

Inhaltsverzeichnis

1 Ziel des Leitfadens IT-Compliance.....	9
2 Einführende Überlegungen zur IT-Compliance im Mittelstand	10
2.1 Digitalisierung als Trend und Treiber der IT-Compliance im Mittelstand	10
2.2 IT-Compliance im Mittelstand.....	12
2.3 Die Rolle des Wirtschaftsprüfers im digitalen Wandel.....	15
3 Abgrenzung der IT-Compliance sowie deren Bedeutung für Unternehmen und Wirtschaftsprüfer.....	19
3.1 Definition und übergreifendes Ziel der IT-Compliance	19
3.2 Übersicht der IT-Compliance-Vorgaben.....	21
3.3 Abgrenzung der IT-Compliance	25
3.3.1 Abgrenzung zwischen „Compliance von IT“ und „Compliance durch IT“	25
3.3.2 Abgrenzung zwischen IT-Governance, IT-Risikomanagement und IT-Compliance	28
3.4 Bedeutung der IT-Compliance für mittelständische Unternehmen	31
3.4.1 Normkonformität als Pflicht für Unternehmen und Geschäftsleitung	31
3.4.2 Gesteigerte Qualität und Transparenz von IT-Prozessen und IT-gestützten Geschäftsprozessen...	40
3.4.3 Einhaltung von datenschutzrechtlichen Vorgaben.....	42
3.4.4 Stärkung der IT-Sicherheit (inkl. Know-how-Schutz)....	47
3.4.5 Abbau von IT-Risiken.....	50
3.4.6 Mittel- und langfristiger Wettbewerbsvorteil, sowie Erhöhung des Unternehmenswertes	50
3.5 Bedeutung der IT-Compliance für den Wirtschaftsprüfer	52

4 IT-Compliance-Leitfaden für den Wirtschaftsprüfer im Mittelstand	55
4.1 Praxisnahe Anleitung für die schrittweise Durchführung von IT-Prüfungen.....	55
4.1.1 Grundsätzliche Überlegungen vor Beginn der Prüfung.....	55
4.1.2 Schritt 1: Definieren von Zielsetzung und Art der Prüfung	57
4.1.3 Schritt 2: Heranziehen ausgewählter IT-Compliance-Vorgaben.....	59
4.1.4 Schritt 3: Erheben und Bewerten von mandantenspezifischen Basisinformationen zur Ableitung möglicher Risiken.....	60
4.1.5 Schritt 4: Festlegen und Durchführen der Prüfungshandlungen sowie Beurteilung des Prüfungsergebnisses.....	62
4.1.6 Schritt 5: Erstellen und Abstimmen des IT-Prüfungsberichts und ggf. Sensibilisierung zu Handlungsbedarfen.....	69
4.1.7 Schritt 6: Follow-up-Prozess als optionaler Schritt zur Qualitätssicherung.....	74
4.2 Probleme und Risiken typischer Schwachstellen der IT im Mittelstand und abgeleitete Handlungsempfehlungen für die IT-Prüfung	76
4.2.1 Einleitende Hinweise.....	76
4.2.2 Mangelhafte oder fehlende IT-Strategie.....	77
4.2.3 Mangelndes oder nicht wirksames IT-Compliance-Managementsystem.....	83
4.2.4 Kein ausgeprägtes IT-Risikomanagement	84
4.2.5 Fehlende organisatorische Verortung von IT-Aufgaben.....	89
4.2.6 Fehlende Kontrolle über Auslagerungen	96
4.2.7 Unzureichende Vorbereitung auf Informationssicherheitsbedrohungen	104
4.2.8 Vernachlässigung physischer Sicherheit	113

4.2.9 Vernachlässigte Benutzerberechtigungsverwaltung (inkl. Funktionstrennungsverletzung).....	119
4.2.10 Ungenügende Kontrolle von Zugriff durch mobile Endgeräte	130
4.2.11 Unsystematische Datensicherung und Archivierung ..	134
4.2.12 Unzureichende IT-Betriebsüberwachung ..	144
4.2.13 Fehlende Überwachung von Anwendungskontrollen..	148
4.2.14 Selbstgemachte Handlungsunfähigkeit bei Notfällen/Systemausfällen.....	151
4.2.15 Belassen von Standard-Grundeinstellungen.....	157
4.2.16 Intransparenter Umgang mit Anwendungsänderungen (Changes).....	159
4.2.17 Nicht nachvollziehbare Migrationen.....	167
4.2.18 Technische Probleme bei der Erstellung von Datenextrakten	175
4.2.19 Lücken in der Verfahrensdokumentation	178
4.2.20 Unsachgemäßes Umgang mit Hard- und Software.....	182
4.2.21 Unkontrollierbarkeit durch Schatten-IT.....	185
4.2.22 Geringe Erfahrung im Umgang mit neuen Vorgaben ...	192
4.3 Anregungen für die IT-Compliance-Beratung.....	194
4.3.1 Beratung beim Beheben von Schwachstellen.....	194
4.3.2 Proaktive IT-Compliance-Beratung außerhalb bestehender Schwachstellen.....	195
4.4 Exkurs: Referenzmodelle in der IT-Compliance	198
5 Zusammenfassung: Ein abschließender Blick auf die IT-Compliance im Mittelstand	201

6 Verzeichnisse.....	204
6.1 Glossar.....	204
6.2 Abkürzungsverzeichnis.....	208
6.3 Abbildungsverzeichnis.....	211
6.4 Tabellenverzeichnis.....	211
6.5 Literatur.....	211
6.6 Ausgewählte Standards und Regelwerke.....	216