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

ISBN: 978 3 503 11093 3

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 Mitarbeiterschutz 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 Richtline 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 Praxisbesipiel 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