05.13

8. Jahrgang
Oktober 2013
Seiten 193 – 240

ZRFC

Risk, Fraud & Compliance

www.ZRFCdigital.de

Prävention und Aufdeckung durch Compliance-Organisationen

ESV ERICH SCHMIDT VERLAG

64683

Keywords:
Compliance
CMS
IDW PS 980
Überwachung
Qualitäts-management
Verbesserung

Compliance-Verbesserung im Sinne IDW PS 980

Qualitätssicherung zu Compliance im Unternehmen

RA Dr. Christian Schefold*

Die Risiken wurden analysiert, die Ziele sind gesteckt und die Maßnahmen wurden definiert. Eine Compliance-Organisation steht für die Umsetzung sowie die fortwährende Begleitung von Compliance im Unternehmen bereit. Neben der Kommunikation sind Überwachung und Verbesserung ein wesentlicher Teil der Compliance-Maßnahmen. Deswegen haben die Autoren des IDW Prüfungsstandards 980 der Überwachung und Verbesserung als Optimierung von Compliance ebenfalls ein eigenes Element gewidmet. Dabei aber sollte aus der Sicht einer Compliance-Organisation dieses Element eher „Überwachung zur Verbesserung" heißen. Ein Compliance-Management-System (CMS) kann schnell recht umfangreich und komplex werden. Dann heißt es: Übersicht bewahren, Komplexität reduzieren und Qualitätsmanagement betreiben.

1. Einleitung

Am 11. März 2011 hat das Institut der Deutschen Wirtschaftsprüfer (IDW) den Prüfungsstandard PS 980 verabschiedet. Danach sollen Konzeption, Angemessenheit, Implementierung und Wirksamkeit eines CMS durch Prüfung von sieben Grundelementen festgestellt werden: Kultur, Ziele, Risiken, Programm, Organisation, Kommunikation und Überwachung.[1] Nach einer Risikoanalyse war es angebracht, die Richtung für Compliance im Unternehmen vorzugeben. Vollständig ist ein Compliance-Management-System erst, wenn es selbst auch seine eigene Effektivität und Effizienz prüfen und mit darauf aufbauenden Optimierungsmaßnahmen immer auf einem aktuellen und auch wirkungsvollen Stand bleiben kann. Dabei spielt die Kommunikation – wie überall bei Compliance – auch beim Compliance-Qualitätsmanagement eine hervorgehobene Rolle. Die Rückmeldung über Compliance-Vorfälle und den erreichten Compliance-Status (den Erfolg bei der Umsetzung des Compliance-Programms zur Erreichung der Compliance-Ziele) an Geschäftsleitung und Compliance-Organisation ist für die Wirksamkeit von Compliance im Unternehmen entscheidend. Ein Qualitätsmanagement dient der Verbesserung des Compliance-Status' und soll eine laufende Anpassung aller übrigen Compliance-Grundelemente sicherstellen. Eine erfolgreiche Überwachung ist ebenfalls von essentieller Bedeutung für die Wirksamkeit von Compliance und daher – obwohl eigentlich Teil des Compliance-Programms – ein eigenes Grundelement.[2]

Dr. Christian Schefold

Die Autoren des IDW-Standards PS 980 fordern eine stete Überwachung der Angemessenheit und Wirksamkeit eines CMS: Schwachstellen oder gar Regelverstöße müssen dazu führen, dass etwaige Mängel des CMS beseitigt werden und eine (Qualitäts-)Verbesserung des Systems erfolgt. Aber es ist nicht allein kriminelle Phantasie, die die Wirksamkeit eines CMS in Frage stellt. Auch neue Entwicklungen im Unternehmen sowie neue Geschäftsstrategien führen immer wieder zu aktuell ändernden Anforderungen für Compliance. Defizite wachsen gerade dann, wenn bestehende und bewährte Risikomanagement-Systeme nicht mehr an aktuelle Gegebenheiten angepasst werden. Hier bedarf es der Aufmerksamkeit gegenüber weiteren Anforderungen – sowohl unternehmensimmanent als auch von außen (z. B. aus der Entwicklung der Gesetzgebung). Wichtig ist zudem der kritische Blick auf mögliche Defizite des bestehenden Systems (z. B. erkannte Schwächen) und auch auf Neuentwicklungen in der Wirtschaft (etwa über *Peer-Review* oder *Benchmarking* gegenüber anderen Unternehmen).

2. Darf Compliance überhaupt ein CMS überwachen?

Dabei haben die IDW-Autoren die Anforderungen für die Überwachung und Verbesserung von Compliance allerdings eher aus der Sicht der Internen Revision und der Wirtschaftsprüfung formuliert. Wichtig ist nach den Vorgaben des Standards insbesondere die Unabhängigkeit einer Prüfung: Als zuständiger Unternehmensbereich wird die Interne Revision benannt und es stellt sich die Frage, ob eine Compliance-Organisation – aus Sicht der Autoren – überhaupt für die Überwachung zuständig sein kann. Zudem muss man den Eindruck gewinnen, als ob die Überwachung nach den Vorstellungen des IDW PS 980 nicht nur auf das CMS beschränkt ist. Den Autoren geht es wohl eher um die Unternehmensüberwachung als solches. Stammaufgaben der Unternehmenssicherheit und der Internen Revision sollen so in das CMS mit eingebunden werden. Fraglich ist aber, ob dies eine geeignete Zielrichtung dieses Elements ist. Ob aber Überwachung und Verbesserung auf eine allumfassende Wirksamkeitskont-

* Dr. Christian Schefold ist Rechtsanwalt im Düsseldorfer Büro von Mayer Brown LLP.

1 Schefold, C.: Compliance-Management-Systeme nach deutschem Standard, in: ZRFC 5/11, S. 221ff.

2 Schefold, C.: Compliance-Programm im Sinne des IDW PS 980, in: ZRFC 1/13, S. 12ff.

Qualitätsmanagement verbessert die Wirksamkeit eines CMS.

rolle hinweist – und damit Anschluss an das „große Ganze" einer Prüfung bietet – könnte ein Überstrapazieren des Compliance-Programms und der Compliance-Organisation im Unternehmen bedeuten.

Überwachung und Verbesserung allein mit der Folge arbeitsrechtlicher Zwangsmaßnahmen, wie in der Beschreibung des IDW PS 980 angedeutet, genügen aber nicht, um Compliance in einem Unternehmen wirksam zu integrieren. Hierzu ist ein umfassendes Compliance-Qualitätsmanagement erforderlich. Dabei kann die praktische Umsetzung der Compliance-Überwachung und -Verbesserung nicht allein Aufgabe der Internen Revision sein. Es ist mit einer der wichtigsten Tagesaufgaben der Compliance-Organisation. Compliance geht alle im Unternehmen etwas an. Dies gilt insbesondere für eine (Selbst-)Überwachung und (Selbst-)Verbesserung. Für eine entsprechende Anleitung und Umsetzung muss der Unternehmensbereich sorgen, der für Compliance zuständig ist. Er ist für eine ständige Optimierung verantwortlich – nämlich der Überwachung der Umsetzung im Unternehmen sowie der Verbesserung der Anforderungen, der Maßnahmen und der Organisation.

3. Überwachung als Qualitätsmanagement

Erfahrung in diesen Aufgaben hat das Qualitätsmanagement im Unternehmen und damit kann das vorletzte Element des IDW PS 980 auch eine Aufgabe für das Qualitätsmanagement sein. Der Compliance-Officer ist jedenfalls gut beraten, im engen Kontakt mit den Spezialisten der Prozesseffektivität und -effizienz sein CMS zu entwickeln und auch weiterzuentwickeln.

Der enge Zusammenhang mit dem Qualitätsmanagement gerade in diesem Element lässt die kritische Frage aufkommen, ob Compliance denn vielleicht nichts anderes als Qualitätsmanagement ist? Es geht bei Compliance weniger um Produktqualität als um Leistungsqualität – sofern man mit Unternehmensleistung das Gesamtauftreten des Unternehmens auf dem Markt versteht. Compliance und Qualitätsmanagement haben auch einen risikobasierten Ansatz gemeinsam: Letztendlich geht es darum, dafür zu sorgen, dass ein wie immer gearteter „Output" eines Unternehmens zu einem positiven Betriebsergebnis und keinem Risiko für das Unternehmen führt. Entgegen dem produktbezogenen Qualitätsmanagement ist Compliance aber auf das entsprechende Regelungsumfeld ausgerichtet. Man sollte gut prüfen, ob Compliance-Maßnahmen und Compliance-Organisation vor dem Hintergrund der gesetzten Compliance-Ziele angemessen ausgestaltet und wirksam sind. Grundlage der Prüfung ist so auch die ursprüngliche Risikoanalyse und Anforderungsdefinition. Deswegen ist es aus Sicht des Standards auch von großer Wichtigkeit, Grundlagen, Anforderungen, Maßnahmen und Organisation eines CMS in einem Compliance-Konzept oder -Handbuch zu dokumentieren.

Mit der ersten Umsetzung von Maßnahmen eines Compliance-Programms sollte geprüft werden, ob die Maßnahmen geeignet sind, Compliance-Risiken einzudämmen und die gesetzten Zielvorgaben zu erreichen. Oft werden Maßnahmen umgesetzt, die für andere Unternehmen entwickelt oder aber aus Dringlichkeitsgründen eher vorläufig angesetzt wurden. Hier klärt die Prüfung, ob tatsächlich die erwünschte Wirkung im Unternehmen eingesetzt hat.

4. Maßnahmen der Überwachung zur Verbesserung

Eine systematische Überwachung der Umsetzung des Compliance-Programms erlaubt zudem eine aktuelle Ergänzung der Risikoanalyse und führt schon so automatisch zu einer steten Aktualisierung des Compliance-Programms. Auf diese Weise entsteht ein Überblick über den Erfolg des Compliance-Management-Systems. Sowohl die Compliance-Organisation als auch die einzelnen Einheiten sowie die Geschäftsleitung haben einen Überblick über den Status von Compliance im Unternehmen und können entsprechend eingreifen – also verbessern. Nichts anderes verlangt § 130 OWiG.

4.1 Unternehmenseigene Untersuchungen

Bleiben wir aber zunächst bei der Sicht des IDW-Standards und blicken wir auf eine typische „Überwachung" durch Interne Revision, Rechtsabteilung und zuweilen auch externer Unterstützung durch Anwälte, Wirtschaftsprüfer und Berater: die „unternehmenseigene Untersuchung".

Unternehmenseigene Untersuchungen (*internal investigations*) werden anders als behördliche Untersuchungen von einem Unternehmenszweck geleitet. Das Ziel ist es, ein möglichst gutes Betriebsergebnis bzw. die Chancen auf gute Betriebsergebnisse zu wahren. Demnach ist eine unternehmenseigene Untersuchung darauf ausgerichtet, Prozesse wirtschaftlich zu optimieren – denn Fehlverhalten stellt keinen optimalen Geschäftsablauf dar. Das Ergebnis einer Untersuchung sollten konkrete Verbesserungsvorschläge sein. Es geht darum, Sachverhalte aufzuklären und Verbesserungen zu erzielen. Es ist nicht vorrangig Ziel, „Täter" zu finden. Dahingegen sind behördliche Untersuchungen entweder auf die Abwehr von Gefahren für die Allgemeinheit ausgerichtet (polizeilich präventiv) oder aber darauf, Täter zu ermitteln (kriminalistisch repressiv). Diese unterschiedliche Zielrichtung bedeutet auch, dass behördliche Untersuchungen keine Optimierung von Geschäftsprozessen anstreben und eine

Compliance-Maßnahmen können auch im Qualitätsmanagement genutzt werden.

unternehmenseigene Untersuchung auf die Ursachen von Gefahren oder Kriminalität parallel zu den staatlichen Untersuchungen erforderlich ist. Das Erkennen einer Gefahr (oder eines Risikos) oder eines Täters muss im Unternehmen weitere Konsequenzen haben als das bloße Ausschalten von Gefahrenquellen. Es ist erforderlich, betroffene Geschäftsprozesse anzupassen, sodass diese Risiken nicht mehr auftreten können und eine Verbesserung herbeigeführt werden kann.

4.2 Beratung

Eine ganz andere Quelle für Verbesserungsmöglichkeiten ist die Compliance-Beratung. Individuelle Compliance-Kommunikation hat auch seine Auswirkungen auf die Überwachungs- und Verbesserungsmechanismen eines Compliance-Programms. Dies betrifft insbesondere die Rückkopplung, also die Rückmeldung aus dem Unternehmen, von den Geschäftspartnern oder der Öffentlichkeit zurück an Unternehmensleitung und die Compliance-Organisation.

Eine Compliance-Helpline ist nicht nur ein Beratungsinstrument, um insbesondere den operativen Bereichen in ihren Compliance-Nöten beizustehen – Helpline-Mitarbeiter erfahren häufig als Erste von den Schwachstellen eines Compliance-Programms. Individueller Rat der Compliance-Organisation ist damit automatisch oft schon Verbesserung und dies ohne Überwachungsaufwand. Erfahrungen der Compliance-Beratungsstelle in einem Unternehmen führen häufig zu konsequenten Verbesserungsmaßnahmen. Dies kann einerseits die Überarbeitung einer miss- oder schwer verständlichen Richtlinie sein, andererseits kann es die Korrektur von Compliance-Maßnahmen sein, die sich insgesamt als wenig praktikabel herausgestellt haben. Beratungseinrichtungen haben aber den Nachteil, dass sie durch die Beratung geschäftliche Verantwortung operativer Bereiche übernehmen. Gute Beratung schürt häufig auch eine hohe Nachfrage und damit erheblichen Aufwand und Kosten. Es bedarf eines guten Fingerspitzengefühls und der Disziplin der Berater, hier eine vernünftige Abgrenzung zu finden gegenüber den Anfragenden.

5. Whistleblowing

Von der Beratung ist die Compliance-Hotline oder Beschwerdestelle (*Whistleblower-Hotline*) zu unterscheiden. Traditionell wandte sich ein Arbeitnehmer in Deutschland bei Missständen im Unternehmen an den Betriebsrat. Der Betriebsrat ist dann entweder offen für den Arbeitnehmer eingetreten und hat Missstände angeprangert oder aber er hat – was nicht selten vorkam – entsprechende Umstände aufmerksam registriert und sie dann später „politisch“ etwa als Druckmittel gegen unliebsame Geschäftsleitungen oder als Verhandlungsoptionen verwendet. Beschwerden sind auf unterschiedlichsten Wegen an ein Unternehmen herangetragen worden und es war häufig eher Glücksache, wenn derartige Hinweise eine Geschäftsleitung erreicht haben.

Eine Beschwerdestelle kann dem wirksam abhelfen. Dabei ist aber auch zu beachten, dass sie – ähnlich wie bei der unternehmenseigenen Untersuchung – strikt auf das Unternehmensinteresse ausgerichtet sein sollte. Ein effektives Hinweismanagement ist Teil des „betrieblichen Vorschlagwesens“ indem es Verbesserungen imitiert. Auch der typische *Whistleblower*-Fall aus dem Lehrbuch, die bösartige Verschwörung einer Gruppe von Mitarbeitern zur Veruntreuung von Unternehmensvermögen, die durch eine oder einen *Whistleblower* aufgedeckt wird, sollte aus der Unternehmenssicht in Verbesserungen münden: Wie kann man derartiges in Zukunft verhindern?

Auch hier ist die Aufdeckung und Verfolgung von Tätern ein Nebenzweck. Die Kündigung oder Versetzung offensichtlich ungeeigneter Personen ist zwar auch eine Verbesserung, es sollte aber auch um Veränderungen im Betriebsablauf oder in der Unternehmensorganisation gehen. Wer in Hinblick auf diese Ziele ein Hinweismanagement betreibt, der wird auch in der Lage sein, mit offensichtlich fehlgeleiteten „Beschwerden“ umzugehen, die allein der Denunziation oder Verleumdung dienen. Diese werden kaum zu einer sinnvollen Verbesserung führen.

6. Stichprobenprüfungen: Compliance Spot Checks

Prüfungen werden üblicherweise durch die Interne Revision und in manchen Fällen durch die Unternehmenssicherheit durchgeführt. Warum sollte Compliance dann ebenfalls Prüfungen durchführen? Dabei darf es nicht die Aufgabe einer Compliance-Organisation sein, eine „bessere“ Interne Revision dazustellen oder das Interne Kontrollsystem (IKS) des Unternehmens zu übertreffen. Compliance-Prüfungen müssen anders geartet sein, sollten sie einen vernünftigen Mehrwert zur Compliance-Überwachung und -Verbesserung darstellen. Sowohl die Interne Revision als auch das IKS lassen sich eher von den Maßstäben der unternehmenseigenen Rechnungslegung und Buchführung leiten. Das IKS baut auf Kontrollprozessen auf. Ziel des IKS ist es, Risiken frühzeitig zu erkennen. Wem es gelingt, diese Prozesse systematisch zu unterwandern, der kann ein IKS ausspielen. Die Interne Revision ist von definierten Standards abhängig; sie braucht Prüfungsgrundlagen, nach der sie die Unternehmenswirklichkeit bewerten kann. Ihr eigentliches Ziel ist es, Effektivität und Effizienz im Unternehmen zu verbessern. Wer abseits der Standards und Prozesse handelt und Regelrevisionen geschickt ausweicht, der wird oft nur durch ein *Whistleblowing* verraten.

Compliance Spot Checks zielen auf die Verbesserung des CMS ab.

Compliance Spot Checks sind Compliance-spezifische Maßnahmen der Überwachung. Durch sie wird ein Verständnis der Geschäftstätigkeit und in der Handhabung der Prozesse erfragt und daraus weiterer Handlungsbedarf für ein Compliance-Programm abgeleitet. Den Stand der Rechtstreue – eine der vielen Übersetzungsmöglichkeiten für den englischen Begriff „Compliance" – kann man oft nur im Gespräch oder in der detaillierten Analyse von Geschäftsprozessen erfahren. Deswegen ist nur eine Stichprobenprüfung möglich. Die Kunst einer derartigen Compliance-Prüfung ist es, in ausreichender Kenntnis der neuralgischen Bereiche eines Unternehmensteils gerade kritische Situationen zu testen. Dabei muss man sich nicht von einem „Ermittler-Näschen" leiten lassen. Gründliche Vorbereitung durch intensive Informationen über den zu prüfenden Geschäftsbereich gepaart mit der betrieblichen Compliance-Erfahrung werden fast automatisch die richtigen Überwachungsbereiche erkennen lassen.

Es sind nur wenige und an repräsentativen Unternehmensstellen durchgeführte *Compliance Spot Checks* erforderlich, um eine aktuelle Compliance-Statusübersicht oder aber auch *Compliance Risk Map* zu bilden. Damit lässt sich dann eine anschließende Verbesserung präzise ansteuern und im Bericht an die Geschäftsleitung griffig erläutern. Übrigens sollten bei *Compliance Spot Checks* die Compliance-Organisation, die Interne Revision und auch das Qualitätsmanagement eng zusammenarbeiten. Insbesondere bei der Vorbereitung einer solchen Stichprobe ist Wissen aus den Stabsbereichen äußerst wertvoll. Ergebnisse werden natürlich untereinander kommuniziert und können damit den weiteren untersuchenden Bereichen im Unternehmen helfen.

7. Compliance Status Assessment

Ein in der Ausführung sehr einfaches Mittel sind Umfragen. Mittlerweile wird überall der Meinungsstand zu Produkten und Leistungen abgefragt. Warum dann nicht zum CMS? Dabei sollten die Fragen gut vorbereitet sein und die Anwendung des CMS testen. Simple „Ja/Nein"-Ant-

Man sollte sich nicht auf die Fachkenntnis externer Kräfte verlassen.

worten werden dabei nicht unbedingt einen ehrlichen Status verraten. Sinnvoller sind hier Antworten auf einer Skala von 1 bis 10. Dies erlaubt auch, Unsicherheiten im Umgang mit Compliance-Themen zu testen. Im Gesamtbild kann es zudem viel über den Zustand des CMS im Unternehmen verraten. Oft ist dies eine erste Grundlage, um Handlungsbedarf für eine Compliance-Organisation festzustellen – oder aber einen *Compliance Spot Check* zu veranlassen.

8. Fazit

Auch wenn eine zu enge Verbindung abgelehnt wird, Compliance-Überwachung und -Verbesserung knüpft auch an den Prüfungsprozess im Rahmen des IDW PS 980 an. Die Prüfung selbst erfolgt nach dem Standard in drei Schritten: Zunächst wird die Eignung eines Compliance-Konzepts geprüft, dann die Angemessenheit im Hinblick auf die Umsetzung des Konzepts und schließlich die Wirksamkeit des nun umgesetzten CMS. Diese letzte Stufe lässt sich mit dem vorletzten Element der Überwachung und Verbesserung verknüpfen. Dabei sollte man sich allerdings nicht allein auf die Fachkenntnis externer Kräfte verlassen. Nur eigene Ressourcen zur Compliance-Qualitätssicherung werden eine ausreichende Wirksamkeit des unternehmenseigenen CMS gewährleisten.

Was aber ist eine ausreichende Wirksamkeit, was ist die Aufgabe eines CMS? Es wird im letzten Element des im IDW PS 980 beschriebenen Regelkreises dargestellt: die Compliance-Kultur. Der letzte Beitrag dieser Reihe wird sich im nächsten Heft mit der Frage beschäftigen, ob und wie Compliance auf die Unternehmenskultur Einfluss nimmt, sie gestaltet und auch verändert. Kann eine derart gestaltete Compliance-Kultur auch das Betriebsergebnis eines Unternehmens verbessern? Welche Vorteile kann der hohe Aufwand eines CMS nach IDW PS 980 einem Unternehmen bringen?