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 > 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:

IDW VERLAG GMBH

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

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

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

www.idw-verlag.de

1 Ziel des Leitfadens IT-Compliance

Ziel dieses Leitfadens ist es, Wirtschaftsprüfern einen praxisnahen Einstieg in die IT-Compliance im Mittelstand zu geben. Aufbauend auf einer vorangehenden Begriffsabgrenzung wird die Bedeutung der IT-Compliance für mittelständische Unternehmen und den Wirtschaftsprüfer aufgezeigt.

Es wird dargelegt, wie eine IT-Prüfung unter Einhaltung der Anforderungen aus gesetzlichen, regulatorischen und verbandsspezifischen Vorgaben Schritt-für-Schritt vorgenommen werden kann. Gleichzeitig werden typische Schwachstellen in der Umsetzung der IT-Compliance und ihre Bedeutung in der Prüfung behandelt. Für diese gibt dieser Leitfaden dem Wirtschaftsprüfer ausgewählte Handlungsempfehlungen an die Hand.

Abschließend werden spezifische Anregungen zur IT-Beratung im Hinblick auf die Konzeption und Gestaltung geeigneter Compliance-Maßnahmen gegeben, deren Ausgangspunkt mögliche Schwachstellen in der IT des Unternehmens sind. So werden Möglichkeiten aufgezeigt, wie der Mandant hinsichtlich der Entwicklungen von IT-Compliance-Anforderungen beraten werden kann.

Hinweis:
Dieser Leitfaden richtet sich primär an die Anforderungen mittelständischer Produzenten und Dienstleister in Deutschland. Explizit wird darauf hingewiesen, dass für ausgewählte Branchen darüber hinausgehende spezifische IT-Compliance-Vorgaben bestehen und in jeweiligen Prüfungen/Beratungen zwingend berücksichtigt werden müssen (bspw. MaRisk und BAIT sowie jeweilige EBA-Guidelines für Kreditinstitute oder NIS-2 für kritische Anlagen sowie wichtige und besonders wichtige Einrichtungen).

2 Einführende Überlegungen zur IT-Compliance im Mittelstand

2.1 Digitalisierung als Trend und Treiber der IT-Compliance im Mittelstand

Digitale Technologien durchdringen jeden Bereich des gesellschaftlichen und ökonomischen Lebens. Vernetzte IT-Systeme bestimmen sämtliche Geschäftsprozesse und Handlungsabläufe im unternehmerischen Alltag – etwa in Form von integrierten ERP-Systemen, Logistik-Steuerungssystemen, Supply-Chain-Managementsystemen, Robotic Process Automation oder im Bereich von Cloud Computing[1].

Gerade für den in diesem Leitfaden betrachteten Mittelstand gewinnen digitale Technologien zunehmend an Bedeutung, um nicht nur die Leistungsfähigkeit erhalten zu können, sondern letztendlich Wettbewerbsvorteile auf dem nationalen und internationalen Markt zu schaffen. Es lassen sich neue Geschäftsmodelle entwickeln und Betriebe können effizienter, schneller und kostengünstiger arbeiten. Die IT wird mehr und mehr zum zentralen Nervensystem eines jeden Unternehmens.

Der Megatrend der Digitalisierung erweist sich einerseits als Schlüssel zum wirtschaftlichen Erfolg. Andererseits stellen die zunehmend komplexen modernen Technologien mittelständische Unternehmen vor erhebliche Herausforderungen. Neben der effektiven technischen und organisatorischen Implementierung von IT-Systemen sind sie verpflichtet, sich mit immer komplexer werdenden Rahmenbedingungen auseinanderzusetzen. Dies betrifft insbesondere die umfassende Einhaltung der IT-Compliance, die für eine ordnungsgemäße Unternehmensführung unerlässlich ist. Je mehr neue innovative Technologien entwickelt werden und den Markt beeinflussen und damit einhergehende Risiken hervorbringen, desto mehr Vorgaben werden von gesetzlicher, regulatorischer und auch unternehmensinterner Seite gestellt. So soll eine Kontrolle und zugleich Beherrschbarkeit technologischer Innovationen gewährleistet werden können. Dies bedeutet für Unternehmen, dass mit zunehmender Digitalisierung der Umfang, der relevanten zu beachtenden Regelwerke (rechtlich/extern/intern) gleichsam steigt, was wiede-

[1] Knorr/Bredendiek/Knoche (2023)

3.2 Übersicht der IT-Compliance-Vorgaben

Die Quellen für die IT-Compliance-Anforderungen werden in Anlehnung an Klotz wie folgt definiert:

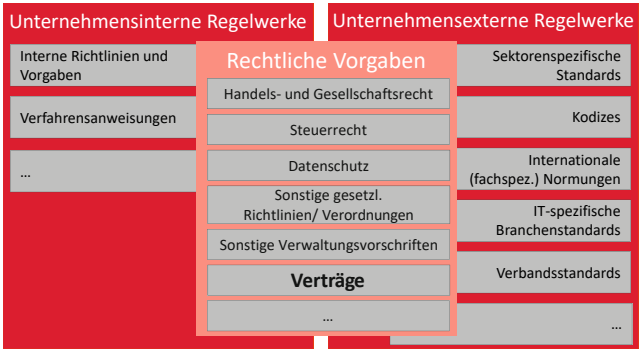

Abb. 3.1: Quellen der IT-Compliance[16]

Unternehmensinterne Regelwerke umfassen Vorgaben aus dem Unternehmen selbst, wie bspw. Sicherheitsleitlinien oder Richtlinien zum Umgang mit der IT für Mitarbeiter. Diese sind nicht immer zwingend von außen reglementiert und werden vom Unternehmen selbst festgelegt. Oft jedoch setzen Unternehmen externe Regelwerke und rechtliche Vorgaben in internen Regelwerken um bzw. konkretisieren und operationalisieren diese für sich.

Unternehmensexterne Regelwerke umfassen Vorgaben von bestimmten Verbänden, Branchen oder allgemeinen Normen und Kodizes. Diese haben an sich keinen bindenden gesetzlichen Charakter, sind jedoch aufgrund ihrer Etablierung am Markt trotzdem für das Unternehmen empfehlenswert bzw. werden im Falle der IDW-Standards im Rahmen von Abschlussprüfungen auch verpflichtend.

Rechtliche Vorgaben sind zwingend einzuhalten. Sie beeinflussen inhaltlich sowohl die Gestaltung von unternehmensinternen als auch unternehmensexternen Regelwerken. Dabei handelt es sich im We-

[16] Vgl. Klotz (2009), S. 4

sentlichen um Gesetze, Rechtsverordnungen, Rechtsprechung und Verwaltungsvorschriften, allerdings auch um Verträge mit Kunden, Lieferanten und sonstigen Vertragspartnern, soweit IT-relevante Vereinbarungen enthalten sind.

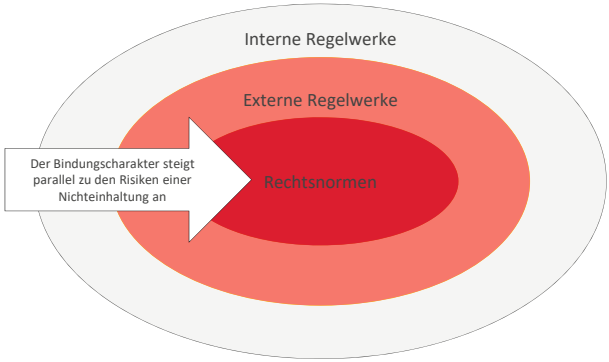

Abb. 3.2: Zwiebelmodell der IT-Compliance-Anforderungen[17]

Für den Wirtschaftsprüfer ist es wichtig, diese Dreiteilung der Quellen von IT-Compliance zu kennen und in seiner Herangehensweise beim Mandanten zu verinnerlichen, um die Anforderungen entsprechend zu kategorisieren und die Auswirkungen in der Prüfung und Beratung bewerten zu können.

In der folgenden Tabelle wird eine Übersicht der bestehenden Vorgaben im Umfeld der IT-Compliance gegeben (**Tab. 3.1**). Die Anforderungen müssen für die jeweils betroffenen Unternehmen (abhängig von deren Geschäftstätigkeit) auf Relevanz geprüft und entsprechend berücksichtigt werden.

[17] Vgl. Klotz (2009), S. 21

Quelle der Vorgaben[18] und betroffene Sektoren		Maßgebliche Regularien/Regelwerke
Rechtliche Vorgaben (Gesetzliche bzw. behördliche Vorgaben)	Handels- und Gesellschaftsrecht	– HGB, AktG, EHUG, UMAG, KonTraG, GmbHG, BilMoG, IFRS
	Steuerrecht	– AO, UStG, KStG, GewStG, EStG
	Datenschutz	– DS-GVO, BDSG, TMG, TKG, TTDSG – EU-US Data Privacy Framework
	Sonstige Gesetze, Richtlinien und Verordnungen	– BetrVG, UWG, GWB, SGB, SRVwV, BGB, VwVfG, StGB, IT-NetzG, NetzDG, IWG, KONSENS-G, BSIG, BSI-KritisV, GeschGehG, ArbStättVO – TRIPS, TT-GVO – IASB, IAS, IFRS, IFRIC, EU-Anti-Terror-VO, NIS2-RL, CRA, Sektorspezifische IT-Sicherheitsgesetze wie z.B. DORA
	Sonstige Verwaltungsvorschriften	– BildschirmarbeitsVO, BITV 2.0, Elektronische-TransaktionenVO, EVB-IT, GoBD
	Rechtsprechung	Höchstrichterliche Rechtsprechung des BGH (z.B. BGH, Urt. v. 27.04.2022 – Az. 5 StR 278/21; Urt. v. 09.05.2017 – Az. 1 StR 265/16 zur bußgeldmindernden Berücksichtigung eines CMS bei der Bußgeldbemessung). Rechtsprechung der Oberlandes- und Landesgerichte (z.B. OLG Hamm, Urt. v. 01.12.2003 – Az. 13 U 133/03 zum Mitverschulden beim Datenverlust).
	Verträge	– Sämtliche Verträge zur IT-Leistungserstellung (Lizenzierung, Entwicklung und Betrieb) – Vertragsdetails zu Servicelevels (SLA, OLA) – Spezifische Regelungen zu ausgelagerten IT-Aktivitäten (inkl. Cloud Computing: SaaS, PaaS, IaaS) – Vertragliche Regelungen zur Nutzung von IT-Hardware (bspw. Rechenzentren) – Allgemeine Verträge mit denkbarem Bezug zur IT, etwa Geheimhaltungsvereinbarungen (NDA), Verträge über die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter (AVV)

[18] Vgl. Klotz (2009), S. 4

Quelle der Vorgaben[18] und betroffene Sektoren		Maßgebliche Regularien/Regelwerke
Externe Vorgaben (insbes. Selbstregulierung/ Good Practice)	Kodizes	– Deutscher Corporate Governance Kodex, OECD Principles of Corporate Governance
	Internationale (fachspezifische) Normungen	– ISO/IEC 27001, ISO/IEC 37301, ISO/IEC 38500, ISO/IEC 20000, ISO/IEC 22301
	IT-spezifische Branchenstandards	– BSI IT-Grundschutz-Kompendium – Leitfaden IT-Sicherheit des BSI
	Verbandsstandards	– ISA 31519, IDW PS 850 n. F., IDW PS 860, IDW PS 880 n. F., IDW PS 951 n. F. – IDW RS FAIT 1, IDW RS FAIT 2, IDW RS FAIT3, IDW RS FAIT 4, IDW RS FAIT 5 – Prüfungsstandards des ISACA (bspw. ITAF)
Interne Vorgaben (Sonstige Vorgaben)	Interne Richtlinien und Vorgaben	IT-Sicherheitskonzept, Passwortrichtlinie, IT-Risikomanagement, Datensicherungskonzept, Archivierungskonzept, Konzept zur physischen Sicherheit, Berechtigungskonzept
	Verfahrensanweisungen	Verfahrensdokumentation, technische Dokumentationen, Anwenderhandbücher

Tab. 3.1: Nationale und internationale Vorgaben im Umfeld der IT-Compliance

Praxistipp:
Es existieren zahlreiche Anforderungen, darunter auch viele branchenspezifische Normen und Standards. Diese vielfältigen Anforderungen sollten vom Wirtschaftsprüfer in enger Zusammenarbeit mit dem Mandanten sorgfältig analysiert werden, um sämtliche relevante Aspekte abzudecken. Hierbei ist es äußerst hilfreich, ein umfassendes Normenregister heranzuziehen, um sicherzustellen, dass alle relevanten Vorschriften und Best Practices berücksichtigt werden. Darüber hinaus ist es entscheidend, Überschneidungen und Synergien zwischen den verschiedenen Anforderungen zu identifizieren. Dies ermöglicht nicht nur eine effizientere Implementierung, sondern auch die Maximierung der geschäftlichen Vorteile, die sich aus der Einhaltung dieser Anforderungen ergeben können. Externe Regelwerke können beispielsweise effektiv und langfristig umgesetzt

[19] Die ISA ermöglichen eine harmonisierte Prüfung und erleichtern den Vergleich von Prüfungsergebnissen über Ländergrenzen hinweg. Dies ist besonders wichtig für multinationale Unternehmen und Investoren.

Zwischen Governance, Risikomanagement und Compliance besteht eine starke Wechselwirkung (siehe **Abb. 3.3**).

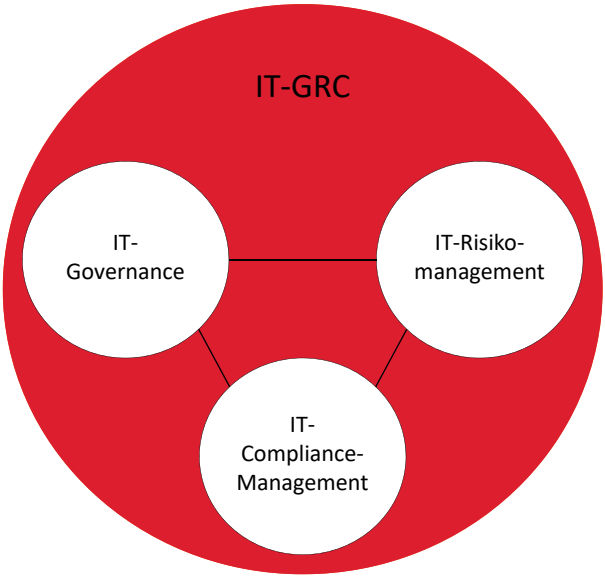

Abb. 3.3: IT-Governance, IT-Risikomanagement und IT-Compliance Management[23]

IT-Governance dient der wertorientierten und nachhaltigen Steuerung und Entwicklung der IT. Sie legt die Grundwerte der Unternehmensführung und damit der IT fest, bspw. mittels einer IT-Strategie, welche auch dafür sorgt, dass IT-Risiken im Unternehmen angemessen, systematisch und zyklisch identifiziert, analysiert, bewertet und behandelt werden und IT-Compliance-Vorgaben umgesetzt werden. In der Regel erfolgt dies durch eine Verantwortungsregelung und Verteilung von Entscheidungsrechten im Unternehmen.[24]

IT-Risikomanagement auf der anderen Seite steigert ein erhöhtes IT-Risikobewusstsein auch für nachhaltige Entscheidungen auf der strategischen Ebene und reduziert gleichzeitig mögliche IT-Compliance-Verstöße.

[23] Vgl. Klotz/Dorn (2008), S. 7
[24] Vgl. Klotz (2020), S. 854 f.

IT-Compliance stärkt die strategische Ebene durch Konformität und führt gleichzeitig zu einer erhöhten Betrachtung des IT-Risikos. Sowohl IT-Governance, IT-Risikomanagement, als auch IT-Compliance haben wesentliche Auswirkungen auf die Ausgestaltung der IT eines Unternehmens.[25]

Beispiel

Erreichen eines Dreiklangs der IT-Governance, IT-Risikomanagement und IT-Compliance im Unternehmen

In einem mittelständischen Unternehmen ist die IT-Landschaft durch eine Vielzahl an Softwareanbietern und selbstentwickelten Lösungen geprägt. Kontrollen werden zum Großteil in der IT manuell durchgeführt. Unternehmensleitung und IT haben nur marginale Berührungspunkte, bspw. wenn bestimmte IT-Anwendungen beschafft werden müssen. Die IT-Governance ist grundsätzlich getrennt von der allgemeinen Unternehmens-Governance und zeigt sich durch unterschiedliche IT-Strategieansätze in IT-Projekten und IT-Organisation. Das IT-Risikomanagement ist in Form einer „Brandbekämpfung" nur reaktiv aufgebaut und die IT-Compliance wird nur in Ansätzen durch die Mitarbeiter der IT beachtet, zumal die Menge an Vorschriften mit dem vorhandenen IT-Personal nicht umsetzbar ist.

In der Prüfung des Wirtschaftsprüfers werden erhebliche Mängel aufgrund der fehlenden Einhaltung der IT-Compliance deutlich. Der IT-Leiter teilt dem Wirtschaftsprüfer daraufhin mit, „wenn das für die Prüfung benötigt wird, können die Nachweise (IT-Dokumentationen, Protokolle etc.) gerne zusammengestellt bzw. eingerichtet werden". Das Unternehmen nimmt daraufhin die Nachdokumentation vor.

Das Unternehmen kann zunehmend nicht mehr der aktuellen Bedrohungslage gerecht werden, da fast alle Maßnahmen der IT durch die Führungsebene nicht unterstützt werden und Projekte, die durch die Führungsebene in der IT umgesetzt werden sollen, implementierte (Sicherheits-)Maßnahmen gefährden. Weiterhin werden immer mehr IT-Compliance-Verstöße verzeichnet, die bereits zu negativen Folgen (wie Strafen) und Reputationsverlust geführt haben. Die eigens für

[25] Knoll (2013), S. 7

den Wirtschaftsprüfer zusammengestellten IT-Compliance-Nachweise werden in der Unternehmenspraxis nicht aktiv genutzt.

Auf Anraten des Wirtschaftsprüfers möchte das Unternehmen den GRC-Dreiklang herstellen. Hierzu wird ein Umdenken der Geschäftsführung notwendig. Die IT wird zukünftig als wichtiger Teilbereich des Unternehmens wahrgenommen und aktiv in die strategische Planung und Steuerung eingebunden. Auf dieser Grundlage kann eine IT-Governance-Struktur geschaffen werden, die die Unternehmensziele auch in der IT widerspiegelt. Ein neu entwickeltes IT-Risikomanagement befasst sich aktiv mit dem Umgang identifizierter Risiken und gibt wesentliche Handlungsimpulse in Richtung IT-Governance. Die Einhaltung von IT-Compliance-Vorgaben wird fortan als wesentliche Aufgabe der IT-Abteilung definiert und aktiv nachgehalten. Dies trägt wesentlich zur Reduktion von IT-Risiken bei, rückt die IT-Abteilung gleichsam mehr in den Fokus der Verantwortung. Bereits nach wenigen Wochen nehmen Management und Mitarbeiter das effektive GRC-Zusammenspiel und dessen positive Effekte auch auf die gesamten Unternehmensprozesse wahr.

Für den Wirtschaftsprüfer ist es wichtig, dass IT-Compliance nicht allein zu betrachten ist, sondern eng mit der IT-Governance und dem IT-Risikomanagement verknüpft ist. Dadurch ermöglicht eine integrierte Betrachtung der drei Sichtweisen Synergieeffekte für die Unternehmen zu generieren. IT-Compliance verfolgt niemals einen Selbstzweck.

3.4 Bedeutung der IT-Compliance für mittelständische Unternehmen

3.4.1 Normkonformität als Pflicht für Unternehmen und Geschäftsleitung

Primär obliegt dem Unternehmen als solches die Pflicht, gesetzliche Vorgaben sowie geltende sonstige Normen und Regularien einzuhalten. Es muss dafür Sorge tragen, dass die unternehmerischen Aktivitäten in einer Art und Weise organisiert sind, dass bestimmte Regeln eingehalten und wesentliche Verstöße hiergegen verhindert werden. Für eine ordnungsgemäße Unternehmensführung trägt wiederum die Geschäftsleitung die Verantwortung. Besteht sie aus mehreren Personen im Sinne einer Gesamtgeschäftsführung, gilt der Grundsatz der Gesamtverantwortung.

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 möchte, 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