuge des (IT)-Compliance-Managements.....	155
9.1 Einsatz unternehmensübergreifender Standards	155
9.2 Compliance-Management-Software.....	162
9.3 Benchmarking des IT-Compliance-Management	181
9.4 Ergebnisse aus den Benchmarkstudien der IT Policy Compliance Group.....	185
Kapitel 10: Wesentliche Maßnahmen der IT-Compliance.....	191
10.1 Managementansatz auf der Basis der wesentlichen Maßnahmen	191
10.2 Maßnahmen der IT-Compliance auf Basis der Motivatoren für IT- Sicherheit aus Unternehmenssicht	192
10.3 Maßnahmen der IT-Compliance auf Basis des Unified Compliance Framework (UCF).....	193
10.4 Beschreibung der wesentlichsten IT-Sicherheitsmaßnahmen bzw. IT-Compliance-Anforderungen.....	198
10.5 IT-Sicherheit nach BSI-Leitfaden zur IT-Sicherheit	202
10.6 Fazit zum Bereich der wesentlichen Maßnahmen der IT- Compliance.....	205
Kapitel 11: Outsourcing und IT-Compliance	207
11.1 IT-Outsourcing als gesamtwirtschaftliches Risiko?	207
11.2 Reifegrad der IT und Auslagerungsfähigkeit.....	210

11.3	Umfang der Abhängigkeit vom Auslagerungsunternehmen und Maßnahmen zur Reduzierung	212
11.4	Nachweise der IT-Compliance bei Outsourcing	215
11.5	Berichtstypen von SAS 70/ ISA 402-basierten Compliance- Nachweisen bei Outsourcing	219
11.6	Diskussion zum Thema Nachweis der IT-Compliance bei Outsourcing	221
11.7	Fazit zum Thema Outsourcing und IT-Compliance	222
Kapitel 12:	Schlussbetrachtung und Ausblick	223
Anhang	225
A/1	Linkliste zu IT-Compliance	225
A/2	Übersicht IT-Compliance-Anforderungen des UCF	227
A/3	Übersicht Compliance-Software	239
A/4	Übersicht der Entwicklung von Gesetzen und Richtlinien für automatisierte Anlagen im Gesundheitsbereich	248
Quellenverzeichnis	251
1.	Literaturverzeichnis	251
2.	Verzeichnis der verwendeten Gesetze, Verordnungen und Entscheidungen	255
3.	Verzeichnis der Internetquellen	256
Stichwortverzeichnis	265
Autorenportraits	267