Inhaltsverzeichnis

Vorwort.....

Abkürzungsverzeichnis VII

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 8
1.1 Gesetzliche Anforderungen..... 10
a) Sarbanes-Oxley Act (SOX)..... 11
b) EuroSOX 14
c) Datenschutzrechtliche Grundlagen 17
d) Folgen bei Nichtbeachtung des Datenschutzes 28
e) Meldeanforderungen nach DSGVO 31
f) Datenschutzfolgeabschätzung nach DSGVO 31
g) Benachrichtigung betroffener Personen nach DSGVO 32
h) Durchführung von Penetrationstests nach DSGVO 32
i) Privacy by Design nach DSGVO 32
j) Datenlöschung nach DSGVO 33
k) Anforderungen nach Basel II, III..... 33

l) Gesetzliche Behandlung der Korruption in Deutschland 35
aa) Gesetz über Ordnungswidrigkeiten 35
bb) Strafgesetz 35
cc) Einkommenssteuergesetz 36
m) Gesetzliche Behandlung der Korruption in den USA 36
n) Gesetzliche Behandlung der Korruption im Vereinigten Königreich 40
o) Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) 40
p) Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) .. 41
q) Aktiengesetz (AktG) 43
r) Lizenzmanagement 44
s) Lizenzen und Urheberrecht 45
1.2 Regelungen im nichtgesetzlichen Bereich 47
a) IDW-Standards 47
b) Deutscher Corporate Governance Kodex (DCGK) . 48
c) OECD Principles of Corporate Governance 49
d) Framework in der IT- Governance (ISACA, ITGI) . 50
e) ISO/IEC 2700x 51
aa) Management in der Informationssicherheit gem. ISO/IEC 27001 (ISMS) 52
bb) Code of Practice gem. ISO/IEC 27002 53

cc) Risikomanagement in der Informationssicherheit gem. ISO/IEC 27005 54
dd) Datenschutz gem. ISO/IEC 27018 55
f) IT- Grundschutzkatalog des BSI 55
g) CobiT Framework im IT-Bereich der strategisch-unternehmerischen Managementebene 56
h) COSO 57
i) Val IT 58
j) IT-Grundsätze (Policies) und deren praxisgerechte Implementierung 58
2. Risk 59
2.1 Akteure 61
2.2 Risiken in der Informationstechnologie 63
2.3 Risikobestimmung 65
a) Potenzielle Risiken und Risikoarten 67
b) Datendiebstahl 72
aa) Datendiebstahl von Microsoft Windows-Systemen 74
bb) Datendiebstahl von Linux-Systemen 75
cc) Hacking 76
dd) Malware 77
ee) Botnetze 78
ff) Denail of Service (DoS) 78
gg) Phising 79
hh) Social Media 79

ii) Keylogger 80
jj) Risiko USB-Schnittstelle 81
kk) Risiko WLAN 82
ll) Risiko bei SCADA- Systemen 83
c) Eintrittswahrscheinlichkeit und deren Konsequenzen 84
d) Probleme bei subjektiver Einschätzung der Risiken und deren Bewertung 86
2.4 Grundlagenmethoden des Risikomanagements 87
a) Berechnungsverfahrungen zur Analyse und Darstellung der Risiken 87
aa) Risiko- und Risikobewertungsmatrix 88
bb) Risikoportfolio und die Kriterien zur Einstufung des möglichen Schadens 91
cc) Risikokatalog 94
b) Bestimmungen zur Ausführung von Informationen 95
2.5 Methoden im Bereich des IT-Risikomanagements 95
a) Analyse von Schwachstellen 98
b) Ergreifung von Maßnahmen 99
aa) Maßnahmen zum Schutz personenbezogener Daten 99
bb) Patchmanagement und Virenschutz 100
cc) Netzwerkmonitoring 104
dd) EDV-Sicherungen 106
ee) E-Mail und Internetnutzung 108

ff) Technische Vorgaben zum Lizenzmanagement 109
gg) Überprüfung der umgesetzten Maßnahmen 109
hh) Methodendidaktik CRAMM 110
ii) Fehlermöglichkeits- und Einflussanalyse 114
2.6 Risiko Korruption 115
2.7 Moralische Risiken 116
3. Compliance 117
3.1 Sicherheitskonzepte bei unternehmerischer Infrastruktur 122
3.2 Notfallplan 131
II. Praktische Anwendung des GRC 131
1. Unternehmensbezogener Lösungsansatz am Praxisbeispiel SAP 132
2. Outsourcing 134
2.1 Cloud Computing 137
2.2 Sicherheitsrisiken bei Cloud Computing 144
C. Schlusswort 146
Anlage 1: Mögliche „Tools“ zur Schadensauslösung XVI
Anlage 2: Risikomanagement in der Informationssicherheit gem. ISO/IEC 27005 XIX
Anlage 3: CobiT-Prozess XX
Anlage 4: COSO Internal Control-Integrated Framework ... XXI
Anlage 5: Schadeneinstufungskriterium XXII
Anlage 6: Schadenszenarieneinstufung XXIV
Anlage 7: ISO-Begriffe zu ISO/IEC Guide 73:2009: Risk management- Principles and guidelines XXV

Anlage 8: Beispiele einer Risikomatrix XXVI

Anlage 9: Musterformular zur Einschätzung von IT-Bedrohungen XXVII

Anlage 10: CRAMM-RISK-Matrix XXXIV

Anlage 11: CRAMM-Asset-Modul XXXV

Anlage 12: IT-Notfallplanung bei Bedrohung- und Ereignis XXXVI

Anlage 13: IT-Outsourcing und Compliance-anforderungen XXXVIII

Anlage 14: Compliancenachweise XL

Anlage 15: Schwachstellenanalyse bei Cloud Computing XLII

Quellenverzeichnis XLIV
Literaturverzeichnis XLIV
Aufsätze XLVI
Urteile XLVIII
Internetverzeichnis XLIX

Zum Autor LXII