04.22

17. Jahrgang
August 2022
Seiten 145–192

ZRFC

Risk, Fraud & Compliance

www.ZRFCdigital.de

Prävention und Aufdeckung durch Compliance-Organisationen

Management

Ausweispraxis nicht-finanzieller Werte
Weber-Lewerenz, 151

Mensch oder Maschine?
Schneider, 161

Detection

Angewandte Statistik in der Unternehmenswelt – Teil 3
Tiemann, 165

Legal

10 Jahre IDW PS 980
Schefold, 170

Profession

Anforderungen an Compliance-Experten
Weinert/Jüttner, 178

Compliance bewegt ...
Interview mit Katharina Kneisel, 188

ERICH SCHMIDT VERLAG

In Kooperation mit
DICO
Deutsches Institut für Compliance

64683

10 Jahre IDW PS 980

Zum Jubiläum kommt die Neufassung

Dr. Christian Schefold*

Dr. Christian Schefold

Das Institut der Wirtschaftsprüfer in Deutschland e. V. (Institut der Wirtschaftsprüfer – IDW) hat vor zehn Jahren bahnbrechende Arbeit geleistet: In einer vielbeachteten internationalen Vergleichsarbeit wurden die damals wesentlichen Standards zum Aufbau von Compliance-Programmen (der Begriff eines Compliance-Management-Systems bildete sich damals erst heraus) in der Welt verglichen, und es hat die damals frei verfügbaren Standards in einem neuen IDW-Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen (IDW PS 980)" zusammengetragen. Nun wird eine Neufassung erarbeitet.

1 Einleitung

Die damalige standardvergleichende Tätigkeit wird nun etwas eingeschränkt. Betrachtet werden — im Unterschied zur Vorversion — vor allem die Standards der ISO-Familie (37001:2016; 37002:2021 und 37301:2021) sowie anerkannte Verhaltensrichtlinien bestimmter Branchen in Deutschland (die der Immobilienwirtschaft beziehungsweise des Verbandes Materialwirtschaft, Einkauf und Logistik) und ferner — als Hinweise und Hilfestellung — sowohl die DICO-Standards und Leitlinien als auch die KICG-Leitlinien aus Konstanz, deren Nichtberücksichtigung 2011 zu einigem Unmut geführt hatte.

Ende 2021 wurde ein Entwurf der Neufassung des Compliance-Standards (IDW EPS 980 n. F.) der Öffentlichkeit zugänglich gemacht, und nun geht es an die Konsolidierung von Kommentaren und Rückmeldungen. Die Neufassung ist nach zehn Jahren auch erforderlich geworden, denn Compliance und auch das Tool eines Compliance-Management-Systems (CMS) sind mittlerweile in aller Breite sowohl in der Wirtschaft als auch in Politik und Rechtsprechung bestens anerkannt. Allerdings werden die Bestrebungen für ein Verbandssanktionengesetz noch nicht berücksichtigt, schließlich befindet sich das Gesetz noch in der parlamentarischen Diskussion, und der letzte veröffentlichte Entwurf stammt aus der Feder der alten Bundesregierung. Vielleicht gelingt es noch, hier eine Verbindung zwischen Standard und Gesetzesentwurf (oder gar Gesetz) zu ziehen. Da der Prüfungsstandard seine Verbreitung vornehmlich in Deutschland hat, ist das Verbandssanktionengesetz wesentlich für seine Anwendung und sollte daher Berücksichtigung finden. Insgesamt sind die Renovierungsarbeiten am Standard IDW PS 980 nicht allzu weitgehend, als dass die Neufassung nicht noch ein paar Monate warten könnte.

2 Neues in der Neufassung

Schon ein Blick in das Inhaltsverzeichnis der Neufassung zeigt im Vergleich zum Original einen Paradigmenwechsel: Während 2011 die Risikoanalyse selbst noch wesentlich war, beschränkt sich die Prüfungshandlung nur noch auf die Darstellung der Risikoanalyse. Prüfungshandlungen beschränken sich auf die Identifikation und Beurteilung von Risiken wesentlicher falscher Darstellungen in der CMS-Beschreibung. Dieser Ansatz setzt sich fort: Ausgangsort der CMS-Prüfung ist die CMS-Beschreibung und die dort enthaltenen Darstellungen zur Angemessenheit und Wirksamkeit des CMS. Geprüft werden dann die Angemessenheit und die Wirksamkeit der in der Beschreibung dargestellten Compliance-Regelungen. Die Neufassung berücksichtigt auch, dass ein Wirtschaftsprüfer bei der Beurteilung des CMS nicht alleine steht: Es sollen die Arbeiten von Sachverständigen des Prüfers selbst (hier sind vor allem die in den Reihen von WP-Gesellschaften tätigen Juristen sowie aber auch für eine Prüfung extra beauftragten Kanzleien gemeint.), die Arbeit anderer Prüfer (wohl die jeweiligen Abschlussprüfer eines Unternehmens), Sachverständige von Vorstand beziehungsweise Geschäftsführung und die Interne Revision. Es fehlt das in vielen Unternehmen mittlerweile etablierte Risikomanagement beziehungsweise Interne Kontrollsystem (IKS).

In den Definitionen (Ziff. 1.2 — früher: Begriffsbestimmungen) fällt auf, dass die Begriffe „falsche Darstellung in der CMS-Beschreibung", „Mangel des CMS" und in eigener Sache „Prüfungsrisiko" wie

* Dr. Christian Schefold, LL. M., ist Partner im Berliner Büro der globalen Wirtschaftskanzlei Dentons und Co-Head der deutschen Compliance Praxis. Seit 2011 kommentiert er in der ZRFC die Entwicklung des IDW PS 980 und anderer Standards.

auch „Sachverständige des CMS-Prüfers“ aufgenommen wurden.

Eine CMS-Prüfung nach IDW PS 980 wird in Zukunft keine eigene Bestandsaufnahme des Prüfers mehr bedeuten, sondern sich auf einen kritischen Blick über die Beschreibung des unternehmenseigenen CMS beschränken. Demnach werden Begrifflichkeiten für eine unvollständige oder falsche beziehungsweise irreführende Darstellung (falsche Darstellung) sowie die fehlende Geeignetheit, dass ein CMS mit hinreichender Sicherheit wesentliche Regelverstöße erkennen und damit auch verhindern lässt (Mangel), eingeführt. Hier schon ist die Fokussierung auf die CMS-Beschreibung als Ergebnis des Gesamtprozesses des Aufbaus eines CMS im Unternehmen erkennbar. Dies entspricht moderner Auditlogik: Es wird vom Unternehmen als dem eigentlichem Prüfungsgegenstand erwartet, selbst eine kritische Hinterfragung des eigenen CMS-Aufbauprozesses durchzuführen und in der CMS-Dokumentation zu hinterlegen. Der Prüfer verifiziert dann nur noch die Dokumentation. Erkennbare Defizite der Dokumentation führen dann zu negativen Prüfungsaussagen — und idealerweise zu einem Hinweis während der Prüfung und der Gelegenheit zur Nachbesserung.

Ein Prüfungszertifikat nach IDW PS 980 ist kein Garant für ein einwandfrei funktionierendes CMS. Zuweilen wurden öffentlichkeitswirksam präsentierte Prüfungen renommierter WP-Gesellschaften durch Compliance-Skandale widerlegt. In der Regel gab es hier zwar keine Prüfungsfehler, da Compliance-Defizite fast ausschließlich in den Bereichen auftraten, die nicht geprüft wurden, reputationsförderlich für die Zunft der Wirtschaftsprüfer und den Prüfungsstandard IDW PS 980 war das aber nicht. Wirtschaftsprüfer können ein CMS nicht alleine prüfen, vor allem ist juristischer Rat wesentlich, meist auch aus allen Jurisdiktionen, in denen ein Unternehmen tätig ist. Über zehn Jahre Entwicklung bei Compliance hat aber mittlerweile eine große Zahl erfahrener Compliance-Spezialisten nahezu jeglicher Fachrichtung hervorgebracht. Diese ausdrückliche Öffnung, die der Praxis seit Anbeginn des Standards eigentlich entspricht, ist deutlich zu begrüßen.

3 Die Compliance-Prüfung

Der Prüfungsgegenstand und damit auch der Prüfungsansatz nach IDW PS 980 wird sich in Zukunft als Systemprüfung auf eine Darstellung des CMS durch die gesetzlichen Vertreter eines Unternehmens und dann auch nur auf die Prüfung konkret beauftragter Teilbereiche beschränken (Ziff. 1.3). Auch wenn vorher der Prüfungsauftrag schon auf die in der CMS-Beschreibung enthaltenen Aussagen beschränkt war, zeigen sich in dieser Einschränkung zwei wesentliche Entwicklungen: (1) Das CMS bedarf zumindest in den Grundzügen seiner Beschreibung der Verabschiedung durch die Geschäftsleitung — also einen Vorstands- oder ein Geschäftsführungsbeschluss. Diese Klarstellung ist insbesondere aus gesellschaftsrechtlichen Gründen der Corporate Governance sehr zu begrüßen. (2) Es findet keine Komplettprüfung, sondern nur noch eine Prüfung in Teilbereichen statt; Prüfungsergebnisse werden dann auch entsprechend eingeschränkt abgegeben. Hier wird die Erfahrung der letzten Jahre mit Prüfungszertifikaten wiedergegeben. Diese sind keine Persilscheine für Compliance im Unternehmen allgemein. Zudem liegt auch die Beauftragung und deren Umfang, also die Definition der Prüfungsteilbereiche, bei der Geschäftsleitung. Eine Prüfung dieser Auswahlentscheidung findet übrigens nicht statt, und daher dürfen aus der Einschränkung der Entscheidung wohl auch keine Rückschlüsse auf die Prüfung selbst gezogen werden.

IDW PS 980 konzentriert sich nun stärker auf das CMS-Konzept.

Weiterhin ist es möglich, eine Prüfung des CMS allein auf Angemessenheit und Implementierung einzugrenzen und auf eine Wirksamkeitsprüfung zu verzichten oder diese zu einem späteren Zeitpunkt nachzuholen. Die Neufassung stellt klar, dass eine Prüfung sich auf eine Angemessenheitsprüfung beschränken kann, die zum einen (mit hinreichender Sicherheit) verifizieren soll, ob die in der CMS-Beschreibung dargestellten Regelungen (und damit die entsprechenden Maßnahmen) in Übereinstimmung mit den angewandten CMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sowie auch (abstrakt) geeignet ist, Risiken für wesentliche Regelverstöße zu erkennen und diese auch zu verhindern, und ob diese auch im Unternehmen umgesetzt wurden (Implementierung).

Die Wirksamkeitsprüfung beinhaltet die Angemessenheitsprüfung eines CMS und ergänzt diese um eine konkrete Geeignetheitsprüfung: Zum einen soll sich der Prüfer hinreichend sicher sein, dass die in der CMS-Beschreibung definierten Regelungen im Hinblick auf die jeweils angewandten CMS-Grundsätze angemessen sind und auch umgesetzt wurden und dabei — zumindest im Prüfungszeitraum — im Wesentlichen (konkret) geeignet waren, Risiken für erhebliche Regelverstöße rechtzeitig zu erkennen als auch zu verhindern.

Eine IDW PS 980-Prüfung ist nach wie vor eine Systemprüfung und keine Prüfung einzelner Vorgänge, wobei deren Bewertung etwa im Rahmen der konkreten Geeignetheitsprüfung sicherlich Eingang in die Systemprüfung finden kann.

4 Die Entwicklung der Elemente eines CMS

Die CMS-Elemente nach IDW PS 980 sind in Zahl und Typ gleich geblieben, trotzdem werden neue Aspekte in den einzelnen Elementen berücksichtigt:

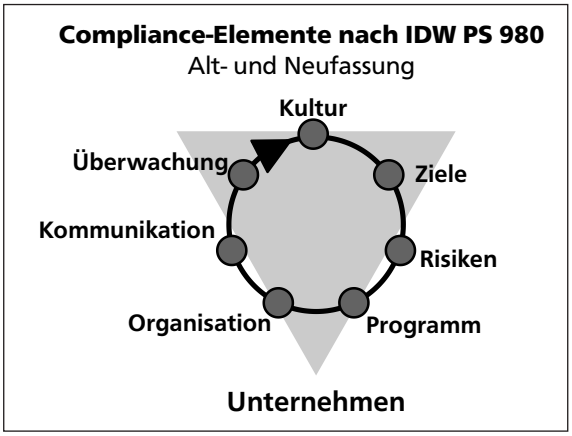

Abbildung 1: Compliance-Elemente nach IDW PS 980

Hinsichtlich der Compliance-Kultur wird nun die Verankerung im Unternehmen betont, und auch die Kommunikation muss diese Kultur in das Unternehmen und sein Umfeld tragen.

IDW PS 980 behält einen flexiblen Prüfungsansatz.

Bezüglich der Compliance-Ziele sieht es zunächst so aus, als hätte es keine Änderung gegeben. In den Anwendungshinweisen zur Neufassung des Standards gibt es dann aber eine wesentliche Änderung in Bezug auf Risikoanalyse und Zieldefinition: Es wird eine erste Risikoanalyse vor Zieldefinition empfohlen sowie die Berücksichtigung des Bedarfs einer besonderen Risikosteuerung bei der Zielsetzung. Der Verzicht auf Geschäftstätigkeiten wegen besonderer Risikohaftigkeit ist hier vielleicht kein so ganz passendes Beispiel, da es ein wesentliches Vorurteil gegenüber Compliance bestärkt: Compliance als Geschäftsverhinderung. Insgesamt, aber wird hier ein Henne-Ei-Dilemma der Originalfassung des Standards angefasst: Kommt nun die Zieldefinition oder die Risikoanalyse zuerst? Der Start sollte mit einer ersten, groben Risikobetrachtung erfolgen.

Die Compliance-Risikoanalyse soll nun auch mögliche Risikointerdependenzen berücksichtigen. Die Anwendungshinweise geben weitergehende Anleitungen zur Prüfung einer Risikoanalyse und damit zur Vornahme der Risikoanalyse selbst, indem sie neben Risikointerdependenzen auch Kriterienbildung, eine Aufteilung zwischen Risikoeintrittswahrscheinlichkeit und Berücksichtigung eines potenziellen Schadensausmaßes ansprechen. Richtig ist der Fingerzeit, dass eine Compliance-Risikoanalyse ein konstanter Prozess sein muss, eine einmalige Analyse reicht nicht aus. Hier empfiehlt sich auch die Verbindung zur konstanten Überprüfung und Verbesserung des CMS als eigenem Element. Die DICO-Standardarbeit dürfte in den Anwendungshinweisen zur Compliance-Risikoanalyse den größten Einfluss gehabt haben. Diese interdisziplinare Zusammenarbeit ist sehr zu begrüßen und sollte weiter intensiviert werden.

Das Compliance-Programm besteht nicht mehr aus Grundsätzen und Maßnahmen, sondern nur noch aus Regelungen. Es heißt hierzu in den Anwendungshinweisen, dass der Schwerpunkt eines Programms auf Regelungen, das heißt Kommunikation von Inhalten und Anweisungen (in der Regel kollektiver Natur durch Richtlinien), gelegt werden soll — und nur noch eher sekundär auf Maßnahmen (als Beispiel wird hier das Hinweisgebersystem genannt). Leider finden Hilfestellung und Beratung keine Berücksichtigung mehr. Diese konkrete Compliance-Maßnahme dürfte aber im Einzelfall die effizienteste Maßnahme zur Risikobegrenzung sein.

Der organisatorische Aufbau, die Compliance-Organisation ist nun im Sinne der Verantwortungsdelegation strikt von der Unternehmensleitung (das heißt „von oben“) her konzipiert: Die Geschäftsleitung definiert Rollen und Verantwortlichkeiten (Funktionen) sowie Aufbau- und Ablauforganisation (objektive Ausstattung). Der Compliance-Bereich ist dabei nun integraler Bestandteil der etablierten Unternehmensfunktionen. Nach den Delegationsgrundsätzen muss die so definierte Funktion auch mit entsprechend qualifiziertem Personal besetzt werden (subjektive Ausstattung) und die für die Aufgabenerfüllung erforderlichen Ressourcen erhalten. Wesentliches ist zu dokumentieren beziehungsweise sogar anzuweisen. Es fehlt in diesem Zusammenhang allerdings ein Hinweis auf die für eine erfolgreiche Delegation abschließend erforderliche Kontrolle. Hierzu besteht zwar ein eigenes CMS-Element, ein Verknüpfungshinweis würde das Delegationsmodell aber vollständig machen.

Wie schon angemerkt, ist ausdrücklich auch die Compliance-Kultur nun in die Compliance-Kommunikation mit einzubeziehen. Die Kommunikation war bisher ein wesentlicher Bestandteil von Maßnahmen eines Compliance-Programms. Wenn nun das Programm aber auf Regelungen reduziert wird, ist es vielleicht angebracht — vergleichbar mit der ISO-Welt — ein neues Element Compliance-Hilfestellung einzuführen.

Compliance-Überwachung und Verbesserung ist nun eine Aufgabe der Internen Revision, auf deren Einsatz in den Anwendungshinweisen besonders hingewiesen wird. Wünschenswert wäre die Aufnahme weiterer Verknüpfungen, insbesondere zur konstanten Compliance-Risikoanalyse.

5 Anforderungen an die Prüfer

Auch wenn sich nach einem ersten Blick in die Neufassung die zukünftige Prüfung mehr auf die CMS-Darstellung beschränkt, muss sich der Prüfer nach wie vor einen Eindruck vom Gesamtunternehmen machen sowie sich ein Verständnis des rechtlichen und wirtschaftlichen Umfelds verschaffen. Diese Vorarbeiten müssen zumindest für die Beurteilung ausreichen, ob die Risiken wesentlicher

falscher Darstellungen in der CMS-Beschreibung beziehungsweise wesentlicher Mängel des in der CMS-Beschreibung dargestellten CMS festgestellt und bewertet werden können.

Die Anwendungshinweise zur Prüfungstätigkeit sind insgesamt praxisnäher geworden. Die Nutzung externer Quellen (Ziff. 3.4.3) wird explizit angesprochen. Stets ist aber zu prüfen, ob ihr Einsatz für die Zwecke der Prüfung geeignet ist. Insbesondere muss eine bestimmte Qualität, aber auch Unabhängigkeit gewährleistet sein. So können etwa Ergebnisse anderer Prüfer und Aussagen von Sachverständigen des Unternehmens und auch der Interne Revision des Unternehmens genutzt werden. Gerade dies dürfte die Interne Revision dann aufwerten, wenn eine Prüfung ihrer Objektivität, Kompetenz und Arbeitsweise (nach IDW oder DIIR Grundsätzen) zu Zwecken der Prüfung geeignet (abstrakt) und ihre Prüfungstätigkeit (konkret) hierzu nutzbar ist.

Nach wie vor wird die Prüfung mit einer Vollständigkeitserklärung der Geschäftsleitung abgeschlossen. Insgesamt wird die Bedeutung von Vorstand und Geschäftsführung für eine Prüfung nach IDW PS 980 und das CMS insgesamt deutlich unterstrichen. Eine Delegation ist zwar möglich, die Letztverantwortung und Compliance-Kultur obliegt aber der Unternehmensleitung.

Auf eine weitere Praxisübung wird bei den Anwendungshinweisen zur Auswertung und Bildung des Prüfungsurteils abgestellt: Drohen negative Ergebnisse, so soll zunächst auf eine Berichtigung der Umstände hingewirkt werden (Ziff. 3.4.4). Damit wird eine weitere Funktion einer Compliance-Prüfung nach IDW PS 980 hervorgehoben: Oft ist eine solche Prüfung eher ein Verbesserungsprogramm beim Aufbau eines CMS als ein Weg zu einem Zertifikat. Diese Zertifikatsfunktion, die vor zehn Jahren für Unternehmensleitungen noch sehr wichtig war, wurde zu oft missbraucht, um noch dieselbe Bedeutung zu bewahren.

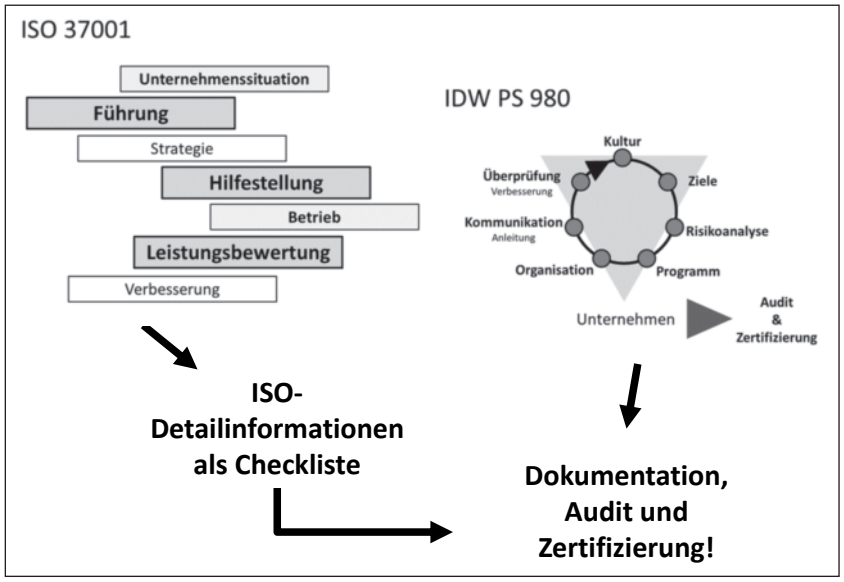

Abbildung 2: Kombinationen mit anderen Standards (unter anderem ISO) sind möglich

6 Kombination mit anderen Standards

Ein entscheidender Vorteil des Prüfungsstandards IDW PS 980 bleibt, da die Basis eines CMS und die Grundlagen seiner Prüfung nach wie vor zuerst festzulegen sind: Der IDW PS 980 lässt sich sehr einfach mit weiteren Standards, etwa aus der ISO-Familie, kombinieren und kann damit – unter Einbezug erfahrener Wirtschaftsprüfer und deren Sachverständige – zu deutlich präziseren und praxisnäheren Prüfungen und Prüfungsergebnissen führen. Dies kann nun mit den entstehenden DICO-Standards zu einer eigenständigen, praxisnahen Standardfamilie mit Prüfungsabschluss führen. Mit der geplanten Neufassung wird dieser Vorteil aktualisiert und bleibt erhalten.

Die Stärke des IDW PS 980 bleibt seine Kombinationsfähigkeit unter anderem mit ISO-Normen.