Sachs

GRC- Management- Governance, Risk and Compliance:

IT- Sicherheit als Bestandteil eines integrierten

*Compliance-Management*s

2. aktualisierte und erweiterte Auflage

Fabian Sachs, LL.M., D.D.F. (Grenoble)

GRC- Management-
Governance, Risk and Compliance:
IT- Sicherheit als Bestandteil eines integrierten Compliance- Managements

GRC- Management- Governance, Risk and Compliance: IT- Sicherheit als Bestandteil eines integrierten Compliance- Managements

2. aktualisierte und erweiterte Auflage 2020

Autor: Fabian Sachs
Umschlaggestaltung, Illustration: Huong Tran
Lektorat: Detlef Sachs

Verlag & Druck: tredition GmbH, Halenreie 40-44, 22359 Hamburg

ISBN 978-3-347-18699-6 (Paperback)

ISBN 978-3-347-18700-9 (Hardcover)

ISBN 978-3-347-18701-6 (e-Book)

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie, detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Printed in Germany

Hinweis für die Nutzung des Werkes:

Erkenntnisse in der Informationstechnologie, als auch gesetzliche und nichtgesetzliche Anforderungen unterliegen einem laufenden Wandel durch Forschung und Entwicklung, der Rechtsprechung und Weiterentwicklung des Rechts bzw. einschlägiger Standards und Frameworks. Der Autor hat nach großer Sorgfalt darauf geachtet, dass die im Werk aufgeführten rechtlichen Angaben dem derzeitigen Wissenstand entsprechen. Es entbindet daher dem Nutzer keineswegs von seiner Verpflichtung anhand weiterer Informationsquellen dies zu überprüfen, ob die im Buch gemachten Angaben mit den dortigen gemachten Angaben abweichen. Der Nutzer sollte in eigener Verantwortung seine Entscheidung entsprechend treffen.

Haftungsausschluss für gemachte Internetverweise
In diesem Buch wurden Links (Internetverweise) zu Seiten im Internet hinterlegt. Hierbei gilt für all diese Links, dass der Autor keinerlei Einfluss für die Inhalte oder Gestaltung der verlinkten Seiten hat. Daher kann für diese fremden Inhalte auch keinerlei Gewähr übernommen werden. Es ist für die Inhalte der verlinkten Seiten immer der jeweilige Betreiber oder der Anbieter der Seite verantwortlich. Zum Zeitpunkt der Links wurden diese vom Autor auf etwaige Rechtsverstöße hin überprüft. Dabei waren zu diesem Zeitpunkt keine rechtswidrigen Inhalte erkennbar. Die stetige inhaltliche Kontrolle der in diesem Buch aufgeführten Links zu den entsprechenden Seiteninhalten ist ohne spezifische Anhaltspunkte einer Rechtsverletzung ohnehin nicht zumutbar. Derartige Links werden vom Autor bei Bekanntgabe entsprechend umgehend entfernt. Der Autor distanziert sich daneben ausdrücklich von allen Inhalten aller Seiten, die in diesem Buch aufgeführt sind.

Für meine Eltern

Vorwort

Zielgruppe dieses Buches sind Beschäftigte, Akademiker und Fachkräfte, welche sich mit der IT- Sicherheit und dem Datenschutz auseinandersetzen und in Unternehmen an einem GRC-Management beteiligt sind. Dieses Buch soll Ihnen einen Einblick in das Thema GRC- Management geben, um neben der Schaffung einer höheren Akzeptanz zum Thema Datenschutz und Datensicherheit auf Managementebene auch eine Etablierung im Unternehmen in die Wege leiten zu können. Unter dem Thema GRC-Management: IT- Sicherheit als Bestandteil eines integrierten Compliance- Managements fallen ganz unterschiedliche Disziplinen, wie z.B. die Informationstechnologie, betriebswirtschaftliche Aspekte, als auch nationales, europäisches und internationales Recht. Daneben existieren noch eine Vielzahl an unterschiedlichen Regelungen im nichtgesetzlichen Bereich, die es zu beachten gilt.

Die zweite aktualisierte und erweiterte Auflage wurde vollständig überarbeitet. Aufgrund der entstandenen Praxisrelevanz und aktueller Gesetzgebung wurde das Thema Datenschutz erheblich erweitert. Darüber hinaus wurde das Thema COBIT und das IT-Sicherheitsmanagement ergänzt. Zusätzliche Informationen und Hilfestellungen zum Vertragsmanagement innerhalb der Informationstechnologie runden, ebenso wie die Bereiche Pandemie und Datenschutz, die Aktualisierung ab.

Für die zahlreichen Anregungen und Wünsche der Leserschaft möchte ich mich herzlich Bedanken. Ein ganz besonderer Dank gilt meinem Vater, der sich für dieses doch nun etwas umfangreicheres Werk die Zeit des fachlichen Lektorats genommen hat, als auch meiner Lebensgefährtin Huong Tran, die sich der Gestaltung des Buchumschlages passioniert angenommen hat.

Ich hoffe Ihnen mit diesem Buch einen umfassenden Einblick zu ermöglichen und begrüße Anregungen und konstruktive Kritik sehr. Sie können mir diese gerne mit dem Betreff Buchkritik GRC an fabian_sachs@email.de via E-Mail zukommen lassen.

Abschließend wünsche ich Ihnen viel Freude bei dieser Lektüre.

Fabian Sachs, LL.M., D.D.F. (Grenoble)

Bad Salzig, München November 2020

Inhaltsverzeichnis

Abkürzungsverzeichnis

A.a.O.	am angegebenen Ort
Abb.	Abbildung
Abs.	Absatz
AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AG*	Amtsgericht
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
Anm.	Anmerkung
AO	Abgabenordnung
APT	Advanced Persistent Threat
ArbGG	Arbeitsgerichtsgesetz
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BayLDA	Bayerischen Landesamtes für Datenschutzaufsicht
BCM	Business Continuity Management
BCR	Binding Corporate Rules

Bd.	Band
BetrVG	Betriebsverfassungsgesetz
BeckOK	Beck'scher Online-Kommentar
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BSA	Business Software Alliance
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzgl.	bezüglich
bzw.	beziehungsweise
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analyse
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BIOS	Basic Input Output System
BZRG	Bundeszentralregistergesetz
ca.	circa
CD	Compact Disc
CDs	Compact Discs
CEO	Chief Executive Officer
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection