
ESV
ERICH
SCHMIDT
VERLAG

IT-Compliance

Erfolgreiches Management regulatorischer Anforderungen

Von
Dr. Michael Rath
Rainer Sponholz

2., neu bearbeitete 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
ESV.info/978 3 503 14458 7

1. Auflage 2009
2. Auflage 2014

Gedrucktes Werk: ISBN 978 3 503 14458 7
eBook: ISBN 978 3 503 14459 4

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: Strauss, Mörlenbach

Vorwort

Liebe Leser,

wir freuen uns sehr, Ihnen die grundlegend überarbeitete 2. Auflage unseres Buches über IT-Compliance präsentieren zu dürfen. Die Erstauflage erschien bereits 2009 und war damit – zumindest nach unserer Wahrnehmung – auf dem deutschen Markt das erste Buch zum Thema IT-Compliance.

Die Idee zu diesem Buch (Erstauflage) ist damals auf einer der ersten Konferenzen zum Thema „IT-Governance“ im Jahr 2005 in Berlin entstanden. Während dieser Konferenz wurde (unter Beteiligung der beiden Autoren) intensiv darüber diskutiert, wie man denn die Vielzahl „regulatorischer Anforderungen“ an die Datenverarbeitung im Unternehmen vorhandene Informationstechnologie (IT) erfassen und deren Einhaltung sicherstellen 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 überhaupt zu kennen und dauerhaft einzuhalten. Denn die Anforderungen reichten von so trivialen Vorgaben wie der Bildschirmarbeitsplatzverordnung über steuerrechtliche Regelungen für die Anerkennung elektronischer Rechnungen bis hin zu den komplexen datenschutzrechtlichen Anforderungen 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 ein Ergebnis dieser Debatte wurde festgestellt, dass sich nicht nur staatlich beaufsichtigte Branchen (bspw. Finanzdienstleistungssektor), 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 Mitarbeiterschutz gewährleistet sind.

Wie aber erhält man Kenntnis von den zahlreichen Anforderungen und wie priorisiert man deren Umsetzung? 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 Zielrichtungen zu verstehen. Zudem muss man einschätzen, wie „verbindlich" diese Regeln sind, ob sie also als formelles Gesetz (und ohne Handlungsalternativen) anzusehen sind oder ob 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. Bewusst werden daher auch die Einhaltung des Datenschutzes und die datenschutzspezifischen Gesetze eher am Rande dargestellt, denn hierzu gibt es bereits eine große Anzahl guter Literatur. Dieses Werk will zudem nicht (nur) die unterschiedlichen regulatorischen Anforderungen aneinander reihen 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 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. 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.

Ergänzt werden die Informationen durch Berichte von Praktikern aus IT-Compliance-Abteilungen unterschiedlicher Unternehmen sowie von Beratern in diesem Segment. In diesem Zusammenhang danken wir Herrn Thomas Knutzen von der Fa. Tanquid GmbH & Co. KG, Herrn Hartwig Laute von der Recommind GmbH, Herrn Dr. Markus Friesen von der Capgemini Consulting Österreich AG, Herrn Ralf Schneider von der TÜV Informationstechnik GmbH sowie den Herren Rüdiger Giebichenstein, Carsten Alexander Schirp und Dennis Hunstock von der WTS Consulting GmbH für ihre wertvollen Beiträge.

Weiterhin möchten wir Herrn Markus Gaulke von der KPMG AG Wirtschaftsprüfungsgesellschaft für die Erstellung und Aktualisierung des Kapitels 5 (IT-Compliance unter Einsatz von CobiT) danken. Besondere Anerkennung verdient weiterhin auch Herr Tobias Stähle für seine kritischen und zugleich konstruktiven Kommentare zur Erstausgabe. Unser Dank gilt weiterhin Frau Karin Thelemann, Präsidentin der ISACA Deutschland, und Frau Manuela Buck sowie Herrn Christian Kraft für ihre wertvollen Hinweise und Anregungen zur ersten Auflage.

Herrn Christoph Maiworm, wissenschaftlicher Mitarbeiter der Luther Rechtsanwaltsgesellschaft mbH, danken wir für die sorgfältige Aktualisierung im Rahmen der zweiten Auflage. Bei dieser Aktualisierung waren wir teilweise darauf angewiesen, manche Zitate oder Fundstellen unverändert aus der Erstauflage zu übernehmen, obwohl diese z.T. so nicht mehr auf einzelnen Webseiten verfügbar waren. Im Übrigen sollte dieses Werk aber den bei Drucklegung aktuellen Stand wiedergeben, auch wenn die einschlägigen Gesetze häufigen Änderungen unterliegen.

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 zu diesem Buch– sprechen Sie uns gerne an oder schreiben Sie uns eine E-Mail.

Dr. Michael Rath und Rainer Sponholz

Inhaltsverzeichnis