01.17

ZRFC

Risk, Fraud & Compliance

12. Jahrgang
Februar 2017
Seiten 1–48

www.ZRFCdigital.de

Prävention und Aufdeckung durch Compliance-Organisationen

Management — Einfluss des Aufsichtsrats auf das Compliance-Management
Ulrich, 7

Prevention — Haftungsfall(e) Material-Compliance
Nieser/Reusch, 14

Detection — Social Engineer und Social Engineering
Drechsler/Haag, 17

Legal — ISO 37001-Compliance
Schefold, 27

Profession — Compliance bewegt ...
Interview mit Aram Kaven-Moser, 37

Wo Rauch ist, ist auch Feuer(?)
Schneider/Bäcker, 39

ESV ERICH SCHMIDT VERLAG

In Kooperation mit DICO Deutsches Institut für Compliance

64683

ISO 37001-Compliance

Anforderungskatalog und Guidance für das Unternehmens-CMS zur Bestechungsprävention

Dr. Christian Schefold*

Schon beim Erscheinen des ersten Compliance-Standards der International Organization for Standardization (ISO), dem Standard 19600 „Compliance Management Systems – Guidelines" war bekannt, dass ein weiterer Standard zur Korruptionsprävention in Vorbereitung war.[1] *Dieser ISO-Standard 37001 „Anti-bribery Management Systems – Requirements with Guidance for Use" ist am 15. Oktober 2016 – gut zwei Jahre nach dem ISO-Erstwerk – erschienen. Dieser Beitrag will eine zusammenfassende Darstellung, Analyse wie auch Einschätzung über seine möglichen Auswirkungen vermitteln. Wie dieser ISO-Standard – der im Unterschied zu ISO 19600 offiziell ein Anforderungsstandard (Requirements) mit einem Anleitungsannex (Guidance for Use) ist – in der Wirtschaft weltweit übernommen wird, bleibt abzuwarten. Auch hier wird die ZFRC aufmerksam die Entwicklung beobachten und über erste Anwendungsfälle und ihre Ergebnisse berichten.*

Dr. Christian Schefold

1 Warum ISO? Warum dieser Standard?

Die ISO dient als internationale Nichtregierungsorganisation unter anderem durch den Abbau von Handelshemmnissen primär der Förderung des internationalen Handels und steht daher nicht nur örtlich der Welthandelsorganisation [World Trade Organization (WTO)] in Genf nahe. Auch mit den beiden Standards bewegt sich die ISO auf dem Feld des internationalen Freihandels: Compliance hat globale Auswirkungen, und es besteht ein Bedarf an weltweit einheitlichen Lösungen. Die Autoren des Standards ISO 37001 berufen sich in der Einführung zu ihrem Standard sogar auf frühere internationale Initiativen der OECD und der UNO. Diese Rechtfertigung scheint notwendig, ist aber wohl zu hoch gegriffen. Mit OECD- und UNO-Konventionen kann das ISO-Werk schon alleine vor dem Hintergrund einer (völker)rechtlich sorgsamen Analyse, Genese und einzelstaatlichen Rezeption nicht mithalten. Für die Behauptung in der Einführung, es reflektiere „international good practice" bei der Korruptionsprävention, besteht kein Nachweis. Aufgabe der ISO ist der Abbau von Handelshemmnissen durch Vereinheitlichung (vornehmlich) technischer Standards. Einen Ansatz, den globalen Freihandel durch Empfehlungen zum Verhalten in unterschiedlichen Rechts- oder Kulturkreisen zu geben, verfolgen ISO 19600 und ISO 37001 aber erkennbar nicht. Sie wollen eher bereits bestehende Anforderungskataloge aus einer internationalen Ebene heraus verdrängen und ersetzen.

Entgegen ISO 19600 spricht der Antibestechungsstandard ISO 37001 jedoch Legislative und Exekutive der Staaten nicht unmittelbar an und hält sich auch mit Anforderungen und Empfehlungen im Verhältnis zwischen Unternehmen, Individuen und staatlichen Behörden wohltuend zurück. Dabei kann ISO 37001 seine Herkunft aus dem modernen britischen Antikorruptionsrecht nicht verleugnen.

Unternehmen haben immer schon vom jeweiligen Gesetzgeber Hinweise zur Erfüllung von Rechtspflichten verlangt. Das war bereits 1977 bei der Verabschiedung des US-amerikanischen Bundesrechts gegen Korruption im Auslandsgeschäft so.[2] Die entsprechende Guidance („A Resource Guide to the U.S. Foreign Corrupt Practices Act") dazu wurde aber erst Ende 2012 veröffentlicht.[3] Der UK Bribery Act durfte erst in Kraft treten, nachdem eine Guidance der britischen Regierung veröffentlicht wurde.[4] Daher erklärt sich auch die erhebliche Ver-

* Dr. Christian Schefold ist Rechtsanwalt bei Dentons Europe LLP in Berlin.

1 Zum ISO-Standard 19600 siehe Schefold, C.: ISO-Compliance, ZRFC 1/2015, S. 10 ff.

2 Dann im Rahmen von Gesetzesänderungen in 15 U.S.C. § 78-dd-1/2 (d) für den August 1989 gefordert aber erst am 14. November 2012 veröffentlicht.

3 Bribery Act 2010 vom 08. April 2010 (UK Bribery Act).

4 Sektion 19 Subsektion (1) bis (3) in Verbindung mit Sektion 9 des UK Bribery Act – Inkrafttreten am 01. Juli 2011/ *„Guidance about relevant procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)"* vom März 2011 (UK Guidance).

zögerung im Inkrafttreten dieses Gesetzes. Der Begriff einer Guidance – und erst recht der Inhalt – ist aber nicht gesetzlich festgelegt: Die staatlichen Hinweise waren oberflächlich. Es lag daher nahe, dass sich die Wirtschaft selbst hilft und entsprechende Hilfestellung entwickelt – warum nicht gleich dann einen British Standard – oder gar ISO-Standard? Dies ist der Hintergrund des ISO 37001 und auch die Erklärung für unterschiedliche Autorenkomitees innerhalb der ISO.

Es ist nämlich nicht das Projektkomitee ISO/PC271 des Vor-Standards sondern ein neues Projektkomitee ISO/PC278, welches für den neuen ISO 37001 verantwortlich zeichnet. Das erklärt vielleicht auch, warum die Hinweise auf den ISO 19600 im Text des ISO 37001 eher spärlich sind und sich auf Einführung und Erläuterungsannex beschränken – insbesondere bei dem Hinweis auf weitere Compliance-Themenfelder über „anti-bribery" im „Scope" des Standards hinaus wäre ein Hinweis (oder zumindest ein „Note") auf ISO 19600 angebracht gewesen.

2 Die wahre Guidance zum UK Bribery Act 2010?

Der Begriff „anti-bribery" legt einen britische Einfluss nahe – sonst hätte die Bezeichnung des ISO-Standards wohl mit den Worten „anti-corruption" begonnen. Möglicherweise erlaubt aber dieser britisch/amerikanische-Sprachunterschied weitere Einblicke in die Arbeit des Projektkomitees ISO/PC271.

Ziff. 3.1 des Standards ISO 37001 enthält eine – ausdrücklich allgemeine – Definition des Begriffs „bribery":

> *offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, ..., as an inducement or reward for a person acting or refraining from acting in relation to the performance (3.16 [measurable result]) of that person's duties*[5]

Dies entspricht vom Wortlaut und Stil eher dem UK Bribery Act in Sektion 1 Subsektion (2) und (3) bei der Beschreibung von Case 1 und Case 2 als dem U.S.-FCPA in 15 U.S.C. § 78-dd-3 (a). Allerdings enthält der Standard weitere Interpretationen, Erweiterungen und Einschränkungen gegenüber den Tatbeständen im UK Bribery Act, sodass der Begriff „bribery" zwar offensichtlich vom UK Bribery Act beeinflusst ist, ihm aber nicht vollständig entspricht.

Der Zusammenhang zwischen UK Bribery Act 2010 und ISO 37001 ist deutlich erkennbar.

Im Anleitungsannex sind Empfehlungen zu zwei Sonderfälle der Bestechung aufgenommen: Der Umgang mit „facilitation payments" sollte verboten werden – eine Empfehlung und keine Anforderung im Sinne des Hauptteils des Standards. „Extortion payments" sollten – so die Empfehlung – nur im Fall einer drohenden Gefahr für Gesundheit, Sicherheit oder Freiheit einer Person gestattet werden. Für den zweiten Fall werden Anleitungen des Unternehmens gefordert. Die Vorgänge sind zudem sämtlich zu dokumentieren und in der Buchhaltung zu erfassen. Insoweit werden hier Anforderungen des U.S.-FCPA erfüllt.

Eine kritische Klippe umschifft ISO 37001. Bei der Durchsicht des Anforderungsteils erwartet man eigentlich ein striktes Verbot von Geschäft mit hohem Bestechungsrisiko. Der Anleitungsannex stellt jedoch klar: Grundsätzlich ist Geschäftstätigkeit auch in Situationen mit einem höheren als nur niedrigen Bestechungsrisiko erlaubt. Es müssen aber entsprechende Compliance-Vorkehrungen zum Umgang mit einem höheren Bestechungsrisiko getroffen werden.

Der Standard ISO 37001 wendet sich sowohl gegen Bestechungen im Amtsträgerbereich als auch in der Privatwirtschaft und verfolgt damit ebenfalls die Linie des UK Bribery Acts. Dies ist insoweit bemerkenswert als auch die internationalen Konventionen sich allein gegen die Bestechung staatlicher Amtsträger richten. Das Phänomen der Korruption geht aber weiter und reicht auch hin zu den Entscheidungsträgern in Unternehmen.

Der Standard umfasst aber nur Bestechungen als Korruption im engeren Sinne. Der europäische Begriff der Korruption geht über den des US-Rechts – zumindest den des U.S.-FCPA – hinaus. Korruption ist die missbräuchliche Ausnutzung oder Beeinflussung gerade staatlicher Funktionen auch über die reine Vorteilsgabe hinaus: Korruption umfasst auch das Ausnutzen von Interessenkonflikten, Umfeld-Beeinflussung, kritisches Filtern und Auswählen von Informationen. Korruption ist der Inbegriff für den Versuch unrechtmäßiger Einflussnahme jenseits der dafür vorgesehenen staatlichen Strukturen hinaus. Dieses weitere Feld wird von ISO 37001 nicht aufgenommen. Dies hat möglicherweise auch etwas mit dem strikten Anforderungsregime des Standards zu tun. Die umfangreichen Anforderungen können sich nur auf relativ präzise Bereiche richten -sonst wären Unternehmen schlicht überfordert.

3 Struktur des ISO-Leitfadens

Positiv zu vermerken ist, dass trotz des Abstandes zwischen beiden ISO-Standards der Aufbau und die Gliederung des ISO 37001 dem ISO 19600 folgt. Auch der ISO 37001-Standard setzt auf sieben, eher funktionale Bereiche eines CMS auf:

1. Ziff. 4 – Unternehmenssituation (Context of the Organization)
2. Ziff. 5 – Führung (Leadership)
3. Ziff. 6 – Strategie (Planning)
4. Ziff. 7 – Hilfestellung (Support)
5. Ziff. 8 – Betrieb (Operation)

5 Ziff. 3.1 ISO 37001 – Streichungen „..." und Ergänzungen „[abc]" durch den Verfasser.

6. Ziff. 9 – Leistungsbewertung (Performance Evaluation)
7. Ziff. 10 – Verbesserung (Improvement)

Den Schwerpunkt des Standards bilden – wie bei ISO 19600 – die Bereiche Führung (Ziff. 5), Hilfestellung (Ziff. 7) und Leistungsbewertung (Ziff. 9). Anders als bei dem Vor-Standard wird aber dem Betrieb (Ziff. 8) mehr Aufmerksamkeit geschenkt, das Interesse an dem Thema Unternehmenssituation (Ziff. 4) wird mit Empfehlungen im Anleitungsannex angereichert. Weniger berücksichtigt werden – ebenfalls wie bei ISO 19600 – Strategie (Ziff. 6) und Verbesserung (Ziff. 10). *(Abbildung 1)*

Ergänzt wird der Anforderungstext des ISO 37001 durch den Anleitungsannex A, der ausdrücklich nur informativen Charakter hat; er gilt als „Guidance on the Use of this Document". Wer allerdings unmittelbare Referenzen zwischen den einzelnen Anforderungen und der Guidance erwartet, wird enttäuscht. Es besteht ein Zusammenhang allenfalls über die „Notes" im Anforderungstext. Dies sind, mit Fußnoten oder Anmerkungen vergleichbare Hinweisen unter den Anforderungsabschnitten des Haupttextes der ISO-Norm. Eine intensivere Verzahnung – etwa über gleiche Gliederungsziffern – wurde durch die Autoren nicht vorgenommen. Dies betrifft insbesondere den Aufbau des Anleitungsannexes, der sich eher an einzelnen Sonderthemen (wie etwa Risikoanalyse, Ressourcen oder Due Diligence) denn der Gliederung des Hauptteils in seine funktionalen Bereiche orientiert.

Der Antibestechungsstandard sieht vier Grade der Verbindlichkeit von Anforderungen vor: (1) Anforderung (shall), (2) Empfehlung (should), (3) Erlaubnis (may) und (4) Möglichkeit (can). Bei der ersten Durchsicht des Anforderungsteils des ISO 37001 ist das Verb „shall" das Meistverwendete – die Häufigkeit des Wortes „can" kann man an den Fingern einer Hand abzählen. „Should", „may" und „can" sind dem Anleitungsannex vorbehalten.

Das Grundprinzip Nr. 1 der UK Guidance, dass ein Antibestechungs-CMS „reasonable and proportionate" sein muss, ist für ISO 37001 nur ein Kapitel im Anleitungsannex wert. Dabei wäre es sinnvoll gewesen, den Anforderungskatalog im Sinne von Mindestanforderungen zu gestalten, die je nach Unternehmensgröße und -ausrichtung anpassbar sind. Die Autoren des Standards haben den Mut zu einer flexiblen Anforderungsgestaltung nicht aufgebracht – sie hoffen wohl aber auf eine Reduzierung der Verpflichtungen bei der Bemessung der Umsetzung der Anforderungen. Diese Betrachtung bleibt aber letztendlich dem Prüfer oder Zertifizierer vorbehalten und gibt diesen Personen eine entsprechende Macht.

Schon bei ISO 19600 wurden bei einem, sonst vorherrschenden hohen Detaillierungsgrad keinerlei Hinweise auf mögliche Anforderungsreduktionen gegeben, so dass im Zweifel wohl immer auf eine vollständige Umsetzung hingewirkt werden wird – gerade aus Risiko- oder Haftungsgesichtspunkten. Wirklich mittelstandsfreundlich ist der Standard damit nicht.

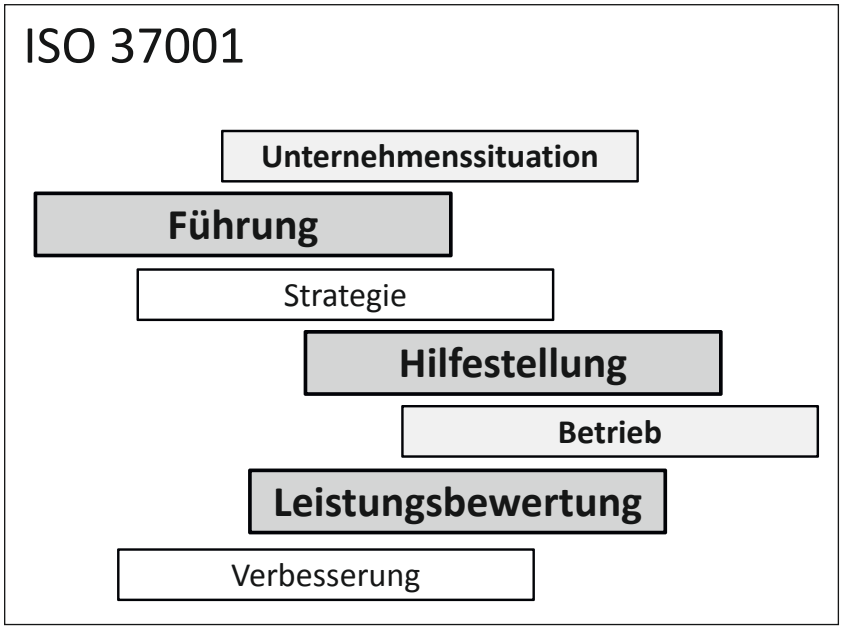

Abbildung 1: Bereiche eines AB-CMS nach ISO 37001

3.1 Unternehmenssituation

Beide ISO-Standards setzen als Grundlage auf einem Verständnis des Unternehmens, seines Umfelds und seiner Situation auf. Dabei fordert ISO 37001 nun regelmäßige und auch dokumentierte Bestechungsrisiko-Assessments (Bribery Risk Assessment), die auch bereits bestehende Kontrollen mit einer Geeignetheit und Wirksamkeitsprüfung erfassen sollen. Weitere Ausführungen hierzu gibt es dann im Anleitungsannex. Hier folgen – insoweit auf das Bestechungsthema bezogen – die Empfehlungen im Wesentlichen den Grundaussagen von ISO 19600.

ISO 37001 folgt dem Aufbau des ISO 19600 aber nicht dem Ansatz.

Das Unternehmen muss alle wesentlichen externen und internen Anhaltspunkte für Bestechungsrisiken berücksichtigen: Der regulatorische, soziale und kulturelle Kontext (das gesellschaftliche Umfeld), der Unternehmenszweck, die wirtschaftliche Situation (das wirtschaftliche Umfeld), bereits bestehende interne Regeln, Verfahren (Prozesse), Vorgehensweisen (Prozeduren) und die zur Verfügung stehenden Ressourcen. Auch sind alle relevante Personen und deren Interessen einzubeziehen. Ferner sind die Wechselwirkungen auf Unternehmensergebnisse und Compliance-Ergebnisse zu beachten und einzuschätzen. Wie eine Risikoanalyse durchzuführen ist, wird dann mit teilweise hoher Detailtiefe im Anleitungsannex beschrieben.

3.2 Führung

Die Führung und das Engagement (Commitment – auch Bekenntnis) für Compliance liegen bei der Geschäftsleitung (Governing Body) und dem Top-

ISO 37001 besteht aus einem Anforderungskatalog mit einem Anleitungsannex.

management. Der Geschäftsleitung obliegt es, die Anti-bribery-Policy des Unternehmens zu verabschieden und auch die Unternehmensstrategie insgesamt darauf abzustimmen. Sie ist der Empfänger von Berichten und muss für eine ausreichende Ausstattung des auf Antibestechungsthemen fokussierten Compliance Managementsystems (Antibestechungs-CMS) sorgen. Letztendlich ist die Geschäftsleitung auch letzte Kontrollinstanz. Ausführenden Aufgaben obliegen dem Topmanagement. Diesem Führungsmodell liegt ein gesellschaftsrechtliches One-Tier-Modell zugrunde. Ein Board umfasst sowohl Managing Directors als auch Non-executive Directors mit Beratungs- und Überwachungsaufgaben. Hier lassen sich die Aufgaben zwischen Gremium und dem eigentlichen Management trennen. Bei einer GmbH wird die gesamte Aufgabe eher bei der Geschäftsführung liegen. Im Falle einer Aktiengesellschaft dürfte allenfalls eine letzte Kontrollinstanz beim Aufsichtsrat bestehen – sonst ist auch hier der Vorstand allein zuständig und gesamthänderisch verantwortlich.

Kern der Führung ist die Antibestechungsrichtlinie. Sie muss Bestechung ausdrücklich verbieten und in ihrem Inhalt und Umfang den Geschäftszwecken des Unternehmens entsprechen. Sie stellt den Rahmen für die Festlegung, Umsetzung und Überwachung der Antibestechungsziele dar und postuliert das Bekenntnis des Unternehmens gegen Bestechung und der kontinuierlichen Verbesserung des Antibestechungs-CMS. Die Richtlinie muss zudem vorschreiben, dass jedes Vorgehen gegen Bestechungsrisiken oder -handlungen nicht sanktioniert werden darf und auch frei von negativen Gegenmaßnahmen sein muss. Sie legt auch die Kompetenz und Unabhängigkeit der Antibestechungsfunktion fest und beschreibt die Konsequenzen der Nichtbefolgung der Vorschriften. Selbstredend muss die Antibestechungsrichtlinie im Unternehmen kommuniziert werden und für jeden Interessierten frei verfügbar sein.

Im Unternehmen sind Rollen, Verantwortung und Zuständigkeit für die Umsetzung des Antibestechungs-CMS festzulegen – und zwar auf jeder Ebene der Unternehmensorganisation. Grundsätzlich zuständig sind die Führungskräfte, aber jedem von Bestechungsrisiken Betroffenen muss seine Rolle und Aufgabe klar sein. Dafür ist die Geschäftsleitung aber auch jeder Einzelne für sich selbst verantwortlich. ISO 37001 baut damit auch auf der Eigenverantwortung des Einzelnen auf. Es ist die Aufgabe des Unternehmens, die Wahrnehmung der Eigenverantwortung zu ermöglichen.

Der Antibestechungsfunktion obliegt die Umsetzung und insbesondere auch die Unterstützung und Anleitung der Mitarbeiter des Unternehmens. Sie muss über den Compliance-Status sowohl an die Geschäftsleitung wie auch an eine übergeordnete Compliance-Funktionen im Unternehmen berichten. Wichtig ist ihre ausreichende Ausstattung, damit sie ihre Aufgabe auch wirksam wahrnehmen kann. Diese Aufgabe ist auch außerhalb des Unternehmens delegierbar. Ausdrücklich ist auch eine Delegation innerhalb des Unternehmens möglich. Insbesondere bei einer internen Delegation muss aber sichergestellt sein, dass der Übernehmer der Antibestechungsfunktion selbst frei von Interessenkonflikten entscheiden kann, dabei aber über ausreichend Macht und Standing im Unternehmen verfügt. Bei jeder Delegation verbleibt aber eine Kontroll- und Überwachungspflicht bei der Geschäftsleitung.

Im Anleitungsannex werden die Anforderungen an eine Delegation näher ausgeführt: Die entsprechende Stelle muss Kompetenz, Status, Autorität und Unabhängigkeit haben und mit ausreichenden Personal-, Ausstattungs- und finanziellen Ressourcen ausgestattet werden. Hier erfolgt auch ein Hinweis auf ISO 19600, der sich dem Thema Führung stärker widmet.

3.3 Strategie

Das Antibestechungs-CMS soll auf der Grundlage der Risikoanalyse und unter Berücksichtigung der Unternehmenssituation sowie der Antibestechungsrichtlinie geplant werden. Bei der Zielplanung müssen die festzulegenden Ziele erreichbar und messbar sein. Die Planung hat die Überwachung im Sinne von Kontrolle und Wirksamkeitsprüfung des CMS im Hinblick auf eine kontinuierliche Verbesserung zu berücksichtigen. Hier sollen konkrete Ergebnisse feststellbar und auch Korrekturen der Ziele und der Maßnahmen zu ihrer Erreichung möglich sein. Dies bedeutet, dass Ziele nicht allgemein, sondern spezifisch zu definieren sind. Bei der Zielplanung sind auch die Auswirkungen der Zielsetzung zu beachten: Unerwünschte Auswirkungen sind zu vermeiden. Bei der Umsetzungsplanung sind dann Maßnahmen, Ressourcen und Verantwortlichkeiten zur Zielerreichung zu bestimmen. Zudem müssen Fristen für die Zielerreichung, ihre Messung sowie Bewertung und entsprechende Berichtspflichten definiert sein. ISO 37001 verlangt an dieser Stelle auch eine Aussage darüber, wer bei Verstößen und Zuwiderhandlungen Sanktionen oder Strafen verhängt. Die Planung ist – wie alle Vorgänge um das Antibestechungs-CMS zu dokumentieren.

3.4 Hilfestellung

Das Unternehmen muss die für den Aufbau, die Umsetzung, den Erhalt und die kontinuierliche Verbesserung des Antibestechungs-CMS erforderlichen Ressourcen planen und dann bereitstellen. Sofern nicht im Unternehmen bereits vorhanden, sind die dazu erforderlichen Kompetenzen zu beschaffen.

Dies betrifft nicht allein die Antibestechungsfunktion und damit die Compliance-Organisation sondern die gesamte Belegschaft eines Unterneh-

mens. Es gilt das Prinzip der Eigenverantwortung. Schon bei der Einstellung ist darauf Wert zu legen, dass nur solches Personal eingestellt wird, das Gewähr für Compliance mit den Antibestechungsmaßnahmen bietet. Diese Anforderung erschöpft sich nicht nur auf die Einstellung als solche, sondern umfasst den gesamten Prozess der Personalverwaltung (und wohl auch Personalentwicklung). Die Belegschaft ist umfassend zu informieren, Sanktionssysteme für Zuwiderhandlungen sind zu definieren. Es ist sicherzustellen, dass es keine negativen Folgen für diejenigen gibt, die sich weigern, an Geschäften mit mehr als nur geringem Bestechungsrisiko zu beteiligen oder die auf Bestechungsrisiken hinweisen. Anreizsysteme um Bestechungsrisiken wirksam anzugehen sind aber als Anforderung nicht für erforderlich gesehen worden. Insgesamt entsteht so der Eindruck einer äußerst repressiven Compliance-Kultur, die keineswegs modernen Führungs-Gesichtspunkten entspricht.

Insgesamt erscheinen diese Anforderungen als gut gemeint aber wenig praxisnah. Wenn in Zukunft die Weigerung ohne Konsequenzen bleibt, sich an Geschäften mit mehr als nur geringem Bestechungsrisiko zu beteiligen – wer definiert dann im Unternehmen, ob das Bestechungsrisiko gering oder höher ist? Ist die anfängliche Risikoanalyse ausschlaggebend (Bruttorisiko) – oder müssen dabei Maßnahmen des Unternehmens zur Eindämmung und Beherrschung von Compliance-Maßnahmen berücksichtigt werden (Nettorisiko)? Ist es dann die Aufgabe der Antibestechungsfunktion oder die Managements? Wer gibt die erforderlichen Anweisungen an die Belegschaft, wenn die (folgenlos) dazu ermuntert wird, sich dem zu widersetzen?

Überall dort wo es mehr als nur geringe Bestechungsrisiken gibt, sind Personaleinstellung nur nach vorheriger genauester Prüfung der Kandidaten (Due Diligence) möglich. Zielvereinbarungen und Anreizsysteme im Unternehmen sind auf mögliche Auswirkungen auf Bestechungsrisiken zu untersuchen. Personal im Einsatzgebiet mit mehr als nur geringem Bestechungsrisiko muss die Kenntnis des Risikos und der Gegenmaßnahmen bestätigen – und dann auch genauestens einhalten. Abgesehen von der wachsenden Unternehmensbürokratie ist dies als Anforderung wohl kaum umzusetzen.

Die Belegschaft muss wach im Hinblick auf Bestechungsgefahren sein und ist zum Thema Bestechungsrisiken ausreichend zu schulen. Die Schulung muss über die Folgen von Bestechungsvorfällen für das Unternehmen aufklären, darstellen in welchen Situationen Bestechungen vorkommen können, wie diese erkannt werden können und wie man angemessen im Einzelfall darauf reagieren kann. Entsprechende Prozesse sind zu etablieren. Die Schulungen müssen auch den Beitrag des einzelnen Mitarbeiters sowohl zum Antibestechungs-CMS als auch der kontinuierlichen Verbesserung des CMS umfassen. Für Kommunikation und Schulung ist ein umfassendes Konzept erforderlich, dass umfassende Schulungsthemen für jeden Mitarbeiter vorsieht. Alles, auch die Aktualisierung und die Kontrolle der Schulung, ist zu dokumentieren.

Der Anleitungsannex enthält einen größeren Abschnitt zur Geschäftspartnerprüfung. Hier muss verifiziert werden, ob der Geschäftspartner wirklich legal existiert und ausreichende Qualifikation, Erfahrung sowie Ressourcen für ein wirkungsvolles Antibestechungsengagement mit sich bringt. Dabei können die erforderlichen Informationen über Fragebogen, Internetrecherchen, Behördeninformationen, öffentliche (schwarze) Listen, Drittreferenzen und dem weiteren Einsatz fachkundiger Dritter erfasst werden. Dabei wird darauf hingewiesen, dass ein solcher Geschäftspartnercheck kein perfektes Tool ist und die Informationen nur ein Teil eines adäquaten Risikomanagements darstellen können.

3.5 Betrieb

Den operativen Bereichen des Unternehmens obliegt die Umsetzungsplanung für Maßnahmen im Rahmen des Antibestechungs-CMS. Ist das Bestechungsrisiko mehr als nur niedrig, müssen Natur und Umfang des konkreten Bestechungsrisikos für jede einzelne Transaktion, jedes Projekt, ja jede Geschäftsaktivität, jeden Geschäftspartner und auch jeden Mitarbeiter bestimmt werden. Hierzu ist ausreichendes Informationen beizubringen und stets aktuell zu halten (Due Diligence) sowie die Informationen stets im Hinblick auf Bestechungsrisiken zu untersuchen. In den operativen Bereichen sind Finanzkontrollen zu etablieren – neben Kontrollen in allen anderen Bereichen des Unternehmens.

Trotz der vielen Anforderungen an die Geschäftsleitung und Compliance setzt ISO 37001 auf Eigenverantwortung der Mitarbeiter.

Diese Maßnahmen müssen auch in einem Konzern für alle Tochtergesellschaften und beherrschten Beteiligungsunternehmen durchgeführt werden. Auch sämtliche Geschäftspartner eines Unternehmens sind betroffen. Es muss geprüft werden, ob Geschäftspartner Antibestechungskontrollen implementiert haben und wie sie mit Bestechungsrisiken umgehen. Werden hier Defizite festgestellt, müssen gegenüber Geschäftspartnern Antibestechungsmaßnahmen getroffen werden. Ist dies nicht möglich, so sind diese Defizite ein Kriterium für die weitere Zusammenarbeit und auch für Überwachungsmaßnahmen bei der Fortsetzung einer Zusammenarbeit. Als Anforderung werden Antibestechungsverpflichtungen (Commitments) verlangt – dabei bleibt es offen, ob dies standardmäßige Compliance-Klauseln in Verträgen sein können oder hier mehr verlangt wird. In den Verträgen mit Geschäftspartnern muss jedenfalls sichergestellt sein, dass das Geschäftsverhältnis im Falle von Bestechungsvorfällen kündbar ist.

Diese Anforderung gegenüber Geschäftspartnern kann zu einem kaskadenförmigen Zwang

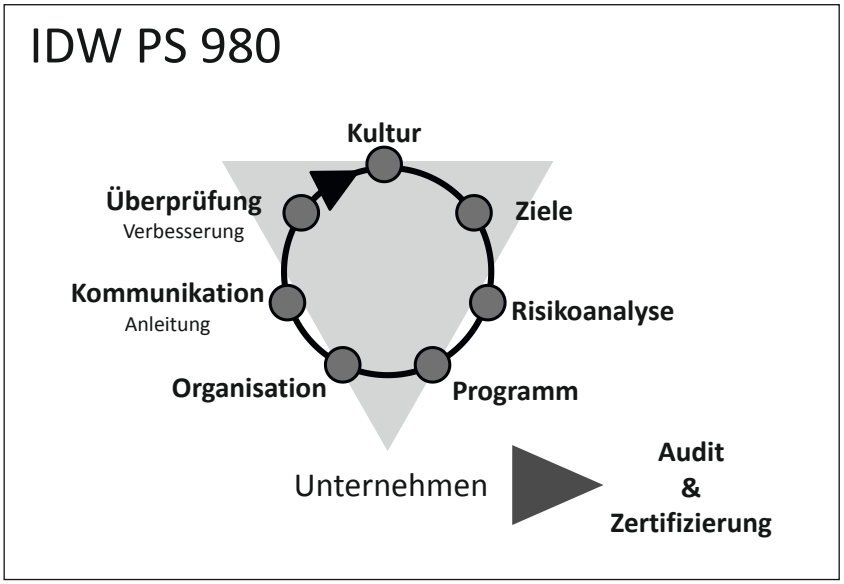

Abbildung 2: Elemente eines CMS nach IDW PS 980

führen, Geschäftspartner und Untergeschäftspartner mit Anforderungen im Sinne des ISO 37001 zu konfrontieren.[6] Idealerweise ist eine Zertifizierung nach ISO 37001 vorzuweisen. Im Hinblick auf die Entwicklung bei der ISO 9000-Welle kann nicht ausgeschlossen werden, dass das Projektkomitee der ISO darauf baut.

ISO 37001 setzt auf kontinuierliche Verbesserung des CMS und fordert stets entsprechende Maßnahmen.

ISO 37001 verlangt auch Prozesse zur Verhinderung von Geschenke, Einladungen, Spenden und ähnlichen Vorteilen, die als Bestechung angesehen werden könnten. Es gibt auch Anforderungen für einzelne Projekte oder Geschäfte: Sollte ein Risiko bestehen, dass das Antibestechungs-CMS des Unternehmens in Bezug auf drohende Bestechungsrisiken nicht ausreichende Vorkehrungen bietet, müssen Kündigungen, Leistungsunterbrechungen sowie -suspendierung oder ein Rücktritt von bestehenden Vorgängen geprüft werden. Neue Projekte müssen verzögert oder ihre Weiterführung unterbrochen werden.

Nochmals wird auch in diesem Abschnitt betont, dass es möglich sein muss, ohne Furcht vor negativen Konsequenzen über Bestechungsrisiken zu berichten. Derartige Reports sind zu fördern; Vertraulichkeit und Anonymität ist zu gewährleisten. Schon im Voraus müssen Verfahren angelegt werden, wie bei einem Verdacht von Bestechungen dann Untersuchungen der Bestechungsvorfälle durchgeführt und wie mit diesen Vorfällen umgegangen wird. Es muss ein unabhängiger Untersuchungsverantwortlicher bestimmt und beauftragt werden, betroffene Mitarbeiter müssen mitwirken, Ergebnisse sind an die Antibestechungsfunktion zu berichten. Die Untersuchung und ihre Ergebnisse sind vertraulich zu behandeln. Untersuchungen können auch an Externe delegiert werden. Vorausgesetzt das jeweilige nationale Arbeits- und Datenschutzrecht lässt dies zu ...

3.6 Leistungsbewertung

Die Bewertung des Antibestechungs-CMS, seine Überwachung, die Messung seiner Erfolge, deren Analyse und Beurteilung ist zu planen. Dies gilt auch für eine Revision des Antibestechungs-CMS. Die Überwachung, Prüfung und Bewertung muss verhältnismäßig sein und Risiko-basiert erfolgen. Im Falle von Bestechungsvorfällen und -verdachtsfällen aber auch anderen Zuwiderhandlungen gegen die Vorschriften des Antibestechungs-CMS müssen Untersuchungen eingeleitet werden. Erkenntnisse daraus sind für die kontinuierliche Verbesserung des CMS zu verwenden. Die Überwachung ist unabhängig zu gestalten – keiner darf seine eigene Arbeit prüfen. Dabei müssen Prüfungen nicht durch die Revision sondern können auch durch andere erfolgen.

Die Geschäftsleitung muss selbst prüfen – und dies wird auch für den Aufsichtsrat einer AG gelten (siehe oben Ziff. 2). Dabei ist es nicht erforderlich, dass der Aufsichtsrat eigene Prüfungshandlungen vornimmt und etwa in Prozesse bestimmter (risikobehafteter) Unternehmensbereiche einsteigt. Ihm ist aber zuzumuten, die Berichte der Revision zu prüfen und aus der Gesamtsituation heraus selbst den Status des Antibestechungs-CMS im Unternehmen einzuschätzen. Hier könnte ein Einsatzbereich auch von Wirtschaftsprüfern nach dem IDW PS 980 bestehen. Mehr als die Zertifizierungsunternehmen haben Wirtschaftsprüfer den Kontakt zu Aufsichtsräten und kennen deren Arbeitsweise und Überwachungskultur.

3.7 Verbesserung

Nachdem auf die Notwendigkeit der kontinuierlichen Verbesserung (Kaizen) in nahezu jedem einzelnen Abschnitt des ISO 37001 Standards hingewiesen wurde, ist dieser Abschnitt jetzt recht kurz. Das Unternehmen muss auf Verstöße reagieren und sie müssen Anlass für eine Verbesserung sein.

4 IDW PS 980

Das Deutsches Institut der Wirtschaftsprüfer hat 2011 den Prüfungsstandard IDW PS 980 für Compliance-Management-Systeme veröffentlicht. Dieser Standard ist ein Prüfungsstandard, der auch Hinweise für Mindestanforderungen an wirksame Compliance-Management-Systeme als Auditgrundlage beinhaltet. Diese Mindestanforderungen – wie überhaupt die Prüfungsanforderungen als solche – wurden von zahlreichen Compliance-Standards (unter anderem AS 3806-2006, US-FSGO 2010 sowie der Guidance zum UK Bribery Act 2010) abgeleitet. Der Prüfungsstandard geht von sieben Elementen aus: Compliance-Ziele, -Risiken, -Programm, -Orga-

6 Vgl. im Hinblick auf die Auswirkungen der ISO 9001-Zertifizierungen, Schlegel, W.: Der Standard TR CMS 101 von TÜV Rheinland, ZRFC 2/16, S. 55, 59.

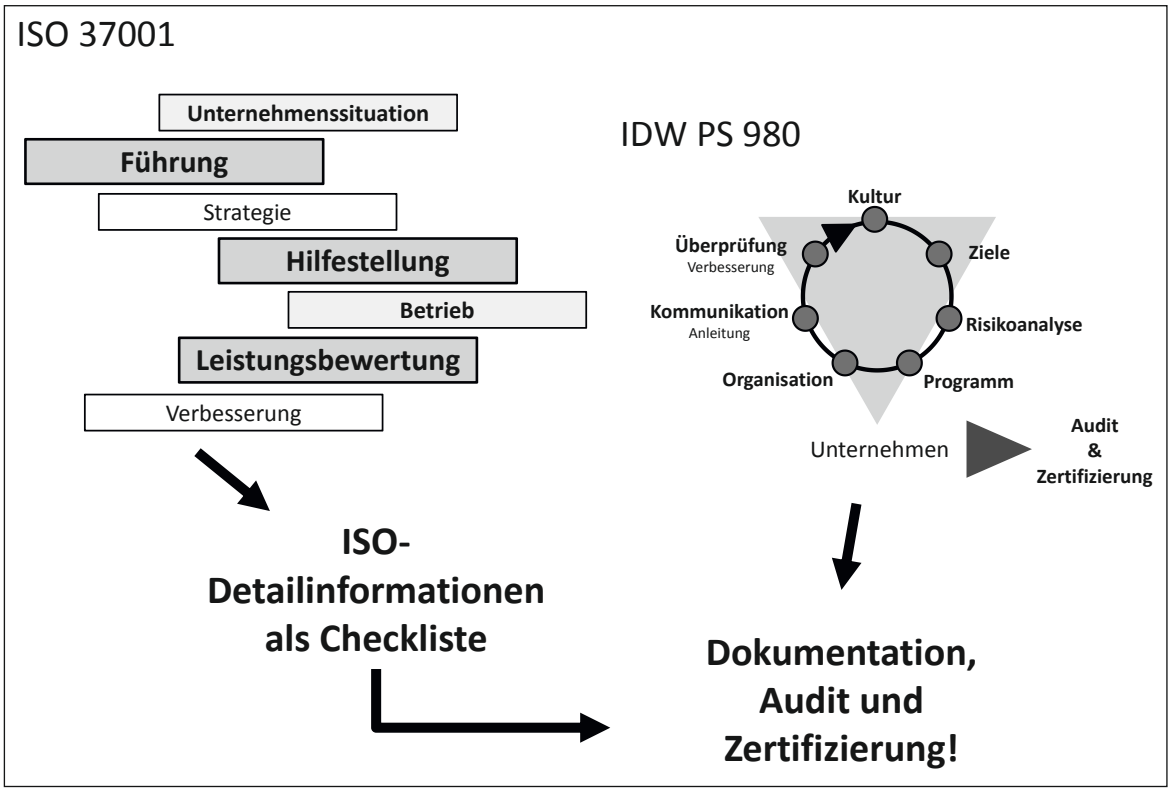

Abbildung 3: Kombination eines Ansatzes mit ISO 37001 und IDW PS 980

nisation, -Kommunikation, -Überwachung und -Kultur.[7] *(Abbildung 2)*

Bei einem Vergleich zwischen den neuen ISO-Standards und dem gar nicht so alten IDW Prüfungsstandard 980 droht eine Verwirrung zwischen den unterschiedlichen Begriffswelten. Jeder Compliance-Ansatz arbeitet mit seiner eigenen Begriffswelt. Eine intensive Begriffsklärung ist insbesondere dann erforderlich, wenn der ISO-Standard als Rahmenkonzept zur Grundlage einer IDW PS 980 Prüfung genommen werden soll.

Es treffen offensichtlich unterschiedliche Welten zusammen: Im IDW-Standard die Welt des betriebswirtschaftlichen Risikomanagements sowie der Wirtschaftsprüfer und im ISO-Standard die Welt des technisch geprägten Qualitätsmanagement. Eine Welt ist daran interessiert, Compliance in die Prozesse und Prozeduren der Unternehmen einfließen zu lassen. Die andere Welt versucht eine zusammenfassende Gesamtschau aus der Perspektive der Geschäftsleitung sowie des Aufsichtsrates. Dabei muss festgestellt werden, dass der IDW PS 980 nach seinem Standarddokument deutlich sorgfältiger vorbereitet wurde.

Es hat den Anschein, als würde die Welt des Qualitätsmanagements mit dem ISO 37001-Standard auf die Perspektiven der Geschäftsleitungen und Aufsichtsgremien wie auch die Wirtschaftsprüfer zielen. Hier wird aber eine unmittelbare Konkurrenz zu einer Vorgehensweise im Sinne des IDW PS 980 bestehen.

5 Kritik

Der ISO-Standard 37001 ist trotz seines Anforderungscharakters überaus detailreich. Zudem gibt es noch eine wohlmeinende Guidance als Anleitungsannex dazu. Betrachtet man dieses Werk nicht mit einer QM-Brille aus der Perspektive der ISO-Philosophie, kann man in ihm eine weitere CMS-Checkliste sehen – ganz speziell auf das Thema Antibestechung zugeschnitten. Dabei werden subtilen Methoden der Beeinflussung (eben Korruption) noch nicht einmal von dieser Checkliste reflektiert. So kann auch der Mittelstand mit den überbordenden Anforderungen gut umgehen. Die Verwendung als Checkliste in Zusammenhang mit einem anderen Prüfungsverfahren (etwa IDW PS 980) erlaubt eine vernünftige Eingrenzung und kann in dem weiten Anforderungsfeld unter Einbezug der Empfehlungen des Anleitungsannexes insgesamt eine Materialsammlung zum Aufbau eines effektiven Antikorruptions-CMS darstellen. *(Abbildung 3)*

ISO 37001 ist als Grundlage für eine IDW PS 980 Prüfung geeignet.

Es besteht aber die Gefahr der großen Vereinfachung: Einkaufsorganisationen internationaler Konzerne werden sich unter Anleitung des Risikomanagements möglicherweise auch auf dem Feld der Antibestechungs-Compliance auf ISO-Normen stürzen. Nachdem in mühsamen Verhandlungen

7 Siehe: Schefold, C.: Compliance-Management-Systeme nach deutschem Standard, ZRFC 5/2011, S. 221 ff.

Inwieweit Qualitätsmanagement-Ansätze für die Beurteilung von Compliance-Maßnahmen geeignet sind, bleibt abzuwarten.

die Allgemeingeltung der Verhaltenskodizes globaler Unternehmen auf ein erträgliches Maß reduziert und die Gegenseitigkeit bestehender Antikorruptionsbestimmungen durchgesetzt haben, beginnt nun wohl eine neue Welle von Forderungen nach Zertifizierungen, Verhandlungen und Gegenmaßnahmen. Die Erfahrungen mit den Zertifizierungswellen im Qualitätsmanagement werden sich wiederholen. Ist Compliance aber Qualitätsmanagement?

In manchen Bereichen kann Compliance sich der Methoden und Erfahrungen des Qualitätsmanagements bedienen. Im Gegensatz zu technischen und prozessualen Vorgaben muss Compliance aber mit rechtlich-soziologischen Verhaltensmustern umgehen. Hier ist eine andere Vorgehensweise gefragt. Mögen technische Überwachungsvereine und Zertifizierer wie der TÜV Rheinland von der Prüfung der MARisk- oder MAComp-Compliance der Banken träumen,[8] die Wirklichkeit wird anders aussehen. Können Qualitätsprobleme durch technische und prozessuale Anforderungen noch verhindert werden, sieht dies auf dem Feld der Rechtstreue anders aus. Viel zu vielschichtig sind Verhaltensmuster und ihre Konsequenzen. Wie können die Anforderungen der Dokumentation und Compliance-Leistungsmessung mit Arbeitsrecht und Arbeitnehmerdatenschutz in Einklang gebracht werden? ISO 37001 verlangt unter anderem ein anonymes Hinweissystem und die Allzuständigkeit der Compliance-Funktion – wie können dabei Verfahrensrechte der Betroffenen und auch der Unternehmen selbst gewahrt werden?

Ein korrekter und auch durchaus selbstkritischer Warnhinweis ist in der Einführung des ISO 37001 bereits enthalten: Die Übereinstimmung mit dem Antibestechungsstandard allein genügt nicht, um Bestechung oder gar Korruption in der jeweiligen Organisation auszuschließen. Die Übereinstimmung mit ISO 37001 kann allenfalls helfen, das Korruptionsrisiko zu senken. Hier sind Compliance- und Rechtsabteilungen aber auch die Interne Revision im Unternehmen weiterhin gefragt.

8 Siehe Schlegel, W.: Der Standard TR CMS 101 von TÜV Rheinland, ZRFC 2/2016, S. 55, 61.