Praxistipps IT

Leitfaden IT-Compliance

Anforderungen, Chancen und Umsetzungsmöglichkeiten

Diana Nestler / Julian Modi

IDW VERLAG GMBH

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 KRITIS für Unternehmen mit kritischen Infrastrukturen, u. a. Energieversorger).

2 Einführende Überlegungen zur IT-Compliance im Mittelstand

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

Digitale Technologien durchdringen zunehmend jeden Bereich des gesellschaftlichen und ökonomischen Lebens. Vernetzte IT-Systeme bestimmen mehr und mehr 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 Digitalisierung scheint einerseits Schlüssel für wirtschaftlichen Erfolg zu sein. Andererseits stellen die modernen Technologien mit zunehmender Komplexität gerade mittelständische Betriebe vor erhebliche Herausforderungen. Neben der effektiven technischen und organisatorischen Implementierung von IT-Systemen kommen sie nicht umhin, sich mit immer vielschichtiger werdenden Rahmenbedingungen, besonders hinsichtlich der einzuhaltenden IT-Compliance, für eine ordnungsgemäße Unternehmensführung zu beschäftigen.

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 zunehmen-

[1] Schulke/Jütte (2018)

der Digitalisierung der Umfang, der zu beachtenden relevanten Regelwerke (rechtlich/extern/intern) gleichsam steigt, was wiederum nicht unerhebliche Auswirkungen technischer, organisatorischer und letztlich personeller Natur haben kann. Für den Mittelstand bis dato oft vernachlässigte Regelungen werden nun bedeutender denn je (bspw. die Einführung angemessener technischer und organisatorischer Maßnahmen zum Schutz von personenbezogenen Daten gemäß der seit 2018 anzuwendenden EU-Datenschutzgrundverordnung (DS-GVO) bzw. zur Aufrechterhaltung der IT-Sicherheit nach den Vorgaben des BSI).

Der Trend der Digitalisierung treibt so zwangsläufig die Entwicklung der (IT-)Compliance dynamisch voran.

Hinweis:
Die Zunahme von digital gestützten Datenverarbeitungsprozessen führte beispielsweise auch zur breiten Befassung der Politik mit dem Thema Datenschutz. Ein Ergebnis daraus ist die DS-GVO und ein neues Bundesdatenschutzgesetz (BDSG).

Ein geeignetes Compliance-System, das nachweislich auf die Beachtung eines regel- bzw. rechtskonformen Verhaltens ausgerichtet ist, dient nicht nur der Vermeidung zunehmender potentieller Haftungsrisiken und Schadensersatzforderungen gegenüber dem Unternehmen und der Unternehmensleitung. Vielmehr können hierdurch Vertrauen und Reputation gegenüber Mitarbeitern, Kunden und sonstigen Geschäftspartnern gesichert und gefördert werden. Letztlich können Compliance-Strategien im Falle eines regelwidrigen Verhaltens zur Abwendung oder Minimierung straf- und ordnungsrechtlicher Konsequenzen führen.

Zusammenfassend lässt sich feststellen, dass die IT-Compliance aufgrund zunehmender Digitalisierung und damit einhergehenden innovativen Technologien zum Dreh- und Angelpunkt in jedem mittelständischen Unternehmen wird und stetig an Bedeutung gewinnt.

2.2 IT-Compliance im Mittelstand

Die Digitalisierung schreitet unaufhaltsam voran, so auch im Mittelstand. Häufig laufen mittelständische Unternehmen dem Digitalisierungstrend dennoch hinterher. Sie sind, aufgrund praktischer und

finanzieller Gegebenheiten oft weniger in der Lage, stetig auf dem aktuellsten Stand der technischen Möglichkeiten zu stehen.

Hinweis:
Der deutsche Mittelstand ist hinsichtlich der Digitalisierungsbemühungen sehr unterschiedlich aufgestellt. Verschiedene Studien zeigen zwar einen zunehmenden Einsatz von innovativen Technologien in mittelständischen Betrieben, jedoch ist deren Verbreitung nicht mit der in Großunternehmen in Deutschland vergleichbar[2]. Besonders Unternehmen des verarbeitenden Gewerbes haben Schwierigkeiten dabei, die Möglichkeiten, die ihnen die Digitalisierung bietet, in ihrem Betrieb vollumfänglich auszuschöpfen[3]. Dagegen sind reine Dienstleister oder Handelsunternehmen schon weiter. Aufgrund von Kundenanforderungen, haben hier innovative Technologien vermehrt Einzug gehalten (besonders hinsichtlich Kundenakquise/-service sowie des digitalen Datenaustauschs mit Kunden und Lieferanten)[4].

Die Umsetzung digitaler Prozesse findet gerade bei kleinen und mittelständischen Betrieben mitunter kurzfristig und ohne nachhaltige strategische Überprüfung statt. Gesetzliche oder sonstige regulatorische Maßstäbe finden im Vorfeld häufig kaum Berücksichtigung. Diese Handlungsweise erscheint fahrlässig und kann langfristig zu erheblichen Problemen führen.

Je vielschichtiger digitale Datenverarbeitungsprozesse stattfinden, umso mehr nimmt auch die Gefährdungslage für die Datensicherheit zu. Vertrauliche Unternehmensdaten, angefangen von sensiblen Mitarbeiter- oder Kundendaten über Preiskalkulationen, Zahlen und Daten über neue Geschäftsmodelle oder Unternehmensstrategien bis hin zu Angaben über innovative Entwicklungen, Erfindungen oder sonstiges Unternehmens-Know-how, durchlaufen heute schnell eine Vielzahl unterschiedlicher Endgeräte, Schnittstellen, Serverstrukturen, interner und externer Speichermedien. Der Datenfluss über mehrere interne und externe digitale Infrastrukturen hinweg, ohne angemessene Risi-

[2] z. B. Bitkom (2017), Bitkom (2019), KfW Research (2019), Ernst & Young GmbH (2018)
[3] Vgl. Bitkom (2017)
[4] Vgl. Bundesministerium für Wirtschaft und Energie (2018)

kobetrachtung und hinreichenden technischen und organisatorischen Sicherheitsmaßnahmen, geht indes zwangsläufig mit einer Zunahme von Gefahren für die Übermittlung, Speicherung und Verarbeitung von Daten einher. IT-Systeme werden angreifbarer, je umfangreicher Datenverarbeitungsvorgänge werden, Anwendungen können fehlerhafte Ergebnisse liefern oder ganz ausfallen, Daten können gelöscht werden oder verloren gehen, manipuliert oder gestohlen werden.

Der Bedarf an angemessenen Regeln zum korrekten und sicheren Umgang mit Daten sowie zur Nutzung der IT nimmt dementsprechend zu, ganz gleich, ob es sich um Gesetze, daraus abgeleitete Rechtsnormen oder sonstige Standards oder Richtlinien handelt, die ein Unternehmen zu erfüllen hat. Durch neue Rechtsakte des Gesetzgebers und die höchstrichterliche Rechtsprechung oder maßgebliche Leitlinien der Behörden erweitern sich damit kontinuierlich die einzuhaltenden Pflichten.

In Anbetracht der bereits existierenden, nur schwer überschaubaren Vorgaben, deren Zusammenspiel zudem nicht immer homogen erscheint, sondern die vielmehr oft nicht ohne weiteres miteinander vereinbar sind, haben Unternehmen häufig Schwierigkeiten dabei, diese rechtlich und regulatorisch korrekt anzuwenden. Dies wiederum kann zu potenziellen Sicherheitslücken und Haftungsszenarien führen.

Gleichsam wächst die Verantwortung der Unternehmen und der Geschäftsleitung. Merklich rückt auch das Thema IT-Compliance von mittelständischen Unternehmen zunehmend in den Fokus der Öffentlichkeit (sei es in Fachtagungen, Fachpublikationen und sogar den allgemeinen Medien[5]).

Oft sieht man im Mittelstand auch, dass sich Unternehmen zwar intensiv mit Compliance-Vorschriften befassen, die nachhaltige Verfolgung einer langfristigen IT-Compliance-Strategie jedoch kaum Beachtung findet.

Die Vielzahl an Anforderungen muss zudem mit der vorhandenen Organisationsstruktur harmonisiert werden, was zusätzlich zu Problemen führen kann, besonders in alteingesessenen mittelständischen Unternehmen. Dem Wirtschaftsprüfer kann hierbei eine wichtige Schlüsselrolle zuteilwerden.

[5] Vgl. Klotz (2009)

Hinweis:

Das Feld der zu betrachtenden IT-Compliance-Regelungen ist nicht nur groß und unübersichtlich; es unterliegt auch einer steten Veränderungsdynamik. Im Mittelstand fehlt zum Teil das Bewusstsein für die Notwendigkeit und auch die finanziellen Mittel einer dem Digitalisierungstrend entsprechenden IT-Compliance-Strategie. Häufig werden Digitalisierungsprojekte durchgeführt, ohne an die Folgen für die Einhaltung existierender Anforderungen zu denken. Der unmittelbare gesetzliche bzw. regulatorische Druck für die Beachtung wirkt sich oft erst nachgelagert aus (bspw. externe Betriebsprüfungen, Umsatzsteueraußenprüfungen, Kapitalertragssteuerprüfungen, Umsatzsteuernachschau, Datenschutzprüfung, Abschlussprüfung).

IT-Compliance wird häufig als zwingende Anforderung und nicht als Chance zur proaktiven Umsetzung von Verbesserung der operativen Abläufe angesehen.[6] An sich geltende Maßstäbe für ein ordnungsgemäßes unternehmerisches Handeln, insbesondere ausgerichtet auf einen sicheren Umgang mit Unternehmensdaten/personenbezogenen Daten, werden immer wieder außer Acht gelassen. In Folge dessen werden mittelständische Unternehmen auch häufiger Opfer von Angriffen.[7]

2.3 Die Rolle des Wirtschaftsprüfers im digitalen Wandel

Mit der zunehmenden Bedeutung der Digitalisierung in den mittelständischen Unternehmen steigt gleichzeitig der Bedarf nach zielgerichteter Prüfung und Beratung.

Je mehr Anpassungen und Neuerungen durch moderne Informationstechnologien im Unternehmen durchgeführt werden (müssen), desto komplexer ist auch der Beratungsbedarf mit Blick auf gesetzliche und sonstige regulatorische Anforderungen im Zusammenhang mit der IT. Gleichzeitig steigt die Bedeutung der Bewertung von IT im Rahmen von Prüfungen. Dies muss sich auch in einer weiterentwickelten Prüfungslogik und -technik widerspiegeln. Die Gewichtung der IT-bezogenen Prüfungshandlungen gemessen an den Gesamtprüfungshandlungen

[6] Vgl. Sollis (2010), S. 1 f.
[7] Fissenewert (2018), S. 34 f.

erhöht sich und wird damit hinsichtlich der Prüfungssicherheit wesentlich für das Ergebnis der Prüfung. Zudem gibt es immer mehr Prüfungen, die sich insbesondere mit IT-Prozessen und -Systemen befassen, bspw. Prüfungen nach IDW PS 860, IDW PS 880 und IDW PS 951.

Dem Wirtschaftsprüfer wird in diesem Konstrukt eine besondere Rolle zuteil. Aufgrund seiner methodischen und analytischen Expertise sowie Erfahrungen aus u. a. Abschlussprüfungen, Assurance-Leistungen und Beratungen, besitzt dieser einen umfassenden Einblick in verschiedenste Formen der Digitalisierung in einem weiten Feld an Geschäftsmodellen und Branchen. Einhergehend mit seinem Know-how bezüglich der in diesen unterschiedlichen Umgebungen einzuhaltenden (IT-) Compliance, macht es ihn zu einem wichtigen Partner für das Unternehmen und verknüpft damit die Bereiche IT und Compliance sowohl in der Prüfung als auch in der Beratung.

Meist sind Wirtschaftsprüfer über einen mehrjährigen Zeitraum für ein Unternehmen zuständig und kennen sich daher tiefgehend mit den aktuellen Abläufen sowie laufenden/zukünftigen Veränderungen im Unternehmen aus. Dieses Wissen kann der Wirtschaftsprüfer nutzen, um in Prüfungen Risikofelder, die sich aus einer zunehmenden Digitalisierung und erweiterten Anforderungen hinsichtlich der (IT-)Compliance ergeben, zu identifizieren. Für die Bewertung des Prüfungsrisikos ist es mit zunehmender technischer Komplexität der Unternehmensprozesse von großer Bedeutung auch alle rechnungslegungsrelevanten Systeme mit einzubeziehen, um die Ordnungsmäßigkeit auch nach berufsrechtlichen Anforderungen gewährleisten zu können.

In Beratungssituationen wird es mit zunehmendem Einsatz der IT immer wichtiger, Synergien zwischen bestehenden und neuen digitalen Geschäftsprozessen zu knüpfen, damit innovative Technologien effektiv im Unternehmen und unter Berücksichtigung relevanter rechtlicher und regulatorischer Vorgaben Einzug erhalten. Der Wirtschaftsprüfer ist damit ein Wissensträger für interne Geschäftsprozesse des Unternehmens und kann dies mit seinem Compliance-Know-how verbinden.

Hinweis:
Es gibt mittelständische Unternehmen, welche als führende Treiber der Digitalisierung marktbestimmend sind. Diese Mandanten kann der Wirtschaftsprüfer mit seinen Compliance-Know-how betreuen und ihnen beratend zur Seite stehen.

Daneben existiert auch eine große Anzahl an Mittelständlern, die zwar ihr Kerngeschäft sehr gut beherrschen, jedoch mit Digitalisierung nur geringfügig Berührung haben und sich dennoch IT-technisch weiterentwickeln müssen und dies auch möchten. Der Wirtschaftsprüfer kann auf dem herausfordernden Weg bei der Einführung neuer Technologien und zugleich Einhaltung damit verbundener (IT-)Compliance-Anforderungen unterstützen. Hier kann es auch die Aufgabe des Wirtschaftsprüfers sein, den Mandanten Digitalisierungsmöglichkeiten im Rahmen der vorhandenen Mittel zur Verbesserung und Stabilisierung der Geschäftsprozesse und IT-Compliance aufzuzeigen.

Unternehmen profitieren auch von der Vernetzung der Wirtschaftsprüfer untereinander, bspw. über Verbände und Arbeitsgruppen. Der Wirtschaftsprüfer hat dadurch einen sehr guten Einblick in Veränderungen, sowohl im Bereich der IT-Entwicklungen als auch in der Weiterentwicklung der (IT-)Compliance-Anforderungen. Dies ermöglicht es ihm, frühzeitig seine Mandanten über Neuerungen zu informieren und seine Prüfungs- wie Beratungsleistungen entsprechend auszurichten.

Für ein Unternehmen ist der Wirtschaftsprüfer häufig eine Vertrauensperson. Denn die Tätigkeiten des Wirtschaftsprüfers beruhen auf der Befolgung der berufsrechtlichen, ethischen Normen, zu denen insbesondere Unabhängigkeit, Transparenz, Gewissenhaftigkeit, Verschwiegenheit und Eigenverantwortlichkeit gehören. Die Einführung innovativer Technologien und Prozesse kann mit Begleitung des Wirtschaftsprüfers auch hinsichtlich der Einhaltung externer Anforderungen sichergestellt werden.

Praxistipp:
Der Wirtschaftsprüfer ist angehalten, die Anforderungen aus der Vielzahl an externen (IT-)Compliance-Vorgaben seinem Mandanten verständlich zu vermitteln. Häufig ist der Wirtschaftsprüfer der einzige Ansprechpartner für das mittelständische Unternehmen hinsichtlich Fragestellungen der IT-Compliance. Auch sollte der Wirtschaftsprüfer des zu betreuenden Unternehmens bei Einsatz neuer Technologien immer direkt auf die Auswirkungen bzgl. der IT-Compliance hinweisen, um Negativfolgen zu vermeiden. Hilfreich kann hierbei sein, die Bedeutung der Compliance-Anforderungen für das Unternehmen herauszustellen (siehe Kapitel 3.4), um die negativen Folgen der Nichteinhaltung und gleichzeitig die zahlreichen Vorteile der Befolgung von Compliance-Anforderungen zu verdeutlichen bzw. die Risiken aus dem Bestehen von Schwachstellen hervorzuheben (siehe Kapitel 4.2).

Weit verbreitet ist die Annahme, dass sich der Wirtschaftsprüfer zwar mit Compliance-Anforderungen auskennt, jedoch keine oder geringe IT-Kenntnisse aufweist. Dieses Bild ändert sich jedoch zunehmend. Mit steigender Digitalisierung muss sich auch die Kompetenz des Wirtschaftsprüfers verändern. Es besteht die Anforderung an den Wirtschaftsprüfer, alle Bereiche des Unternehmens und dessen Zusammenhänge sowie Abhängigkeiten zu verstehen und angemessen zu bewerten. Die IT gewinnt an Bedeutung; sie vernetzt mitunter immer mehr verschiedene Geschäftsbereiche, insbesondere in mittelständischen Unternehmen. Immer mehr Wirtschaftsprüfer nutzen daher die Angebote des IDW oder anderer Anbieter, um ihr IT-Know-how auszubauen und die Brücke zwischen Compliance und innovativen Informationstechnologien schlagen zu können.

Praxistipp:
Der Wirtschaftsprüfer sollte sich mit den aktuellen Trends der Digitalisierung und die damit verbundenen IT-Compliance-Anforderungen auseinandersetzen, um die Mandanten angemessen beraten zu können. Hierfür bieten sich Fachliteratur, Digitalblogs und Newsletter ausgewiesener Fachgruppen (bspw. ISACA) sowie Fachtagungen/ Fortbildungsangebote an.

Zusammenfassend zeichnet sich die besondere Rolle des Wirtschaftsprüfers dadurch aus, dass er sich in den letzten Jahren, aufgrund seines Know-hows und seiner Erfahrungen, zu einem Bindeglied und Mediator zwischen den rechtlichen und regulatorischen Anforderungen einerseits und den Herausforderungen der technischen Innovationen andererseits etabliert hat und dadurch zunehmend ein wichtiger Partner bei den Digitalisierungsbestrebungen seiner Mandanten wird.