

Sachs

GRC- Management- Governance, Risk and Compliance:

IT- Sicherheit als Bestandteil eines integrierten

Compliance-Managements

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***

© 2020 Sachs, Fabian
Theodor-Hoffmann-Platz 15, 56154 Boppard

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, Halenreihe 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)

Das Werk, einschließlich seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung ist ohne Zustimmung des Verlages und des Autors unzulässig. Dies gilt insbesondere für die elektronische oder sonstige Vervielfältigung, Übersetzung, Verbreitung und öffentliche Zugänglichmachung.

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	IX
A. Entwicklung von IT- Bedrohungen	1
I. Industrie 4.0	3
II. Folgen der Vernetzung	3
B. GRC- Management- Governance, Risk and Compliance: IT- Sicherheit als Bestandteil eines integrierten Compliance- Managements	7
I. GRC- Management: Governance, Risk and Compliance	8
1. Governance	9
1.1 Gesetzliche Anforderungen	11
a) Sarbanes-Oxley Act (SOX).....	11
b) EuroSOX	15
c) Datenschutzrechtliche Grundlagen	18
aa) Verwendung von Cookies.....	19
bb) Rechtliche Stellung der Datenschutzgrundverordnung (DSGVO)	23
cc) Notwendigkeit eines Datenschutzbeauftragten.....	25
dd) Verarbeitung von personenbezogenen Daten innerhalb der EU	32
ee) Verarbeitung von personenbezogenen Daten außerhalb der EU/EWR.....	33
ff) Verarbeitung von EU/EWR- personenbezogenen Daten in den USA	35
gg) Bereitstellung von Webseiten	53
hh) Kundenstammdaten und die Verwendung bei Webseiten	54
ii) Nutzungsdaten bei Webseiten.....	55

jj) Aufklärung neben der Datenschutzerklärung	56
kk) Informations- und Aufklärungspflichten an Mitarbeiter	56
ll) Datensicherheit nach DSGVO	57
mm) One Stop Shop (OSS) nach DSGVO	58
nn) Beschäftigtendatenschutz	59
oo) Auskunftersuchen an Betriebsräte	62
d) Folgen bei Nichtbeachtung des Datenschutzes	64
e) Meldeanforderungen nach DSGVO	71
f) Datenschutzfolgeabschätzung nach DSGVO	72
g) Benachrichtigung betroffener Personen nach DSGVO	73
h) Durchführung von Penetrationstests nach DSGVO	73
i) Privacy by Design nach DSGVO	73
j) Privacy by Default nach DSGVO	74
k) Datenlöschung nach DSGVO	75
l) Übermittlung zwischen Konzernunternehmen	75
m) Datennutzung für die Compliance-tätigkeiten	77
aa) Beteiligung des Betriebsrates	77
bb) Kommunikation gegenüber Mitarbeitern	78
cc) Nutzung von personenbezogenen Daten bei internen Ermittlungen	79
n) Planung in datenschutzrechtlicher Hinsicht	81
aa) Analyse bereits bestehender Strukturen	83
bb) Gap-Analyse	83
cc) Verarbeitungsverzeichnis	83
dd) Zweckänderung und -festlegung	85
ee) Löschkonzepte	86

ff) Recht auf Vergessenwerden	89
gg) Recht auf Datenübertragbarkeit	89
hh) Recht auf Verarbeitungseinschränkung.....	89
ii) Recht auf Auskunft	90
jj) Recht auf Berichtigung.....	91
kk) Widerspruchsrecht.....	92
ll) Gemeinsam für die Verarbeitung Verantwortliche	92
mm) Auftragsverarbeitung innerhalb der EU und EWR	92
aaa) Weitere Auftragsverarbeiter	94
bbb) Pflichten des Auftragsverarbeiter	95
ccc) Verhaltensregeln	96
nn) Auftragsverarbeitung außerhalb der EU und EWR (Drittland)	97
oo) Datenschutzfolgeabschätzung.....	104
pp) Umgang mit Datenpannen	108
qq) Datenschutz und Pandemien	109
o) Anforderungen nach Basel II, III.....	116
p) Gesetzliche Behandlung der Korruption in Deutschland	117
aa) Gesetz über Ordnungswidrigkeiten	118
bb) Strafgesetz	118
cc) Einkommenssteuergesetz	119
q) Gesetzliche Behandlung der Korruption in den USA	119
r) Gesetzliche Behandlung der Korruption im Vereinigten Königreich	122
s) Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)	123

t) Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG)	124
u) Aktiengesetz (AktG)	126
v) Lizenzmanagement	127
w) Lizenzen und Urheberrecht	128
1.2 Regelungen im nichtgesetzlichen Bereich	130
a) IDW-Standards	130
b) Deutscher Corporate Governance Kodex (DCGK)	130
c) OECD Principles of Corporate Governance	132
d) Framework in der IT- Governance (ISACA, ITGI)	132
e) ISO/IEC 2700x	134
aa) Management in der Informationssicherheit gem. ISO/IEC 27001 (ISMS)	135
bb) Code of Practice gem. ISO/IEC 27002	136
cc) Risikomanagement in der Informationssicherheit gem. ISO/IEC 27005	137
dd) Datenschutz gem. ISO/IEC 27018	138
f) IT- Grundsatzkatalog des BSI	138
g) CobiT Framework im IT-Bereich der strategisch-unternehmerischen Managementebene	139
h) COSO	142
i) Val IT	143
j) IT-Grundsätze (Policies) und deren praxisgerechte Implementierung	143
2. Risk	144
2.1 Akteure	147
2.2 Risiken in der Informationstechnologie	148
2.3 Risikobestimmung	152

a) Potenzielle Risiken und Risikoarten	153
b) Datendiebstahl.....	159
aa) Datendiebstahl von Microsoft Windows-Systemen	161
bb) Datendiebstahl von Linux-Systemen.....	161
cc) Hacking.....	162
dd) Malware	163
ee) Botnetze	164
ff) Denial of Service (DoS)	165
gg) Phishing	165
hh) Social Media	166
ii) Keylogger	166
jj) Risiko USB-Schnittstelle	167
kk) Risiko WLAN	169
ll) Risiko bei SCADA- Systemen	169
c) Eintrittswahrscheinlichkeit und deren Konsequenzen.....	171
d) Probleme bei subjektiver Einschätzung der Risiken und deren Bewertung	173
2.4 Grundlagenmethoden des Risikomanagements	173
a) Berechnungsverfahren zur Analyse und Darstellung der Risiken	174
aa) Risiko- und Risikobewertungsmatrix.....	174
bb) Risikoportfolio und die Kriterien zur Einstufung des möglichen Schadens.....	178
cc) Risikokatalog.....	181
b) Bestimmungen zur Ausführung von Informationen	182
2.5 Methoden im Bereich des IT-Risikomanagements	182
a) Analyse von Schwachstellen.....	185

b) Ergreifung von Maßnahmen.....	186
aa) Maßnahmen zum Schutz personenbezogener Daten	186
bb) Schutz der Beschäftigtendaten.....	188
bb) Patchmanagement und Virenschutz	190
cc) Netzwerkmonitoring.....	195
dd) EDV-Sicherungen	197
ee) E-Mail und Internetnutzung	199
ff) Technische Vorgaben zum Lizenzmanagement.....	200
gg) Überprüfung der umgesetzten Maßnahmen	200
hh) Methodendidaktik CRAMM.....	201
ii) Fehlermöglichkeits- und Einflussanalyse.....	204
2.6 Risiko Korruption.....	205
2.7 Moralische Risiken	206
3. Compliance.....	208
3.1 Sicherheitskonzepte bei unternehmerischer Infrastruktur	215
3.2 Notfallplan.....	223
a) Business Continuity Management (BCM).....	224
b) Umsetzung des BCM	224
3.3 Präventive Schadensminimierung durch Vertragsmanagement	226
II. Praktische Anwendung des GRC	228
1. Unternehmensbezogener Lösungsansatz am Praxisbeispiel SAP	229
2. Outsourcing.....	231
2.1 Cloud Computing.....	234
2.2 Sicherheitsrisiken bei Cloud Computing	241
3. Nutzung von PIA für die Datenschutzfolgeabschätzung	242
C. Schlusswort	243

Anlage 1: Mögliche „Tools“ zur Schadensauslösung	XXII
Anlage 2: Risikomanagement in der Informationssicherheit gem. ISO/IEC 27005.....	XXV
Anlage 3:CobiT-Prozess	XXVI
Anlage 4: COSO Internal Control-Integrated Framework	XXVII
Anlage 5: Schadeneinstufungskriterium.....	XXVIII
Anlage 6: Schadenszenarieneinstufung	XXIX
Anlage 7: ISO-Begriffe zu ISO/IEC Guide 73:2009: Riskmanagement- Principles and guidelines	XXX
Anlage 8: Beispiele einer Risikomatrix.....	XXXI
Anlage 9: Musterformular zur Einschätzung von IT-Bedrohungen ..	XXXIII
Anlage 10: CRAMM-RISK-Matrix	XXXIX
Anlage 11: CRAMM-Asset-Modul.....	XL
Anlage 12: IT-Notfallplanung bei Bedrohung- und Ereignis.....	XLI
Anlage 13: IT-Outsourcing und Complianceanforderungen	XLIII
Anlage 14: Compliancennachweise	XLIV
Anlage 15: Schwachstellenanalyse bei Cloud Computing	XLVI
Anlage 16: Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern (Standarddatenschutzklausel 2010/87/EU)	XXLVIII
Anlage 17: Alternativen Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (Set II Standarddatenschutzklausel 2004/915/EC).....	LXXIII
Anlage 18: Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (Standarddatenschutzklausel 2001/497/EG)	XCIV
Quellenverzeichnis	CXIII
Literaturverzeichnis	CXIII

Aufsätze	CXVI
Urteile.....	CXIX
Internetverzeichnis.....	CXX
Zum Autor.....	CXXXV

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