

Antikorrupptionsmanagementsysteme nach ISO 37001

Im Blickpunkt: Aufbau, Anforderungen, Umsetzung und Zertifizierung in Unternehmen

Von Johannes Breit, Maxim Huttenlocher und Andreas Pyrcek

Korruption und Bestechung erlangen in den Medien nach wie vor große Aufmerksamkeit, und es ist leider häufig darüber zu berichten. Unternehmen verschiedenster Branchen und Größen sind immer noch die Täter – und Fälle wie beispielsweise bei Telia Schweden, Soci t  G n rale, Odebrecht oder zahlreichen deutschen Unternehmen verdeutlichen immer wieder, wie allgegenwrtig dieses Unternehmensrisiko ist und wie lange sich Skandale in den Medien halten k nnen. Zudem kam es in letzter Zeit zu einer vermehrten Vollstreckung internationaler Gesetze wie des US Foreign Corrupt Practices Act (FCPA) oder auch zu der nun anlaufenden Nutzung des UK Bribery Act (UKBA), was nachfolgend zu einem wesentlichen finanziellen Schaden, Reputationseinbuen und einer nachhaltigen Transformation des Unternehmens f hrte. Diese Entwicklung von regulatorischen Anforderungen wiederum f hrte dazu, dass sich Antikorrupptionsmanahmen mittlerweile als ein fester Bestandteil eines jeden Compliancemanagementsystems (CMS) bei groen und mittelstndischen Unternehmen etabliert haben. Jedoch fehlten bis dato einheitliche globale Vorgaben durch einen Standardsetter, wie ein CMS f r das Risikogebiet Antikorrupktion auszugestalten sei. Dies f hrte in der Praxis, beispielsweise bei der Auswahl geeigneter Lieferanten oder bei einem Strafverfahren



Die Einf hrung eines Compliancemanagementsystems nach ISO 37001 und gegebenenfalls dessen externe Zertifizierung k nnen sich lohnen.

wegen Korruption, zu gewissen Schwierigkeiten in der Bewertung eines umfassenden und systematischen Ansatzes zur Prvention von Korruption und Bestechung im Unternehmen.

Um eine internationale Vergleichbarkeit im Bereich Antikorrupktion zu schaffen, ver ffentlichte die Internationale Organisation f r Normung (ISO) im Oktober 2016 die Norm ISO 37001:2016 auf der Grundlage des „British Standard 10500“ und mit Bezugnahme auf internatio-

nale Antikorrupptionsprinzipien. Die ISO 37001 wurde bewusst flexibel ausgestaltet und erm glicht so eine Implementierung unabhngig von Branche, Unternehmensgr e oder geographischer Prsenz des Unternehmens. Weiterhin kann die ISO 37001 unabhngig oder parallel zu anderen ISO-Managementsystemen implementiert werden. So manifestiert sich die ISO 37001 zum ersten globalen Standard f r die Komponenten eines systematischen Antikorrupptionscompliance systems. ▶

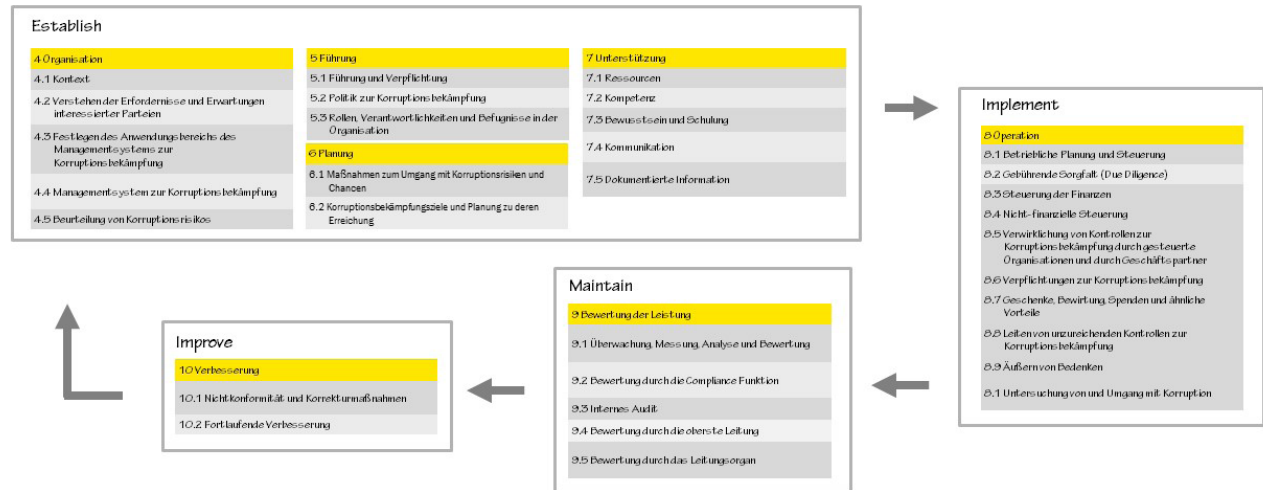
Inhalte der ISO 37001

Der seit Mai 2018 auch auf Deutsch erhältliche Standard ISO 37001:2016 selbst umfasst 47 Seiten und folgt den etablierten Prinzipien „Establish – Implement – Maintain – Improve“ (vormals „Plan – Do – Check – Act“). In der folgenden Darstellung sind die einzelnen Kapitel des ISO-37001-Standards den genannten Prinzipien zugeordnet. Die nicht aufgeführten Kapitel 1–3 beinhalten den Anwendungsbereich, normative Referenzen sowie Begriffe und Definitionen. Diese Kapitel bieten nur einen allgemeinen Überblick und sind für eine Zertifizierung nicht relevant.

Wie bei vergleichbaren nationalen oder auch allgemeineren Standards (wie etwa dem IDW PS 980 oder auch den Transparency-International-Standards in Bezug auf Antikorrupcion) besteht auch hier Einvernehmen darüber, dass durch ein Compiance-system nach ISO 37001 Korruption oder Bestechung im Unternehmen nicht eliminiert werden können. Auch die ISO 37001 ist nicht realitätsfremd und gesteht ein, dass es immer Individuen geben wird, die gegen ein etabliertes System arbeiten werden, um persönliche Ziele oder Unternehmensziele zu erreichen. Die Stärke der ISO 37001 liegt jedoch in der klaren Betonung des systematischen Ansatzes zur Reduzierung des Korruptionsrisikos im Unternehmen. Alle aufbau- und ablauforganisatorischen Aktivitäten sollen geplant, aufeinander abgestimmt, gelebt, dokumentiert und auch überwacht werden. Dies geht im Vergleich zu anderen Standards noch über die Komponenten eines wirksamen CMS hinaus.

Establish

Das Prinzip „Establish“ umfasst die Kapitel 4 „Organisation“, 5 „Führung“, 6 „Planung“ und 7 „Unterstützung“, die als Grundelemente zur Etablierung eines Antikorrupcion-compiance-systems gegeben sein müssen.



Quellen: EY, eigene Darstellung.

Organisation

Ein wesentlicher Aspekt des Abschnitts „Organisation“ ist die Bestandsaufnahme der internen und externen Faktoren, die Einfluss auf Korruption haben könnten („Umfeldanalyse“), beispielsweise die geographische Lage und die globalen Aktivitäten, die Unternehmensorganisation, die Branche des Unternehmens. Auch die Anforderungen hinsichtlich verschiedener Interessengruppen müssen identifiziert werden. Die jedoch wichtigste Anforderung des Kapitels ergibt sich aus

der Etablierung und Durchführung einer auf Korruption fokussierten systematischen Risikoanalyse. Ziel ist es, Korruptionsrisiken zu priorisieren und den Risiken entsprechende Kontrollen einzuführen. Zudem müssen nachweislich entsprechende personelle und finanzielle Ressourcen bereitgestellt werden, um die identifizierten

Korruptionsrisiken zu vermindern.

Die Risikoanalyse und die Effektivitätsbeurteilung der eingeführten Maßnahmen und Kontrollen müssen innerhalb einer selbstgesetzten Frist regelmäßig durchgeführt und eigens überprüft werden. Dies gilt auch, wenn es zu signifikanten Änderungen in der Struktur oder in den Tätigkeitsfeldern des Unternehmens kommt. Hierdurch ist grundsätzlich eine Effektivität des Managementsystems sichergestellt.



Führung

Wie bei jedem erfolgreichen CMS sind der „Tone from the Top“ und die Unterstützung durch die Führungsebene entscheidend für den Erfolg, weshalb der ISO-Standard diese Punkte in Kapitel 5 explizit hervorhebt. Zudem muss eine unabhängige Compliancefunktion benannt werden, die auch für das Antikorruptionsmanagementsystem die Verantwortung trägt. Damit diese ihrer unabhängigen Rolle gerecht werden kann, müssen Interessenkonflikte konsequent vermieden werden.

Weiterhin wird in Kapitel 5 festgelegt, dass die Führungsebene dafür verantwortlich ist, eine an relevante interne wie auch externe Interessengruppen kommunizierte Antikorruptionsrichtlinie zu verabschieden. Diese muss unter anderem Korruption explizit verbieten und auch die Konsequenzen eines Verstoßes gegen die Richtlinie aufzeigen.

Planung

In der Komponentenplanung sollen Risiken und Chancen, die sich in Bezug auf Antikorruption ergeben, identifiziert und die Ziele („Objectives“) des Antikorruptionsmanagementsystems festgelegt werden. Bei der Planung, wie die gesteckten Ziele umgesetzt werden können, sollte man sich die folgenden Fragen stellen:

- Was soll getan werden?
- Welche Ressourcen sind notwendig?
- Wer ist verantwortlich?
- Wann können die Ziele erreicht sein?

- Wie werden die Resultate gemessen?
- Wer wird bei Verstößen Sanktionen oder Strafen verhängen?

Unterstützung

Für eine erfolgreiche Umsetzung des Managementsystems müssen ausreichend personelle, finanzielle und sonstige Ressourcen durch das Unternehmen zur Verfügung gestellt werden. Oftmals können hierbei bereits vorhandene personelle Complianceressourcen genutzt werden, allerdings müssen diese entsprechend der ISO 37001 geschult und ausgebildet werden und das Risikofeld wie auch die Anforderungen des Standards gut kennen.

Generell wird in diesem Kapitel ein Antikorruptionstraining für alle Beschäftigten, die mehr als einem geringen Korruptionsrisiko ausgesetzt sind, verlangt. Dies stellt sicher, dass hier mit Augenmaß und einer risikobasierten Planung vorgegangen werden kann. Ein Antikorruptionstraining für sämtliche Mitarbeiter wird explizit nicht gefordert. Ein weiterer wichtiger Bestandteil des Kapitels ist der Fokus auf den Personalprozess. So muss unter anderem sichergestellt sein, dass bei Einstellungen oder Beförderungen das Personal entsprechend überprüft wird. Auch sollten Leistungsvergütung und vereinbarte Leistungsziele so ausgestaltet werden, dass keine Korruption gefördert wird.

Implement

Das Prinzip „Implement“ enthält das Kapitel 8 „Betrieb“.

Betrieb

Das Kapitel „Betrieb“ enthält konkrete Ausgestaltungshinweise für das Managementsystem. Ein wichtiger Abschnitt behandelt das Thema Due Diligence. So müssen Transaktionen, Projekte, Personal und Geschäftspartner, die einem mehr als geringen Korruptionsrisiko ausgesetzt sind, standardmäßig einem Due-Diligence-Prozess unterworfen werden.

Weiterhin müssen finanzielle und nichtfinanzielle Kontrollen eingeführt werden. Dies kann beispielsweise durch ein Vier-Augen-Prinzip bei wichtigen Transaktionen oder ein transparent durchgeführtes Vergabeverfahren für Aufträge geschehen. Es ist wichtig zu beachten, dass die ISO explizit fordert, dass auch Geschäftspartner („Business Associates“) in die Kontrollen einzubeziehen sind. Im Zweifel müssten Kontrollen bei Geschäftspartnern überprüft sowie deren Einführung gefordert werden – selbstverständlich nur bei Geschäftspartnern, die einem mehr als geringen Korruptionsrisiko ausgesetzt sind. Allerdings fasst die ISO 37001 den Begriff „Geschäftspartner“ bewusst relativ weit.

In diesem Kontext sollte jedoch auf das „Three Lines of Defense“-Konzept verwiesen werden: Der Standard fordert nicht, dass die Complianceorganisation diese Prozesse und Kontrollen durchführt. Sicherlich werden einzelne Aktivitäten bei den Complianceverantwort- ▶

lichen bleiben, aber die Planung, Umsetzung, Dokumentation und Überwachung der Implementierung und Wirksamkeit wird in der Complianceorganisation zu einem Schlüsselement. Dennoch wird sich eine Vielzahl der Aktivitäten in den operativen Einheiten eines Unternehmens wiederfinden.

Auch das Hinweisgebersystem ist als ein wesentliches Element in Kapitel 8 angeführt. Implementierte Verantwortlichkeiten, Systeme und Prozesse sollen sicherstellen, dass Hinweise auf mögliche Korruption entsprechend aufgenommen und verfolgt werden können. Außerdem verweist der Standard auf die Grundannahme, dass Hinweisgeber keine negativen Konsequenzen drohen, wenn sie die Meldekanäle nutzen (Schutz des Hinweisgebers).

Maintain

Unter das Prinzip „Maintain“ fällt das Kapitel 9 „Bewertung der Leistung“. Hierbei ist anzumerken, dass es sich nicht um die Vergütungskomponenten in Bezug zum Compiencesystem handelt, sondern um die systematische Überwachung des CMS durch das Unternehmen.

Bewertung der Leistung

Grundsätzlich sollte das Managementsystem, sofern möglich, messbar gemacht werden. Hierfür muss festgelegt werden, welche Compiencesystemkomponenten und -prozesse zu messen sind, welche Methoden hierfür

angewendet werden sollen und an wen was zu berichten ist.

Weiterhin fordert die ISO 37001 in Kapitel 9, dass regelmäßige Revisionsprüfungen in Bezug auf das Antikorruptionscompiencesystem durchgeführt werden. In diesen Prüfungen sind die eigenen Vorgaben hinsichtlich Antikorruption sowie die einzelnen Vorgaben der ISO 37001 zu auditieren. Die Ergebnisse müssen der Führungsebene nachweislich mitgeteilt werden, die wiederum auf dieser Grundlage Ressourcen bereitstellen kann, sollte dies für den Betrieb des Antikorruptionsmanagementsystems notwendig sein.

Improve

Das Prinzip „Improve“ enthält das Kapitel 10 „Verbesserung“.

Verbesserung

Der Grundgedanke eines jeden Managementsystems ist der kontinuierliche Verbesserungsprozess. Daher wird in Kapitel 10 „Verbesserung“ ein systematischer Prozess zur Verhinderung von Verstößen bzw. zur Behebung von Nichtkonformitäten in Bezug auf Anforderungen des Managementsystems gefordert (dies umfasst natürlich auch Prozessschwächen oder eine nicht vollständige Umsetzung systematischer Präventionsmaßnahmen). So sollte jede Nichtkonformität dazu führen, dass diese abgestellt und das Managementsystem, sofern nötig,

angepasst wird. Hierdurch ist eine kontinuierliche Verbesserung des Gesamtsystems sichergestellt.

Zertifizierung

Bei einer Zertifizierung des Antikorruptionsmanagementsystems nach ISO 37001 werden die im vorangegangenen Kapitel der ISO 37001 genannten Anforderungen auditiert. Grundsätzlich unterscheidet man zwischen drei Arten von Audits, die bei einer Zertifizierung durchgeführt werden:



Quellen: EY, eigene Darstellung.

Zertifizierungsaudit: initiales und auch umfangreichstes Audit. Hier wird das komplette Managementsystem auditiert. Sollte es den Anforderungen der ISO entsprechen, wird ein Zertifikat erstellt. In der Regel ist diese Phase mit sehr viel Dokumentationsanforderungen und Prüfungen verknüpft.

Überwachungsaudit: Im zweiten und dritten Jahr nach erfolgreicher Zertifizierung wird jeweils ein Überwachungsaudit durchgeführt. Dabei werden nur Teilbereiche des Managementsystems auditiert und die wirksame Umsetzung im Unternehmen geprüft. ▶

Rezertifizierungsaudit: Nach Ablauf von drei Jahren verliert das Zertifikat seine Gültigkeit. Bei einem Rezertifizierungsaudit wird das komplette Managementsystem ein weiteres Mal überprüft.

Vorteile einer Zertifizierung des Managementsystems

Wie in der Übersicht über die einzelnen Kapitel dargelegt, erfordert die Einführung und Zertifizierung eines Antikorruptionsmanagementsystems nach ISO 37001 personelle und finanzielle Ressourcen. Lohnt sich das? Drei Gründe sprechen dafür:

Vergleichbarkeit des Antikorruptionsmanagementsystems

Das Hauptziel des ISO-37001-Standards ist ein einheitliches Verständnis für den Aufbau und die kontinuierliche Verbesserung eines Antikorruptionsmanagementsystems. Hierdurch ergibt sich eine gewisse Vergleichbarkeit, die durch eine externe Zertifizierung bestätigt wird. Dies kann beispielsweise im Rahmen internationaler Ausschreibungen oder bei der Auswahl von Lieferanten durchaus von Vorteil sein. Es ist bereits in einzelnen Emerging Markets erkennbar, dass ISO-37001-Zertifikate als Mindestanforderungen in Ausschreibungen von Regierungen etc. genannt werden (etwa Malaysia, einzelne Provinzen in China, Singapur etc.).

Nachweis gegenüber Regulatoren

Eine externe Zertifizierung kann als international anerkannter Nachweis gegenüber Regulatoren dienen, dass Antikorruptionsmaßnahmen eingeführt wurden oder ein systematischer Ansatz zur Verhinderung von Korruption im Unternehmen existiert. Und dies kann gegebenenfalls im Rahmen eines Korruptionsvorfalls als Indikator dienen, der die proaktive und ernsthafte Umsetzung eines Antikorruptionsmanagementsystems durch das Unternehmen untermauert.

Risikobasierter und systematischer Ansatz

Der in der ISO 37001 geforderte risikobasierte und systematische Ansatz stellt sicher, dass den Korruptionsrisiken entsprechende, zielgerichtete Maßnahmen getroffen werden. Ressourcen können so entsprechend effizient eingesetzt werden. Zudem wird sichergestellt, dass sich alle Abteilungen und Personen mit einem mehr als geringen Korruptionsrisiko mit der Thematik auseinandersetzen müssen. Die Unterstreichung des systematischen Ansatzes hilft, die Einzelaktivitäten aus Compliance, operativen Einheiten, Revision, Rechtsabteilung etc. so zu bündeln, dass ein einheitliches, abgestimmtes und nachhaltiges Managementsystem existiert.

Fazit

Für die Einführung eines Antikorruptionsmanagementsystems sind personelle und finanzielle Ressourcen

notwendig. Jedoch können sich die Einführung eines Compliancemanagementsystems nach ISO 37001 und gegebenenfalls dessen externe Zertifizierung durchaus lohnen. Die Vorteile der Vergleichbarkeit der Antikorruptionsmanagementsysteme und des Nachweises extern bestätigter Antikorruptionsmaßnahmen gegenüber Regulatoren sind nicht von der Hand zu weisen. Zudem kann auch von einer positiven Außenwirkung einer Zertifizierung ausgegangen werden, die Wettbewerbsvorteile mit sich bringen kann. Zusammengefasst hilft die ISO 37001 jeder Complianceorganisation, die bereits bestehenden und notwendigen Anforderungen an Antikorruptionscompliance zu reflektieren und systematisch zu verbessern. ◀



Johannes Breit,

Manager, ISO 37001 Lead Auditor,
EY Forensic & Integrity Services,
München

Johannes.breit@de.ey.com



Maxim Huttenlocher,

Senior Consultant, ISO 37001 Lead Auditor,
EY Forensic & Integrity Services,
Hamburg

Max.huttenlocher@de.ey.com



Andreas Pyrcek,

Andreas Pyrcek, CCEP-I, Partner,
EY Forensic & Integrity Services,
Düsseldorf

Andreas.pyrcek@de.ey.com
www.ey.com