

---

Praxistipps IT

# Leitfaden IT-Compliance

Anforderungen, Chancen und  
Umsetzungsmöglichkeiten

Diana Nestler / Julian Modi  
2. Auflage

Inklusive  
Downloads



IDW VERLAG GMBH

# Ihr Zugang zum Download-Bereich von „Leitfaden IT-Compliance“

Folgende Schritte sind zur Freischaltung erforderlich:

1. Melden Sie sich mit Ihren Zugangsdaten im IDW Internetportal an.  
Falls Sie noch keine Zugangsdaten besitzen, führen Sie bitte zunächst eine Erstregistrierung durch.
2. Unter **[www.idw.de/idw-verlag](http://www.idw.de/idw-verlag)** > **Produkt Updates** > **Leitfaden IT-Compliance** geben Sie bitte anschließend den unten abgedruckten Freischaltcode in die dafür vorgesehene Box ein.

Nun stehen Ihnen nach jedem Einloggen Zusatzinformationen zum Buch als Download zur Verfügung.



Freischalt-Code:

---

Praxistipps IT

# Leitfaden IT-Compliance

Anforderungen, Chancen und  
Umsetzungsmöglichkeiten

Diana Nestler / Julian Modi  
2. Auflage



IDW VERLAG GMBH

Das Thema Nachhaltigkeit liegt uns am Herzen:



## 2. Auflage

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne vorherige schriftliche Einwilligung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verbreitung in elektronischen Systemen. Es wird darauf hingewiesen, dass im Werk verwendete Markennamen und Produktbezeichnungen dem marken-, kennzeichen- oder urheberrechtlichen Schutz unterliegen. Die automatisierte Analyse des Werkes, um daraus Informationen insbesondere über Muster, Trends und Korrelationen gemäß § 44b UrhG („Text und Data Mining“) zu gewinnen, ist untersagt.

© 2024 IDW Verlag GmbH, Tersteegenstraße 14, 40474 Düsseldorf

Die IDW Verlag GmbH ist ein Unternehmen des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW).

Satz: Reemers Publishing Services GmbH, Krefeld  
Druck und Bindung: C.H.Beck, Nördlingen  
KN 12110

Die Angaben in diesem Werk wurden sorgfältig erstellt und entsprechen dem Wissensstand bei Redaktionsschluss. Da Hinweise und Fakten jedoch dem Wandel der Rechtsprechung und der Gesetzgebung unterliegen, kann für die Richtigkeit und Vollständigkeit der Angaben in diesem Werk keine Haftung übernommen werden. Gleichfalls werden die in diesem Werk abgedruckten Texte und Abbildungen einer üblichen Kontrolle unterzogen; das Auftreten von Druckfehlern kann jedoch gleichwohl nicht völlig ausgeschlossen werden, so dass für aufgrund von Druckfehlern fehlerhafte Texte und Abbildungen ebenfalls keine Haftung übernommen werden kann.

ISBN 978-3-8021-2937-7

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://www.d-nb.de> abrufbar.

Coverfoto: [www.istock.com/Govindanmarudhai](http://www.istock.com/Govindanmarudhai)

[www.idw-verlag.de](http://www.idw-verlag.de)

# Inhaltsverzeichnis

<b>1</b>	<b>Ziel des Leitfadens IT-Compliance</b> .....	<b>9</b>
<b>2</b>	<b>Einführende Überlegungen zur IT-Compliance im Mittelstand</b> .....	<b>10</b>
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
<b>3</b>	<b>Abgrenzung der IT-Compliance sowie deren Bedeutung für Unternehmen und Wirtschaftsprüfer</b> .....	<b>19</b>
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

<b>4</b>	<b>IT-Compliance-Leitfaden für den Wirtschaftsprüfer im Mittelstand .....</b>	<b>55</b>
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 Unsachgemäßer 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
<b>5 Zusammenfassung: Ein abschließender Blick auf die IT-Compliance im Mittelstand .....</b>	<b>201</b>

<b>6 Verzeichnisse.....</b>	<b>204</b>
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

Eine ausgeprägte IT-Compliance bietet einen großen **strategischen Vorteil**, der zur langfristigen Sicherheit und **Wettbewerbsfähigkeit** eines Unternehmens beiträgt. Die **Einhaltung von IT-Compliance-Richtlinien** ist daher für mittelständische Unternehmen von entscheidender Bedeutung. Dafür ist es unerlässlich, die aktuellen **Anforderungen** zu kennen, potenzielle **Risikofelder** zu identifizieren und die vorgegebenen **Regelungen** zu berücksichtigen.

Die Inhalte in der Übersicht:

- Definition der IT-Compliance und die Bedeutung für das Unternehmen und den Wirtschaftsprüfer
- Anleitung und Tipps für die Durchführung von IT-Prüfungen
- Übersicht über die Anforderungen der IT-Compliance für den Mittelstand
- Hinweis auf typische Schwachstellen und Risiken bei IT-Prüfungen
- Vergleich mit Referenzmodellen in der Praxis

Dieser Leitfaden ist unverzichtbar für Wirtschaftsprüfer in der Prüfung und Beratung, aber auch für Führungskräfte, IT-Verantwortliche und Compliance-Beauftragte im Mittelstand, die sicherstellen möchten, dass ihre IT-Infrastruktur den höchsten Standards entspricht und zugleich **geschäftlichen Erfolg** fördert.



IDW VERLAG GMBH

ISBN 978-3-8021-2937-7

Preis: 54,00 € (D)

[www.idw-verlag.de](http://www.idw-verlag.de)



9 783802 129377