ERICH
SCHMIDT
VERLAG

IT-Compliance

Erfolgreiches Management regulatorischer Anforderungen

Von

Dr. Michael Rath

und

Rainer Sponholz

3., neu bearbeitete und erweiterte Auflage

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
http://ESV.info/978-3-503-19971-6

Zitiervorschlag:
Rath/Sponholz, IT-Compliance, 3. Aufl.

ISBN 978-3-503-19971-6 (gedrucktes Werk)
ISBN 978-3-503-19972-3 (eBook)

Alle Rechte vorbehalten
© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021
www.ESV.info

Druck: docupoint, Barleben

Vorwort zur grundlegend überarbeiteten 3. Auflage

Liebe Leser,

wir freuen uns sehr, Ihnen die erneut grundlegend überarbeitete Auflage unseres Buches über IT-Compliance präsentieren zu dürfen. Die Erstauflage erschien bereits im Jahre 2009 und war damit (unserer Wahrnehmung nach) auf dem deutschen Markt eines der ersten Bücher zum Thema IT-Compliance.

Es müssen sich nicht nur staatlich beaufsichtigte Branchen (bspw. der Finanzdienstleistungssektor), in denen die regulatorischen Anforderungen an die Datenverarbeitung besonders hoch sind, mit den vielfältigen Aspekten von IT-Compliance befassen, 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 Mitarbeiterschutz gewährleistet sind.

Wie aber erhält man Kenntnis von den zahlreichen Anforderungen? Bei dem Streben nach der im Unternehmen notwendigen IT-Compliance gilt es zunächst, den Überblick zu bewahren und die Systematik der relevanten Regelungen sowie deren unterschiedliche Zwecke zu verstehen. Zudem muss man einschätzen, wie „verbindlich" diese Regeln sind, ob sie also als formelles Gesetz (ohne Handlungsspielraum) anzusehen sind oder aufgrund der relativ generischen Anforderungen nur ein Ermessenspielraum für deren Umsetzung geschaffen wird. Alle IT-spezifischen Regularien werden in diesem Buch verallgemeinernd als „regulatorische Anforderungen" bezeichnet, auch wenn eine Vielzahl der hier dargestellten Bestimmungen eben gerade nicht von einem mit unmittelbarer Normsetzungsbefugnis ausgestatteten Normgeber stammen.

IT-Compliance bedeutet aber (ähnlich wie beim allgemeinen Begriff der Compliance) weit mehr als die bloße Einhaltung von IT-spezifischen Regularien. Dieses Werk will zudem nicht (nur) die unterschiedlichen regulatorischen Anforderungen aneinanderreihen und schlicht deren stringente Beachtung postulieren. Vielmehr soll versucht werden, die Herkunft dieser Normen, deren unterschiedliche Zielsetzungen sowie die unterschiedlichen Möglichkeiten der Umsetzung und des Managements von IT-Compliance darzustellen. Wir sprechen daher in diesem Buch auch über Rollen und Organisation der IT-Sicherheit, die Kosten von (IT-)Compliance, die Einführung entsprechender Prozesse und die passenden Werkzeuge. Dabei geht es uns vor allem darum, anhand von Beispielen und der Darstellung einschlägiger Studien ein Gefühl für diese komplexe Materie zu vermitteln.

Vorrangig definieren wir die regulatorischen Anforderungen als Pflichtschutzmaßnahmen im Wirkungsmodell der Informationssicherheit und zeigen auf, wie man mit dem sog. Mapping von Standards verschiedene Compliance-Anforderungen zusammenführen und managen kann. Der Erfolg eines praxisorientierten Managements der IT-Compliance basiert zuallererst auf der risiko- und anforderungsgerechten Implementierung von Schutzmaßnahmen und offen gesprochen nicht so sehr auf der Herausgabe von Richtlinien oder Policies als Lektüre für interne oder externe Prüfer.

Wir setzen den Fokus in diesem Buch deshalb auf das IT-Compliance-Standbein der Triade „Governance, Risk and Compliance (GRC)", da hier durch die Vielzahl möglicher Regelbrüche und Verstöße das größte Potenzial – und somit auch Risiko – für Revisionsfeststellungen, Sanktionen und Haftungsansprüche liegt. Governance- und Risiko-Management sind als organisatorische Prozesse in ihrer Wirksamkeit schwerer zu beurteilen und daher eher selten auf der Liste schwerwiegender Monita der internen und externen Prüfer. Das Buch soll deshalb eindeutig eine Hilfestellung für die Compliance-Praxis sein und ein umsetzungsorientiertes Verständnis für das Arbeiten mit den Standards vermitteln.

Wir wünschen Ihnen viel Spaß bei der Lektüre und der anschließenden Umsetzung von IT-Compliance in der Praxis. Zudem freuen wir uns über Ihr Feedback – sprechen Sie uns gerne an oder schreiben Sie uns eine E-Mail.

Dr. Michael Rath und Rainer Sponholz

Inhaltsverzeichnis

Vorwort zur grundlegend überarbeiteten 3. Auflage 5

Abkürzungsverzeichnis 11

Abbildungsverzeichnis 19

1 Einführung 21
1.1 Ursprung und Ziele von (IT-)Compliance 21
1.2 Governance 24
1.3 IT-Governance 27
1.4 Data Governance 31
1.5 Governance-Risk-Compliance (GRC) 33
1.6 Interdisziplinarität der IT-Compliance 34
1.7 Zusammenfassende Kapitelübersicht 36

2 Wirkungsmodell der IT-Sicherheit 39
2.1 Entwicklung der Computersicherheit und Wirkungsmodell der IT-Sicherheit 39
2.2 Allgemeines GRC-Wirkungsmodell und Anwendungsbeispiele 46
2.3 Pflichtschutzmaßnahmen als regulatorische Anforderungen der IT-Compliance 49
2.4 Fazit zum Thema IT-Compliance als Pflichtschutzmaßnahme im GRC-Wirkungsmodell 51

3 Treiber von IT-Compliance 53
3.1 Überblick 53
3.2 Historische Entwicklung der IT-Compliance 54
3.3 GoB und GoBD 60
3.4 Regelungsbedarf neue Technologien am Beispiel Cloud-Services 62
3.5 Fazit zum Thema Treiber der IT-Compliance 65

4 Rechtlicher Rahmen der IT-Compliance 67
4.1 Regulatorische Anforderungen an IT-Compliance 67
4.2 Normenhierarchie und Gültigkeit regulatorischer Anforderungen 73
4.3 Regulatorische Institutionen der IT-Compliance und deren Ziele 73
4.4 Diskussion der absoluten oder relativen Zielvorgaben sowie der Regelauslegung für Pflichtschutzmaßnahmen der IT-Compliance 81
4.5 Fazit zum rechtlichen Rahmen der IT-Compliance 84

5 IT-Compliance unter Einsatz der ISO 27000-Normenfamilie 87
5.1 Entwicklung der Normenfamilie und Verbreitung 87
5.2 Kurze Beschreibung des ISO-Standards 27001 und seiner Anwendung 89
5.3 Nutzen des ISO-Standards 27001 für das Management der IT-Compliance – Mapping externer Standards 93

5.4 Mapping des ISO-Standards 27001 auf die interne Dokumentation ... 97
5.5 Beurteilung des Einsatzes von Mappings auf ISO-Standard 27001 ... 99

6 IT-Compliance unter Einsatz von COBIT ... 101
6.1 Die Nutzung von COBIT als Governance Management-Standard ... 101
6.2 Entwicklung der ISACA und des Referenzmodells COBIT ... 102
6.3 Die COBIT-Kernprinzipien im Detail ... 105
6.4 Das COBIT-Prozessreferenzmodell im Detail ... 107
6.5 Mapping und Anwendung von COBIT für das IT-Compliance-Management ... 109
6.6 Fazit zum COBIT-Einsatz für die IT-Compliance ... 111

7 Kosten der IT-Compliance ... 115
7.1 Grundsätzliche Überlegungen zur Wirtschaftlichkeit von IT-Compliance ... 115
7.2 Anzahl der Anforderungen und Budgetwirkungen in der Praxis ... 117
7.3 Rentabilitätsanalyse ... 119
7.4 Fazit zur Wirtschaftlichkeits- und Nutzenbetrachtung ... 131

8 Management von IT-Compliance ... 133
8.1 Einleitung zum IT-Compliance Management System ... 133
8.2 IT-Compliance-Organisation (Aufbau- und Ablauforganisation) ... 136
8.3 Weitere Elemente der IT-Compliance-Organisation ... 140

9 Der IT-Compliance-Prozess ... 153
9.1 Gesamtprozess IT-Compliance ... 153
9.2 Identifikation und Analyse von regulatorischen Anforderungen ... 154
9.3 Zuordnung und Behebung von Kontrollschwächen ... 159
9.4 Berichterstattung über Compliance ... 160
9.5 Vorgehensmodell Initialprojekt IT-Compliance ... 161
9.6 Exkurs: Best Practice anhand der „Bankaufsichtlichen Anforderungen an die IT“ (BAIT) ... 167

10 Werkzeuge des (IT-)Compliance-Managements ... 171
10.1 Einsatz unternehmensübergreifender Standards ... 171
10.2 Compliance-Management-Software ... 177
10.3 Messen der Wirksamkeit des IT-Compliance-Management durch Benchmarking ... 191
10.4 Ergebnisse aus den Benchmarkstudien der IT Policy Compliance Group i. V. m. Reifegradmodellen ... 194

11 Wesentliche Maßnahmen der IT-Compliance ... 199
11.1 Managementansatz auf der Basis der wesentlichen Maßnahmen ... 199
11.2 Maßnahmen der IT-Compliance auf Basis der Motivatoren für IT-Sicherheit aus Unternehmenssicht ... 200
11.3 Maßnahmen der IT-Compliance auf Basis des Unified Compliance Framework (UCF) ... 201

11.4 Beschreibung der wesentlichsten IT-Sicherheitsmaßnahmen bzw. IT-Compliance-Anforderungen ... 207
11.5 IT-Sicherheit nach BSI-Leitfaden zur IT-Sicherheit ... 209
11.6 IT-Cyber Sicherheit nach CIS Critical Security Controls for Effective Cyber Defense (SANS 20) ... 212
11.7 Fazit zum Bereich der wesentlichen Maßnahmen der IT-Compliance ... 213

12 Outsourcing und IT-Compliance ... 215
12.1 IT-Outsourcing einschließlich Cloud Computing: Chance und Risiko ... 215
12.2 Reifegrad der IT und Auslagerungsfähigkeit ... 217
12.3 Umfang der Abhängigkeit vom Auslagerungsunternehmen und Maßnahmen zur Reduzierung ... 219
12.4 Nachweise der IT-Compliance bei Outsourcing/Cloud Computing ... 221
12.5 Compliance-Nachweise bei Outsourcing durch Wirtschaftsprüfer ... 223
12.6 Diskussion zum Thema Nachweis der IT-Compliance bei Outsourcing ... 225
12.7 Fazit zum Thema Outsourcing und IT-Compliance ... 226

13 Schlussbetrachtung und Ausblick ... 227

Anhang ... 229
A/1 Linkliste zu IT-Compliance ... 229
A/2 Übersicht IT-Compliance-Anforderungen des UCF ... 231
A/3 Beispiel für ein individuelles Mapping: ISO 27001 auf BaFin BAIT ... 257

Quellenverzeichnis ... 265

Stichwortverzeichnis ... 281

Autorenportraits ... 283