Compliance Prophylaxe im Vertrieb

Joachim Kregel, Diplom-Ökonom, CIA, Köln

Der Autor vertritt die These, dass Fraud-Prophylaxe im Kernprozess Vertrieb des Unternehmen möglich ist, wenn systematisch nach dem System der Red Flags vorgegangen wird und gibt zahlreiche Beispiele, an welchen Stellen ein Interner Revisor oder Compliance-Beauftragter ansetzen kann.

1. Zielformulierung

Der Vertrieb ist in vielen Unternehmen eine der Kernfunktionen. Kernfunktionen haben im Wesentlichen mit externen Märkten zu tun, deren Vertreter die jeweiligen Interessen ihres Unternehmens nach außen wahrnehmen. Sie sind daher dem Verkäufer Unternehmensfremde. Trotzdem entwickeln sich in der Regel vertrauensvolle, partnerschaftliche Verbindungen zu den jeweiligen Marktpartnern. Dies ist insoweit in Ordnung als die unterschiedlichen Interessen des jeweiligen Unternehmens gewahrt werden und der Aufbau vertrauensvoller Beziehungen im Wertekanon des Unternehmens festgelegt wurde.
Beim Vertriebsmann des Lieferanten ist das Interesse an einem Auftrag ausschlaggebend, der eine auskömmliche Marge für sein Unternehmen sichert, zeitlich in das Produktions- und Termingerüst seines Unternehmen passt und durch Lieferung zuverlässiger Qualität den nächsten zukünftigen Auftrag absichert.
Probleme entstehen in dieser Beziehung immer dann, wenn diese Interessen durch Marktungleichgewichte (z.B. Oligopole/ Kartelle oder Monopole) belastet werden, die Interessenlage nicht transparent für die Marktteilnehmer gestaltet wird (Hidden Agenda von einer oder von beiden Seiten), und insgesamt die Vertragsgespräche nicht auf Augenhöhe geführt werden.
Hinzu tritt das von vielen beschworene Principal-Agent-Problem. Das heißt, dass zu den Unternehmensinteressen auch noch das persönliche Interesse der jeweiligen Marktpartner treten kann. Dem Unternehmensgeschäftsführer ist es einerlei, wie er sein Geld erhält. Beim abhängig beschäftigten Vertriebsmanager sieht es anders aus, eine Provision für einen erhaltenen Auftrag von seinem Unternehmen oder eine direkte Zuwendung vom Marktpartner zu erhalten. Denn die Beträge können sehr unterschiedlich in der Höhe sein, im Zweifel werden sie vom Marktpartner um ein Vielfaches höher liegen als die variable Vergütung durch die Akquisition eines Auftrags durch das Unternehmen.

Dieser Artikel will den Leser in die Lage versetzen, im Vorhinein Schwachstellen in den Kontrollsystemen des angesprochenen Unternehmensbereichs Vertrieb zu erkennen und damit beseitigen zu können. Weiter erhält der Leser Ideen, wie trotz ausreichend gestalteter Systeme durch nachgelagerte Kontrollen Compliance-Verstöße aufgedeckt und Vermögens- und Vertrauensschaden reduziert werden können (*Red Flags*).

Das DIIR hat in 2012 einen neuen Standard zum Anti-Fraud-Management herausgegeben, der dem Leser zur grundsätzlichen Einstimmung auf das Thema empfohlen wird[1]. Primär gilt jedoch das Prinzip des ehrbaren Kaufmanns, viel Gutes für sein Unternehmen zu tun, aber nicht auf Kosten anderer[2].

2. Risikoanalyse und Red Flags

[1] DIIR Revisionsstandard Nr. 5 ,24.5.2012.
[2] Siehe www.veek-hamburg.de

Nach den Terror-Anschlägen in Oslo ist uns die potentielle Gefahr vor Terroranschlägen wieder einmal bewusst geworden. Dieses Gespür für potentielle Gefahren hat in zwei Chemieunternehmen, die eine größere Chemikalienbestellung (Cool Packs und Säure) von einem neuen Kunden erhielten, ein Verdachtsmomentum/ Frühwarnsystem (Red Flags) heraufbeschworen. Sie haben daraufhin die Berliner Polizei eingeschaltet. Zwei Verdächtige wurden am 8.9.2011 verhaftet und sitzen nun in Untersuchungshaft[3].

2.1. Definition von Red Flag

In Unternehmen geht es seltener um externe Gefahrenabwehr zum Schutz von Menschenleben, obschon auch hier Schutzmechanismen verabredet sein sollten und greifen sollten. Vielmehr interessiert, wie Frühwarnsysteme in einem Unternehmen ausgestaltet sein sollten, die prophylaktisch Schutz vor Vermögensverlusten geben bzw. welche Indikatoren erste Warnhinweise geben könnten.
Wie bei vielen kriminellen Taten geht es bei den hier relevanten Tatbeständen von Diebstahl, Betrug und Untreue bzw. Kollusion um die drei Elemente einer Tat,

Gelegenheit – Motiv - Rechtfertigung (Rationalisierung).

Verdachtsmomente (Red Flags) ergeben sich bei allen drei Elementen, wenngleich die Systematik für jedes Element unterschiedlich ist.
Durch die konkrete Umsetzung verschiedener Grundprinzipien wie 4-Augen-Prinzip, Funktionstrennung Kompetenzenliste, Zugangs- und Zutrittssicherheit können Unternehmenswerte geschützt bzw. unbefugte Nutzung verhindert werden. Die Anzahl möglicher Gelegenheiten wird so eingeschränkt.
Aufgrund der Organisationsmacht eines Unternehmens bestehen bei der Gestaltung dieses Elements, der Verhinderung der Gelegenheit, die größten Freiheitsgrade.
Anders sieht das beim Motiv und dem Rechtfertigungsdenken eines potentiellen Täters aus. Hier ist es sehr schwer, direkt Erkenntnisse zu erhalten. Der Gesetzgeber zieht hier den Rahmen für Informationsbeschaffung sehr eng (Datenschutzgesetz, Grundrechte der informationellen Selbstbestimmung, Persönlichkeitsrechte am Arbeitsplatz, Verbot der Rasterfahndung etc.). Der Sozialpartner ist hier bei Ermittlungen im Anti-Fraud-Bereich, meist vorab, in Kenntnis zu setzen, wenn es um Mitarbeiter geht, die er vertritt.
Trotzdem gibt es in den Elementen Tatmotiv und Rationalisierung gewisse Handlungsoptionen, die für ein Unternehmen nutzbar sind. Jedoch erzielt man Erkenntnisse bei diesen Elementen meist nur auf indirektem Wege[4].

2.2. Risikosituation Einstellungsprozess

Bei einem potentiellen Innentäter[5] kann man differenzieren in Personen, die in das Unternehmen wechseln wollen und Personen, die in dem Unternehmen schon länger arbeiten.
Bei Neueinstellungen von Mitarbeitern gleich welcher Hierarchiestufe ist zu beachten, dass mit der Person zusätzlich zu den neuen Kenntnissen und Fähigkeiten auch potentielle Risiken mit eingestellt werden können. Um dies zu vermeiden, ist der zweistufige Einstellungsprozess mit Abgleich Jobprofil zu Eignung und Kultur des Unternehmens zu

[3] Berliner Morgenpost vom 8.9.2011
[4] Sog. „Profiling“ (Hintergrundrecherchen) von Personen kann über professionell arbeitende Informationsdienste erzielt werden. Bietet sich eher bei Geschäftspartnerschaften im Ausland an als bei Einstellungen bzw. Verdachtsmomenten gegenüber eigenen Mitarbeitern, ist jedoch sehr teuer. Die gesetzlichen Beschränkungen sind jedoch auch hier einzuhalten. Dies gilt insbesondere für international tätige Unternehmen.
[5] Im Zweifel gilt auch in einem Unternehmen das Legalprinzip der Unschuldsvermutung. Das bedeutet, Red Flags geben Hinweise, sind aber nie allein aussagekräftig für die Begründung eines Anfangsverdachts.

Persönlichkeit des Einzustellenden um den Aspekt „Trackrecord[6]“ zu erweitern. Hierbei ist zu beachten, dass Einschätzungen zum Trackrecord einer Person eine unterschiedliche Glaubwürdigkeit besitzen.
Die unterste Stufe der Evidenz sind mündlich erteilte Selbstauskünfte. Sie können nur geglaubt oder nicht geglaubt werden. Die Glaubwürdigkeit der berichtenden Person ist hier ausschlaggebend. Die Krux an den mündlichen Selbstauskünften ist, dass sie beim einem geschickten Bewerber genau auf die Erwartungshaltung des einstellenden Vorgesetzten abgestimmt werden kann. Die „Papierform“ tritt dann gegenüber dem positiven Erscheinungsbild zurück.
Selbst erstellte Unterlagen (Lebenslauf, Anschreiben, Exposé) haben eine größere Beweiskraft, da sie, einmal formuliert, nicht ohne weiteres wieder verändert werden können. Sie binden die Person, die sie erstellt hat, an das einmal Dargestellte. „Rückzieher“ im Bewerbungsgespräch vermindern dann die Glaubwürdigkeit.
Referenzen von Dritten vermitteln wieder ein objektiveres Bild, da die Beurteilung von außen erfolgt. Die Glaubwürdigkeit der erhaltenen Informationen korreliert sehr eng mit der Glaubwürdigkeit der als Referenz benannten Person. Obwohl diese Person die zu beurteilende meist aus längerer Zusammenarbeit her kennt, also gemeinsame Interesse an einer positiven Beurteilung nicht weg zu diskutieren ist, ist die Glaubwürdigkeit dennoch höher als eine Selbsteinschätzung zu konstatieren. Immerhin hat die als Referenz benannte Person einen Ruf zu verlieren und kann zudem auf Aspekte hinweisen, die die einzustellende Person von sich heraus nicht ansprechen würde Hier ist der blinde Fleck gemeint, also von Persönlichkeitseigenschaften, die man selbst eher verdrängt, die aber nahestehende Dritte sofort erkennen[7].
Zeugnisse von Schulen, Universitäten und anderen Körperschaften beinhalten die höchste Stufe der Glaubwürdigkeit, da die Ersteller der Zeugnisse im Verhältnis zur beurteilten Person nahezu objektiv handeln, also kein Eigeninteresse an einem günstigen oder ungünstigen Urteil besitzen. Eine gewisse Einschränkung gilt Arbeitszeugnissen. Diese sollen gleichzeitig wahrheitsgemäß und wohlwollend abgefasst sein und dürfen keine versteckten Hinweise enthalten. Diese gesetzliche Notwendigkeit entwertet ihre Aussagekraft bisweilen etwas. Eine weitere Entwertung tritt gerade bei Führungskräften dann auf, wenn sie ihre Zeugnisse selbst geschrieben haben, und nur die Unterschrift vom früheren Vorgesetzten tragen.
Die nachfolgende Tabelle fasst diese Evidenzhierarchie zusammen:

Evidenz	**Merkmal**	**Beispiel**
niedrig	Mündlich, selbst	Antworten im Bewerbungsgespräch
höher	Schriftlich, selbst	Bewerbungsschreiben, Lebenslauf
hoch	Mündlich, von Dritten	Referenzen
Sehr hoch	Schriftlich, von Dritten	Zeugnisse: z.B. Schul- und Universitätszeugnisse; polizeiliches Führungszeugnis; bedingt Arbeitszeugnisse

Abbildung 1: Evidenzhierarchie

Menschen, die in anderen Unternehmen oder im Privatleben einmal auffällig geworden sind, können in einem systematisierten Einstellungsprozess, der die Red Flags zusätzlich zum Jobprofil enthält, erkannt werden.
Stichworte sind hier lückenloser Lebenslauf, polizeiliches Führungszeugnis, Arbeitszeugnisse und Referenzen sowie Einstellung zu Ethikthemen in einem

[6] Mit Trackrecord ist ein Gesamtbild einer Person gemeint, ihren Leistungen, ihrem Verhalten gegenüber Vorgesetzten, Mitarbeitern, Kollegen und Dritten in früheren Positionen. Der Begriff geht damit weiter als die bekannteren Begriffe Personalakte und Lebenslauf.
[7] Hier ist der blinde Fleck gemeint, also von Persönlichkeitseigenschaften, die man selbst eher verdrängt, die aber nahestehende Dritte sofort erkennen.

Bewerbungsgespräch. Auch teure persönliche Vorlieben und Gehaltsvorstellungen, die weniger am bisherigen Lebenslauf als am neuen Job orientiert sind, können Hinweise liefern. Um auch an dieser Stelle eines deutlich zu machen, eine 100% Sicherheit gibt es nicht, auch kann jeder einzelne Verdachtspunkt, für sich genommen, nicht zu der Schlussfolgerung führen, „Nicht Einstellen". Das Gesamtbild ist hier entscheidend, jedoch sollte nach der Überzeugung des Autors gerade bei Positionen im Middle- und Top-Management mehr Wert auf die „Papierform" als allein auf den persönlichen Eindruck gelegt werden[8].

2.3. Risikosituation Internes Unternehmensumfeld

Noch schwieriger wird eine Einschätzung von Führungspersonen, die schon lange im Unternehmen arbeiten. Hier gilt zuerst der Grundsatz des Vertrauensvorschusses.
Trotzdem sollte bei der hohen Anzahl von Innentätern und den meist sehr hohen Schadenspotenzialen[9] auch hier den Red Flags eine größere Aufmerksamkeit gewidmet werden.
Hinweise auf Risikosituationen sind

- häufige Kündigungen von Mitarbeitern in bestimmten Abteilungen,
- nur mit Mühe, wenn überhaupt, erreichte Ziele,
- „Opfer" von Umorganisationen mit Verlust an Einfluss,
- Gerüchte über Führungsstile oder unangemessenen Lebenswandel, Verzicht auf längeren Urlaub am Stück und ungewöhnliche Häufung von Überstunden.

Jeder einzelne Hinweis mag eine plausible Erklärung finden, das Gesamtbild ist wiederum entscheidend. Im besten Fall entstehen dem Vorgesetzten Zweifel, die er mit dem Personalverantwortlichen und/ oder dem Leiter der Compliance (CO) und/ oder der Internen Revision (IR) vertrauensvoll bespricht.
Die nachstehende Tabelle gibt hier einige Hinweise. Jedoch sollte beachtet werden, dass es auch Fehlinterpretationen von Verdachtsmomenten geben kann. Diesem Trugschluss kann man durch professionelle Analyse und langjährige Beobachtung der Verdachtsmomente entgehen. Denn nicht ist schlimmer als ein Beta-Fehler[10], d.h. ein Fehlverhalten zu erkennen, das gar nicht vorhanden ist.
Es gilt auch hier wie im öffentlichen Leben die Unschuldsvermutung, ohne Beweis kann nicht gehandelt werden, ohne Anfangsverdacht sollte nicht intern ermittelt werden. Es widerspricht jeglicher ethischer Norm, einen Fall zu konstruieren nur um jemanden „billig loszuwerden".

Verdachtsmoment/ Red Flag	**Möglicher Hinweis auf**	**Gegenindikation**	**Quelle**
Jahrelang häufige Kündigungen von Mitarbeitern	Unethisches Verhalten des Vorgesetzten	Umorganisation	Personalabteilung, ehemalige Mitarbeiter
Mehrjährige Verfehlung von Bereichszielen	Überteuerter Einkauf, Unwirtschaftlicher Ressourceneinsatz	Wettbewerbssituation, Unrealistische Ziele	Vorgesetzter, Controlling,
„Paradies-Vogel"-Image	Management	Äußerst erfolgreicher	Gerüchteküche des

[8] Personalberater sind auf diesen Umstand frühzeitig hinzuweisen. Ihr Ansatz der Kandidatenbeurteilung ist zumeist auf das Überzeugungsvermögen und die Abdeckung des geforderten Jobprofils ausgerichtet. Zeugnisse werden m.W. bei der Besetzung von Führungspositionen selten angefordert.
[9] Siehe hierzu die neueste Studie „Wirtschaftskriminalität in Deutschland 2010, Fokus Mittelstand, von KPMG sowie den Global Fraud Report von Ernst&Young, 2008.
[10] Prüftechnisch wird unterschieden in @- und ß-Fehler. Alpha-Fehler sind tatsächliche Fehler, die vom Prüfer jedoch mangels Erfahrung, Wissen, Methodik etc. nicht erkannt werden, ß-Fehler sind angemerkte Fehler bei Sachverhalten, die tatsächlich objektiv gesehen in Ordnung sind.

	Override[11]	Manager	Unternehmen, Controlling, anonyme Hinweise
Häufige Erbschaften als Hinweis für aufwendigen Lebenswandel	Korruption, Kollusion, Betrug, Diebstahl	./.	Gerüchteküche des Unternehmen, Mitarbeiter
Jahrelang Kurzurlaube statt längerer Urlaube, jahrelang auffällig viele Überstunden	Datenmanipulation, die kein Dritter entdecken soll	Zeitweise hohe Arbeitsbelastung wegen schwieriger Bereichs- und Unternehmenssituation	Personal-abteilung, Vorgesetzter
Mehrtägige Dienstreisen ohne Übernachtungs- oder Bewirtungsbelege		Schulung/ Weiterbildung auf eigene Kosten	Buchhaltung
Lieferant wird mehrfach gegen die Interessen des eigenen Unternehmens trotz Schlechtleistung verteidigt	Kollusion	Einzelfall, bei dem die Lieferantensituation objektiv erklärbar ist	Vorgesetzte, anonyme Hinweise

Abbildung 2: Red Flags im Managementbereich generell

Trotz aller dieser Red Flags sind es im praktischen Leben denn doch oft Zufälle, anonyme Hinweise, die einen Fall entdecken helfen, der sonst nicht aufklärbar gewesen wäre.
Umgekehrt wird auch ein Schuh draus. Wenn Vorstände aus falsch verstandenem Vertrauen zu ihren Mitarbeitern anonyme Hinweise direkt in den Papierkorb wandern lassen, handeln sie zumindest fahrlässig und unprofessionell. Mit der Einrichtung eines externen Ombudsmann für Whistleblowing[12] lassen sich solche Hinweise kanalisieren und von unabhängiger Stelle analysieren, so dass Schaden abgewandt oder verringert werden kann.
Weiter kann durch eine Compliance-Abteilung und/ oder Interne Revision bei Anfangsverdachtsmomenten vorab geprüft werden, ob hinreichend konkrete Hinweise für eine Ermittlung bestehen.
Im Zweifel können auch bei begründetem Anfangsverdacht die Strafverfolgungsbehörden eingeschaltet werden, die Möglichkeiten besitzen, Beweissicherung zu betreiben, die den Schaden reduzieren können bzw. Vermögen des Unternehmens wieder zurückzuholen.

Wichtiger Hinweis *Auf jeden Fall verbietet es sich, sofort ohne Vorrecherche einen Beschuldigten mit dem Vorwurf zu konfrontieren. Die irrtümliche Vermutung, dass der Betreffende gesteht, führt meist zu Ausflüchten, Bestreiten oder Leugnen der Tat. Erst nachdem die Beweislast erdrückend geworden ist, ist ein Geständnis wahrscheinlicher[13]. Es wird jedoch nur das zugegeben, was sowieso unstreitbar beweisbar ist.*

Die Frage nach dem „Warum“ oft verdienstvoller und engagierter Mitarbeiter wird, wie oben schon erwähnt, mit Rechtfertigungen beantwortet. Diese Rechtfertigungen beruhen auf dem psychologischen Moment der Rationalisierung, d.h. der Täter baut sich intern ein Rechtfertigungskonstrukt auf, vor der die Tat als Normalfall und eben nicht als unerlaubter Sonderfall dasteht.

---

[11] Mitarbeiter in einer herausgehobenen Führungsposition hält sich nicht an interne Vorschriften.
[12] Begriff aus der amerikanischen SOX-Umgebung. Beschreibt einen (meist) internen Tippgeber, der nach amerikanischen Verständnis mit allen Mitteln zu schützen ist.
[13] Arbeitsrechtlich ist die 14 Tage-Frist (§626 Abs.2 Satz 1BGB) zu beachten, innerhalb derer ein Mitarbeiter mit den Vorwürfen konfrontiert werden muss. Wann die Frist anfängt zu laufen, ist mit dem Chefjustitiar abzustimmen. Auf jeden Fall sind die Recherchen äußerst vertraulich zu führen.

Gegen diese Rationalisierungen von potentiellen Innentätern kann ein Unternehmen nur sehr indirekt vorgehen.
Zentraler Dreh- und Angelpunkt ist der Vorgesetzte, oder abstrakt für das Unternehmen formuliert die Führungskonzeption eines Unternehmens.
Diese sollte aus einem Wertesystem abgeleitet werden und zusätzlich zu Leistungsaussagen auch Compliance-Aussagen enthalten. Hiermit kann erreicht werden, dass ein Gesamtverständnis im Unternehmen, was o.k. ist oder was nicht, ausgeprägt wird.
Dieses *Wertesystem* sollte dann in einem mitarbeiterorientierten Dialog konkretisiert werden. In diesem Dialog wird die Vertrauensbasis zwischen Mitarbeiter und Vorgesetztem gelegt und mit Zielgespräch, Beurteilungs- Gehalts und Potentialgespräch aufgebaut. In dieser Gesprächskaskade können über Motiv- und Einstellungslage von Mitarbeitern viel erfahren werden, wenn Mitarbeiter ungeschminkt und offen Feedback geben. Wichtiger als die schriftliche Protokollierung dieser Gespräche ist die Information, die mündlich gegeben wird und dem Vorgesetzten Hilfen für seine Führungsarbeit in der Zukunft geben kann.
Jeder Vertrauensbruch hat jedoch zur Konsequenz, dass diese Gespräche nur noch formalen Charakter haben und nichts mehr für die Führungsfähigkeit eines Unternehmen und seiner Vorgesetzten leisten.
Ein weiteres Instrument zur Ausbildung einer Vertrauenskultur im Unternehmen kann eine *Mitarbeiterbefragung*[14] sein. Essentiell ist jedoch auch hier, dass die Vorgesetzten diese Befragung als Instrument zur Verbesserung der Führungsfähigkeit eines Unternehmens verstehen und auf Basis der Antworten einen Dialog mit ihren Mitarbeitern führen.
Merken die Mitarbeiter, dass ihre Antworten nicht zählen, wird die Mitarbeiterbefragung nur noch zu Kosten und nicht zu Erkenntnissen führen.
Die nachfolgende Tabelle gibt einen kleinen Überblick über mögliche Rationalisierungen[15] von Tätern und indirekter Abhilfe durch flankierende, prophylaktische Maßnahmen des Unternehmens:

Tatbestand und Aussage	**Mögliche Ursache**	**Prophylaxe**
Diebstahl: Ich benötigte das Geld mehr als jeder andere im Unternehmen	Spielsucht, momentane finanzielle Engpässe	Mitarbeiterorientierter Dialog: Vertrauensverhältnis zu Vorgesetzten etablieren
Diebstahl: Ich habe es mir nur geliehen und hätte es später wieder zurückgegeben.		Internes Kontrollsystem verbessern
Korruption: Jeder tut das hier.	Illoyalität, Unterentwickelte Unternehmenskultur	Compliance-Fragebogen für alle Mitarbeiter
Korruption: Ich verdiene es.	Illoyalität, Bezahlungssystem nicht transparent oder zu wenig leistungsorientiert	Mitarbeiterorientierter Dialog: Vertrauensverhältnis zu Vorgesetzten etablieren
Korruption: Ich hole mir nur das, was mir zusteht.		
Korruption: Wir sind doch eh versichert.	Illoyalität, Unterentwickelte Unternehmenskultur	Compliance-Fragebogen für alle Mitarbeiter
Bilanzfälschung: Ich wollte dem Unternehmen doch nur helfen.	Falsch verstandene Loyalität	Wertesystem im Unternehmen etablieren und diskutieren

[14] Infratest in München hat mit dem Produkt TRI:M sowohl für Mitarbeiter- und Kundenbefragungen ein Instrument entwickelt, das diese Ziele unterstützt.
[15] Siehe Sykes& Matza: Techniques of neutralization

Abbildung 3: Rechtfertigungen /Rationalisierungen

Zusammenfassend lässt sich festhalten, dass unternehmerische Maßnahmen wie

- einem mitarbeiterorientierten Dialog,
- einer Wertediskussion,
- Mitarbeiterbefragungen und Maßnahmen, die das Verhältnis zwischen Mitarbeiter und Vorgesetzten vertrauensvoll gestalten helfen sowie
- durch ein etabliertes Frühwarnsystem

einiges an Compliance-Verstößen verhindern lässt.

Hingegen sind die angesprochenen Maßnahmen eher wie ein „Breitbandtonikum“ zu verstehen, die den Rahmen für ethisches Verhalten im Unternehmen unterstützen helfen. Die nachstehende Abbildung fasst die oben diskutierten Elemente noch einmal zusammen:

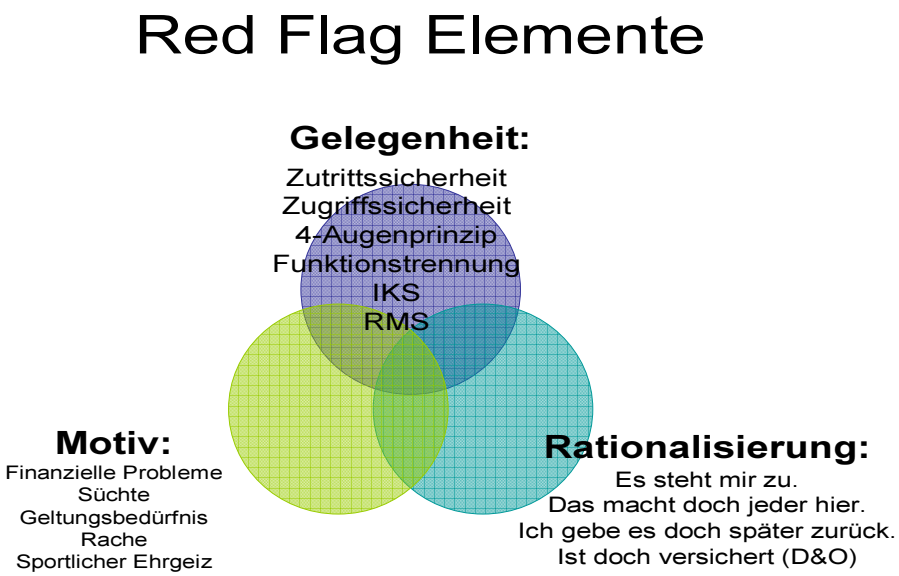

Abbildung 4: Red Flags[16]

3. Marktkante Marketing/Vertrieb

Der Autor verwendet im Folgenden die klassischen 4 P des Marketings Produkt, Preis, Promotion und Placement, obwohl der Promotor der 4 P Philip Kotler[17] sein Modell auf neue Füße gestellt hat[18]. Compliance-Themen können in allen Bereichen relevant werden.

3.1. Produktentwicklung

[16] Siehe auch die Prüfungsstandards PS 210 und ISA 240 des Instituts der Wirtschaftsprüfer (IdW), die das Thema Red Flags ebenso im Rahmen der Abschlussprüfung adressiert haben.

[17] Tatsächlich hat 1960 Jerome Mc. Carthy die 4 P des Marketings in die wissenschaftliche Diskussion eingebracht. Philip Kotler hat in seinem Grundlagenbuch Marketing Management diesen Begriff promotet und weiterentwickelt.

[18] Philip Kotler u.a.: Die neue Dimension des Marketings: Vom Kunden zum Menschen.

Beim Thema Produktentwicklung, wird der geneigte Leser einwenden, können doch Compliance-Themen gar nicht so häufig entstehen, da dieser Bereich streng im Verborgenen eines Unternehmen ohne große Mitbeteiligung Dritter am Markt arbeitet. Außerdem arbeiten in diesem Bereich in der Hauptsache Naturwissenschaftler, deren Primärinteresse die Innovation sei. Das Geldinteresse sei beschränkt auf ein auskömmliches Budget, mit dem Forschungseinrichtungen und hochqualifizierte Mitarbeiter alimentiert werden können. Dieser Einwand ist einerseits berechtigt, andrerseits greift er zu kurz.
Auch Naturwissenschaftler sind Menschen mit allen Motivstrukturen und Rationalisierungsmustern, die bei Compliance-Analysen angewandt werden können. Darüber hinaus haben sie ein ausgesprochenes Mitteilungsbedürfnis, Innovationen der akademischen Fachwelt kund zu tun und von den Forschungsergebnissen ihrer Kollegen wieder zu profitieren („Give and Take"). Dieses Bedürfnis steht einem Geheimhaltungsinteresse des Unternehmens diametral entgegen. Deshalb sollte die Diskussion dieser Problematik vor Einstellungen (ehemals) wissenschaftlich Tätiger einen Teil des Einstellungsgesprächs einnehmen.
Technologiegetriebene Unternehmen aus dem Maschinenbau, der Automobil- und Flugzeugindustrie, Pharma und Chemie, ITK (Informations-Technologie und Telekommunikation) benötigen hochqualifizierten Nachwuchs, können ihn jedoch auch leicht wieder an die Forschung oder den Wettbewerber verlieren.
Nichts definiert die USP (Unique Selling Proposition), also die Unverwechselbarkeit eines Unternehmen so sehr wie das Produkt, seine Entwicklung ist also besonders schützenswert.
In der ITK-Branche überziehen sich die Wettbewerber zurzeit gegenseitig mit einer Vielzahl von Prozessen, deren Streitwerte in die Mrd.-$ hineingewachsen sind[19]. Die USP wird mit Patenten, Gebrauchs- und Geschmacksmusterschutz sowie mit dem Markenschutz versucht zu verteidigen[20]. Idealerweise werden Eigenentwicklungen zum Marktstandard weitergetrieben, die dann für alle verbindlich sind. Der Beginn eines Monopols ist vorgezeichnet. Auf dem Weg dahin wird weiterhin versucht, Abkürzungen zu nehmen und Regulierungsauflagen zu umgehen[21].
Ähnliche Themen sind in der Automobilindustrie zu finden im Kampf um die Marktanteile der Zukunft zwischen Deutschland und Asien, vor allem in China.
In der Pharmaindustrie geht der Kampf um den weltweiten Patentschutz eigener Produkte bis zum Schutz der Produkte gegen Nachahmer-Generika. Milliarden-Umsätzen eines Blockbusters stehen Milliarden-Entwicklungskosten vieler Produktideen gegenüber, die die klinische Erprobungsphase nicht mehr überstanden haben.
Vor diesem Hintergrund verwundert es nicht, dass Schutz gegen Industriespionage, Produktpiraterie und Patentrechtsverletzungen ein brennendes Thema geworden ist, das einige Unternehmen sogar veranlasst hat, bestimmte Märkte als Produktionsstandorte trotz erheblicher Kostenvorteile auszugrenzen, um die Existenz des eigenen Unternehmens abzusichern.
Prophylaxe-Maßnahmen im Unternehmen beginnen wieder beim Mitarbeiter, dem die unterschiedlichen Möglichkeiten der Ausspähung vertraut gemacht werden sollten. Dies beginnt in der Schulung, was Firmengeheimnisse sind und wie mit ihnen auch innerhalb des eigenen Unternehmens umgegangen werden sollte.
Z. B. sollte außerhalb des Unternehmens weder über Namen von Unternehmensangehörigen noch über Unternehmenszahlen gesprochen werden. Im Zeitalter von E-Mail und Handy ist dies ein schwieriges Unterfangen. Nichts desto trotz sind Verschlüsselungen vertraulicher E-Mails, abstrakte Formulierungen am Handy in der Öffentlichkeit bis hin zur Nutzung von SMART-Cards zum PC-Schutz Möglichkeiten, die noch viel stärker genutzt werden sollten.

---

[19] Als prominentes Beispiel sei hier die Klage von Apple gegen Samsung wegen Design- Kopien seines I-Phones und des I-Pads erwähnt. Pikanterweise produziert Samsung den von Apple entwickelten Chipsatz Apple A4 und A5 und setzt ihn in eigenen Produkten ein.
[20] Zu den Unterschieden siehe Deutsches Patentamt: www.dpma.de
[21] Siehe die vielen Verfahren, in denen Microsoft Wettbewerbern und Kartellbehörden Schadenersatz leisten musste.

Über die Möglichkeiten, die Thematik Geheimhaltung schon im Vertragsgespräch zu erörtern, wurde schon erwähnt.
Regelmäßige Schulungen zur Bewusstmachung der Risiken gehören auch dazu.
Entsprechende Geheimhaltungs- und Wettbewerbs-Klauseln in allen Unternehmensverträgen mit der Maßgabe an alle verantwortlichen Manager, diese und keine anderen zu verwenden, kommen hinzu.
Eine aufmerksame und mit aktuellen Kenntnissen und Befugnissen ausgestattete IT-Sicherheits-„Truppe“ kann viel Schlimmes von Außenangriffen verhindern. Außerdem sollte sich auch die Unternehmensspitze darüber klar sein, in welcher Software sog. „Backdoors[22] eingebaut“ sein könnten und wie man sich im Ausland mit seinem Laptop und Handy zu verhalten hat. Dies gilt ganz besonders bei Akquisitionsgesprächen, bei denen der Besprechungsort nicht sorgfältig genug gewählt werden kann.
Ist der Worst Case eingetreten, hilft eine eigene Sicherheits- oder Compliance- oder Revisionsabteilung, viele Fehler von vorneherein zu vermeiden. Dies beginnt mit einer sehr engen Definition des Kreises, der informiert sein sollte, der Entscheidung über pro und contra der Einbeziehung von externen Beratern, Detekteien und Anwälten bis hin zur Entscheidung zu einer Strafanzeige und arbeitsrechtlichen Konsequenzen verbunden mit einem sorgfältig ausgearbeiteten Konzept der Außenkommunikation.

Die nachstehende Tabelle gibt noch einmal einen Überblick:

Risiko-Thema	**Red Flags**	**Prophylaxe**
Industrie spionage	Zeitliche Koinzidenzen einer Neuprodukt-Markteinführung; Verblüffende Ähnlichkeit nicht sichtbarer neuer Features und Funktionalitäten;	Regelung in Lieferantenverträgen; Wettbewerbsklauseln in Mitarbeiterverträgen; Laufende Gesprächsschulung von Mitarbeitern in sensiblen Bereichen; (IT)-Zugangs- und (IT)-Zugriffsschutz; Externe Beratung bei Verdachtsfällen
Produkt piraterie	Ungeplante, z.T. schleichende Umsatz- und Ergebnisverluste; Verlust von Stammkunden	Absicherung in allen Verträgen der Lieferantenkette; Öffentlichkeitsarbeit Anzeigen bei Zoll und Staatsanwaltschaft Lobbying
Patentrechts verletzungen	Ungeplant langsame,teilweise erfolglose Marktbearbeitung; Ähnlichkeit nicht sichtbarer neuer Features und Funktionalitäten;	Schadenersatzklagen; Gerichtsfeste, belastbare (inter)-nationale Patente

Abbildung 5: Risikomaßnahmen für einen Produktschutz

Es versteht sich von selbst und wird auch hier deshalb nur beiläufig erwähnt, dass umgekehrt der CO-Verantwortliche darauf zu achten hat, dass die oben genannten Tatbestände in seinem Unternehmen nicht vorkommen.

[22] Sog. Backdoors könnten ausländischen Geheimdiensten Ausforschungsmöglichkeiten eröffnen. Diese sind bei eigenem nationalem Interesse nicht zur Geheimhaltung verpflichtet und könnten dann Erkenntnisse an nationale Unternehmungen weitergeben. Amerikanische (Microsoft, Cisco) und kanadische Unternehmen (RIM: Blackberry) bestreiten vehement, solche Optionen einprogrammiert zu haben. Nur Hardware-Schutz mit Smartcards bietet nach Auffassung des Autors hinreichenden Schutz vor Ausspähungen, da der sog. private key auf der Karte und nicht im PC oder im Netz (VPN: Virtual Private Network) vorhanden ist.

Zwar gehört ein gut gefüllter „War-Room[23]“ inzwischen zu jedem gut geführten Unternehmen, das sich im harten Wettbewerb befindet. Damit sind jedoch nur legale Maßnahmen im Kampf um Marktanteile beschrieben.

3.2. Preispolitik und Regulierung

Trotz aller USP über die Einzigartigkeit und Qualität ist der Preis des Produkts letztendlich ausschlaggebend für den Erfolg am Markt.

Über Markteintrittsbarrieren wie

- *exklusiven Kundenzugang*: Vertriebsbindung in der Automobil- und in der Mineralölindustrie, Kampf um den Regalmeter bei der Lebensmittelindustrie
- *eigene Entwicklung zum Marktstandard zu etablieren*: z.B. Microsoft-Windows-Betriebssystem, Apple-A4 und A5-Chipsatz, SAP-ERP/SCM/CRM-Software für Branchen
- *hohe Infrastrukturaufwendungen*: Telekommunikation, Energieversorger; Bahn; Mineralölindustrie

wird versucht, ein Monopol zu schaffen und damit den Wettbewerb über den Preis auszuschließen.
Dies führt bei adäquater Marktbeobachtung durch die Regulierungs- und Kartellbehörden zu Gegenreaktionen. Diese bestehen in der Festlegung von Preisobergrenzen, Vorabgenehmigungen für Preise oder nachträglicher Missbrauchsaufsicht über die Preispolitik bis hin als Ultima Ratio zur Zerschlagung von Unternehmen oder des Verbots von Unternehmenszusammenschlüssen.
Die betroffenen Unternehmen sind dann gezwungen, durch erhebliche Rationalisierungsanstrengungen den Druck sinkender Preise und, wegen teilweise unelastischer Nachfrage, sinkender Umsätze auszugleichen. Da der Wettbewerb sich entfalten soll, werden auch die Vorleistungspreise, z. B. für die Mitbenutzung der vorhandenen Infrastruktur, festgelegt (Teilnehmeranschlussleitung oder hochfrequente Bitübertragung ohne Telefonleistung bei der Deutschen Telekom). Die aktuellen Diskussionen um die Infrastruktur der Bahn und Netzentgelte der Energieerzeuger gehören ebenfalls zu diesem Thema.
Compliance-Themen entstehen in der Praxis immer dann, wenn die Märkte unvollkommen sind und vom Kunden bzw. Einkauf die Leistung nur unvollkommen bewertet werden kann.
Ein gewisses „G`schmäckle“ lässt sich nicht leugnen, wenn sich ein gegenüber dem Kunden unabhängig gebender IT-, Media- oder Bauberater vom Lieferanten der Leistung zusätzlich bezahlt wird.
Dieses „G`schmäckle“ gilt ebenfalls für Finanzberater und Bankberater, die für den Vertrieb von Produkten Provisionen der Fonds (Investmentfonds, Immobilienfonds, Schiffsfonds etc.) kassieren.
Die Nähe zur Kollusion (vorsätzliches Zusammenspiel von unabhängig auftretenden Personen mit dem Zweck der Schädigung eines Dritten) ist nicht wegzudiskutieren, wenn die Verbindungen zum Lieferanten von den Beratern nicht offengelegt werden und gleichzeitig der Kunde geschädigt wird, d.h. wenn das vermittelte Produkt nicht werthaltig oder weit überteuert angeboten und verkauft wird.
Im Normalfall ist die Preisstellung in einem Unternehmen durch Richtlinien klar geregelt. Darin enthalten sind dann auch die Kompetenzen, die benötigt werden, um Rabatte, Erlösschmälerungen oder Skonti zu gewähren.

[23] Begriff aus der Strategie und dem Marketing (ursprünglich der Lageraum einer kriegsführenden Partei), in dem alle Informationen zusammengetragen und präsentiert wurden) bezeichnet ein Konzept möglicher Aktion-Reaktion im Verhältnis zu einem Wettbewerber.

Je mehr die gewährten Rabatte vom zunächst genannten Fabrikabgabepreis abweichen, desto größer wird die Möglichkeit von unerlaubten „Zwischengeschäften".
Sichtbar werden diese Marktpreisdifferenzen dem Kunden nur bei einer Ausschreibung des Leistungsverzeichnisses (Bau), Pflichtenheft (IT-Software), Briefingdokument (Werbeaktion). Wenn jedoch der Lieferant dem Kunden bei der Erstellung dieser Verzeichnisse dem Kunden hilft oder sie gar komplett selbst erstellt, kann es dann trotz Ausschreibung einen Vorteil für den Lieferanten bedeuten, bei der Angebotserstellung beraten zu haben.
Für den IR oder CO-Verantwortlichen in einem Lieferantenunternehmen ist es wichtig, sich die Kosten der Absatzmittler, die ja die Umsatzmarge gedrückt haben, im Einzelnen erläutern zu lassen.
Bei der Erschließung neuer Märkte kann es sinnvoll sein, sich eines Experten zu bedienen, der den Kundenzugang erstmalig aufbaut. Nach einigen Jahren sollte das Unternehmen dazu dann allerdings selbst in der Lage sein.
Kritisch wird es zudem, wenn die Preisstellung ungewöhnlich hoch, aber auch die Vertriebskosten ebenfalls hoch ausfallen, so dass trotz auskömmlicher Brutto-Marge netto der Gewinn unterplanmäßig ausfällt.
Im Zweifel sollte der CO-Verantwortliche sich der Internen Revision oder einer „externen" Internen Revision der Abschlussprüfergesellschaften bedienen, um einen intransparenten Sachverhalt aufzuklären.
Risiken eines möglichen Kollusionsvorwurfs verbunden mit einem Reputationsschaden für das eigene Unternehmen sollte das verringern helfen.

Risikofeld	**Red Flag**	**Abhilfe**
Bau	Fehlende Ausschreibung, aber hohe Beratungshonorare	Kurzfristig: Externen Sachverstand einkaufen (Experten für Bau-, IT-, und Media/ Werbungs- Revision);
IT	Niedrige Rabatte trotz mehrerer Verhandlungsrunden ohne Auftragsverlust, aber hohe Beratungshonorare	Mittel- bis langfristig: Eigene Fach- und Sachkompetenz aufbauen
Werbung	Media-, Papier und Druckkosten-Rabatte, die direkt an eine Werbeagentur überwiesen werden sollen	
Bank, Sparkasse, Finanzvermittler Versicherung	Provision als Kickback	Kickbacks für Vermittlung im Unternehmen transparent gestalten oder Nettopreise mit Beratungshonorar

Abbildung 6: Risikofelder und Red Flags Preispolitik

3.3. Promotion/Kommunikation und Werbung

Einer der großen Sachkostenblöcke im Unternehmen, der von den Verantwortlichen im Unternehmen zumeist mit Verve verteidigt wird, ist das Werbebudget. Obwohl es auch heute immer noch schwierig ist, seine direkte Wirkung auf den Umsatz zu belegen, wird es auch bei großen Ergebnisproblemen eines Unternehmens selten radikal gekürzt, weil jeder das Marktrisiko mangelnder Präsenz in den Werbemedien scheut.
Ähnlich wie bei IT, Bau und M&A (Mergers& Acquisitions) sind Werbemaßnahmen in sich immer einzigartig, ihre Machart folgt jedoch einem mehr oder weniger standardisierten Prozess. Abgeleitet aus der Unternehmensstrategie und der Umsatz- und Absatzplanung, entwickeln sich konkrete Werbemaßnahmen immer aus der Überlegung heraus,

Stammkunden wieder ans Unternehmen zu binden und *neue Kunden* für das Unternehmen und seine Leistungen zu begeistern. Ein zentrales Element bei der Auswahl der einzelnen Werbeträger/ Medien ist der 1000- Kontakt-Preis. Er sollte als Preis für die zu erwartende Aufmerksamkeit die Werbekosten bei den unterschiedlichen Werbeschaltungen wie TV/ Radio, Print und neuerdings auch Internet[24] normalisieren, d.h. vergleichbar machen.
Die sehr hohen Kostenblöcke in den Werbebudgets werden im Wesentlichen durch die Vorleistungslieferanten verursacht. Anders als beim traditionellen Einkauf überlassen Unternehmen den Einkauf dieser Leistungen Werbe- und Media-Agenturen. Das führt in der Praxis zu Intransparenz und der Gefahr überhöhter Kosten. Die Intransparenz entsteht durch die Rechnungen der Agentur, die meist ihre eigenen Leistungen mit denen ihrer Zulieferer in einer Rechnung zusammenfasst. Die Gefahr überhöhter Kosten entsteht durch die Konzentration der Werbeagentur auf die Kreativleistung und nicht so sehr auf den kostengünstigen Einkauf.
Positiv wäre es, wenn Agenturverträge eine Revisionsklausel enthielten, wie sie bei anderen Lieferanten von Outsourcing-Leistungen üblich ist, sodass eine CO/ IR- Abteilung unbefangen einer Agentur ihre Fragen stellen könnte, ohne befürchten zu müssen, dass die Agentur eine politische Einmischung oder gleich das Ende einer Geschäftsbeziehung herannahen sieht. Etwas mehr Sachlichkeit im Umgang könnte beide Seiten befruchten: die Agentur, die sich vom Kundenunternehmen besser verstanden fühlt, und die CO/ IR, die vor Werbeprüfungen nicht mehr zurückschreckt.
Sind nun die Mediaplanungsentscheidungen für das kommende Jahr strukturell im Einzeln festgelegt, geht es in die konkrete Umsetzung der einzelnen Werbeobjekte. Bei der konkreten *Werbeobjektplanung* geht es um die auftragsgerechte Umsetzung der Einzelmaßnahmen. Hierbei treffen ca. 10 – 20 % kreative auf 80 – 90 % handwerkliche Leistungen, für den letzten größeren Teil immer ein Einkaufsthema, das nicht der Werbeagentur allein überlassen werden sollte. Insbesondere spielt der *Mediaeinkauf,* der für 40 – 50 % der Gesamtkosten verantwortlich ist, eine entscheidende Rolle für die Beantwortung der Frage, ob die Effizienz gewahrt wurde. Professionelle Mediaagenturen, nicht Werbeagenturen, führen diese Effizienzüberlegung für wenige Prozentpunkte der Werbekosten durch.
Die nachfolgende Tabelle fasst die einzelnen Prozessschritte zusammen und empfiehlt einige Maßnahmen zur Vermeidung von Intransparenz und fehlender Budgetkontrolle, die ihrerseits CO-Verstöße provozieren könnten.

Prozessschritte: Werbeobjekt planung	**Risikofelder/ Red Flags**	**Abhilfe**
Briefing für Katalog/Beilage/ Mailing/Werbespot	Prozessschritt ist nicht dokumentiert; Bezug zum Jahres-Budget nicht erkennbar;	Dokumentieren und Budgetbezug herstellen
Entwurf: Lay-out/Drehbuch	Prozessschritt ist	Dokumentieren

[24] Google und auch z.T. Facebook bieten Unternehmen eine Vielzahl von Daten an, auf welchen Wegen potenzielle und auch aktuelle Kunden zu den oder der Unternehmens-Website (s) gelangt sind. Diese Daten unterscheiden sich in ihrer Detailliertheit signifikant von denen der klassischen Medien.

Foto-Shooting/ „Dreh“ (Produktion)	nicht dokumentiert;	
Litho + Satz/Schnitt + Nachvertonung	Fehlende Ausschreibung; Seit Jahren gleiche Lieferanten;	Vergabe selbst in die Hand nehmen; Erstellen des Leistungsverzeichnisses durch die Werbeagentur
Druck	Fehlende Ausschreibung; Seit Jahren gleiche Lieferanten; Keine internationale Ausschreibung	Vergabe selbst in die Hand nehmen Erstellen des Leistungsverzeichnisses durch die Werbeagentur
Porto TV und Radio-Schaltung	Fehlende Ausschreibung; Seit Jahren gleiche Lieferanten;	Vergabe selbst in die Hand nehmen; Erstellen des Leistungsverzeichnisses durch die Werbeagentur Vertrauenswürdige Mediaagentur einschalten oder selbst eine gründen
Debriefing/ Erfolgskontrolle	Prozessschritt ist nicht dokumentiert; Bezug zum Jahres-Budget nicht erkennbar;	Dokumentieren und Budgetbezug mit Erfolgkontrolle unter dem Stichwort „Lessons Learnt“ herstellen

Abbildung 7: Prozessschritte klassische Werbung

Im Themenkomplex Promotions werden potentiellen Kunden Angebote gemacht, die Produkte des eigenen Unternehmens mit einem Gewinnspiel verknüpfen. Über das Gewinnspiel werden Adressen potentieller Kunden gewonnen, die dann für weitere Werbeaktionen zur Verfügung stehen.

Es versteht sich eigentlich von selbst, es wird aber an dieser Stelle noch einmal darauf hingewiesen, dass Gewinne eines Gewinnspiels nur Interessenten, nicht aber Unternehmensangehörigen zur Verfügung gestellt werden sollten. Dasselbe gilt für Sonderveranstaltungen und Teilnahme an besonderen Veranstaltungen (VIP-Lounges), die nur von dem Vertrieb, nicht jedoch von Unternehmensangehörigen genutzt werden sollten.

Die Überprüfung dieser Budgets auf adäquate Verwendung ist immer ein lohnenswerter Ansatz für den CO-Verantwortlichen oder die IR. Gleichzeitig sollte er die Aktualität der Geschenke- und Veranstaltungsrichtlinie überprüfen, dass für die Koordinatoren und die Unternehmensangehörigen Klarheit darüber herrscht, was in dem Unternehmen als gewünschtes Verhalten eingefordert wird.

3.4. Placement/ Marktbearbeitung: Absatzmittler, Vertrieb und Absatzlogistik

Generell gilt hier seit einigen Jahren in Deutschland das Verbot der steuerlichen Abzugsfähigkeit von ausländischen Bestechungsgeldern. Unternehmen, die auch in den USA tätig sind, sei es direkt oder indirekt über eine Tochtergesellschaft, unterliegen dem

Foreign Corrupt Practises Act[25]. Verstöße gegen dieses Gesetz, egal in welchem Land der Erde begannen, können zu sehr empfindlichen Geldbußen führen (siehe u.a. Siemens, Daimler).
Der CO-Verantwortliche eines Unternehmens sollte federführend die Verabschiedung einer Richtlinie über das Verbot von Zuwendungen an Kunden betreiben.

WichtigerHierbei ist für die Akzeptanz im Unternehmen entscheidend, dass der betroffene Hinweis Vertriebsmitarbeiter die Sicherheit erhalten, keine Nachteile befürchten zu müssen, wenn sie Aufträge an den Wettbewerb verlieren, der sich nicht adäquat verhält.

Solche Informationen sollten an ihn und an die Unternehmensleitung weitergeleitet werden, damit entsprechende Maßnahmen eingeleitet werden können wie z.B. Rückzug aus dem Markt, Anzeige bei der Kartellbehörde, vertrauliche Gespräch zur Unterlassung der unerlaubten Handlung mit dem anderen Unternehmen etc.
Bei CO-Analysen im eigenen Vertrieb[26] kann z.B. die Grundsatzfrage angeschnitten werden, nach welchen Kriterien der Vertriebsmitarbeiter entlohnt wird,

- nach Anzahl Neuverträge/Neukunden,
- nach Erreichen bestimmter Absatzziele,
- nach Erreichen bestimmter Umsatzziele,
- nach bezahltem Umsatz (Umsatz – Forderungsverluste)
- oder gar nach dem erzielten Kundendeckungsbeitrag (bezahlter Umsatz – Vertriebskosten).

Die letzte Größe ist steuerungstechnisch nach Auffassung des Autors die sauberste. Die Problembereiche, die Rentabilität kosten, sind in diesem System weit gehend eliminiert. Weiter werden Möglichkeiten eliminiert, Vertriebsziele auf Kosten des Unternehmens zu erreichen.
Nur Neuverträge als Kriterium für die Provision können beispielsweise dazu führen, dass Altverträge überproportional gekündigt werden, Vertragsstornos steigen, die Kundenqualität und -rentabilität abnimmt und trotzdem noch Provision gezahlt wird.
Absatz statt Umsatz als Provisionskriterium kann das Risiko in sich bergen, dass absolute Deckungsbeiträge rückläufig werden und Fixkostenbeiträge zunehmend nicht mehr erwirtschaftet werden.
Fakturierten Umsatz statt bezahlten Umsatz zu provisionieren kann den Anteil nicht zahlungsfähiger Kunden und damit die Forderungsverluste ansteigen lassen. Der Vertrieb wird bei dem Kriterium bezahlter Umsatz auch diszipliniert, das ungeliebte Thema Datenpflege im Kundenstamm anzugehen und die Adressdaten zu aktualisieren. Fehlende Adressdaten, wenn sie nicht beim Kaufabschluss aktualisiert werden, sind in der Folge einer der Hauptgründe für Forderungsausfälle, da ein Schuldner ohne aktuelle Adresse schwer zu finden ist.
Letztlich führt die Einbindung der eigenen Vertriebskosten in die Provisionsziele zu einem sorgsamen Umgang mit den eigenen Ressourcen und zu einer Selbststeuerung im Vertrieb, da jeder von Kostensteigerungen betroffen wäre und gleichermaßen von Kostensenkungen in seiner Vertriebsprovision profitieren würde.
Für Compliance-Analysen bietet es sich an, mit Hilfe der IT in den Kundendaten auffällige

[25] Siehe www.justice.gov/crinimal/fraud/fcpa/
[26] Der Autor beschränkt sich hier aus Vereinfachungsgründen auf den eigenen Vertrieb. Die Themen gelten analog auch für Vertriebspartnerschaften wie Franchising, Kommisions- und Konsignationsgeschäfte u.ä. Der Zugriff auf die Daten kann eingeschränkt sein, wenn die Verträge nicht im Einzelnen konkrete Rechenschaft der Partner vorsehen.

Muster herauszufinden und dann im Einzelnen zu analysieren.
Bei personenbezogenen Daten sind immer der Sozialpartner und der Datenschutzbeauftragte in Kenntnis zu setzen. Die Analysen sind zunächst anonymisiert durchzuführen und erst bei bestätigtem Verdacht dem Sozialpartner vorzulegen, um die dann notwendige Personalisierung zu erreichen.
Auffälligkeiten in Kundenumsätzen können sprunghafte Entwicklungen sein, d.h. die Umsätze nehmen sehr schnell in 6-12 Monaten zu, um danach wieder in sich zusammenzufallen (*Strohfeuereffekte*). Statt dauerhaft interessierten Stammkunden wurden Neukunden unter falschen Voraussetzungen geworben, die nach kurzer Zeit wieder dem Unternehmen den Rücken gekehrt haben, also inaktiv wurden.
Ebenso auffällig sind *100% Stornos* gerade beim Werben von Unternehmenskunden. Hier könnte der Verdacht bestehen, dass die Unternehmen gar nichts davon wussten, dass sie als Kunden geworben worden waren. In der Neukunden-Provisionierung wurden sie jedoch mit gezählt.
Wenn nach großen Werbeaktionen in sechs Monaten danach die Anzahl der dubiosen Forderungen stark ansteigt, könnte das Bonitätssystem des Unternehmens umgangen worden sein, dass das Unternehmen vor nicht zahlungsfähigen Kunden schützen sollte.
Auffällig sind auch Umsatz- und Bezahlungsmuster bei einzelnen Kunden, die zunächst unauffällig erscheinen, um dann plötzlich im Umsatz zu explodieren zusammen mit dann schleppender Bezahlung. In diesem Fall sind alle Hintergründe der Auftragsfreigaben inkl. manueller Eingriffe in Systemsperren zu analysieren.
Hohe Erlösschmälerungen (Rabatte, Skonti, Sondergutschriften; Retouren, Stornos) bei einem Kunden sprechen für eine angespannte Kunden-Lieferanten-Beziehung. In diesem Fall sollte weiterführende Gespräche mit dem Kunden geführt werden, um die wahren Ursachen der Verärgerung oder Unzufriedenheit zu entdecken. Lässt sich auf Managementebene jedoch nichts Auffälliges feststellen, sollten alle Rücküberweisungen bankkontenmäßig analysiert werden, um festzustellen, ob die Gelder überhaupt an die richtigen Kunden zurückgeflossen sind.
Viele *manuelle Buchungen* auf Kundenkonten können für akuten Handlungsbedarf stehen, insbesondere dann, wenn die Kundenstatistik nicht aus dem zentralen Buchhaltungssystem abgeleitet wird, sondern selbst erstellt wird (fehlendes CRM: Customer Relationsship Management).

Die nachstehende Tabelle fasst das Gesagte noch einmal zusammen:

Vorgang	**Red Flag**	**Abhilfe: Maßnahme**
Kunden-auswahl	Sehr schnell hohe Umsätze	Zug-um-Zug-Auftragsfreigabe; Provisionierung von nachhaltigem Umsatz
	100% Stornos von Aufträgen und Verträgen	Provisionierung von Umsatz statt Auftragsvolumen
	Auftragserteilung ohne Legitimationsprüfung	Provisionsabzug bei dubiosen Forderungen von Neukunden
Zahlungs-verhalten	Schleppend bis gar nicht von Anfang an	Bonitätsprüfung vor Auftragfreigabe
	Zunächst vertragsgemäß, danach bei höheren Umsätzen immer schleppender	Einsatz von intelligenter Software mit Mustererkennung und Clusterverfahren
Kunden-Deckungs beiträge	Signifikant niedrigere DB`s bei Umsatz- und Absatzzuwächsen;	Überprüfung der Rabattierungen und Deckungsbeiträge; Einführung von Sondergenehmigungen nur durch die Geschäftsleitung
	Überproportional hoher Anteil an Erlösschmälerungen	Genaue Analyse der Retouren, Sondergutschriften; Boni und Skonti auf Berechtigung; Einführung von Sondergenehmigungen nur durch die

Geschäftsleitung

Abbildung 8: Red Flags im Vertrieb

4. IT-Kontrollen im Vertrieb

Mit der Einführung von CRM (Customer Relationshipment Management) ist es heute in modernen Unternehmen möglich, die Vertriebsdaten mit denen im Rechnungswesen zu verzahnen. Es kann in allgemeine und spezielle Kontrollen unterschieden werden. Zu den allgemeinen Kontrollen gehören u.a. Zugangs- und Verarbeitungskontrollen.

4.1. Zugriffskontrollen

Es gilt, dass der Zugang zu den Unternehmensdaten nur Berechtigten gewährt werden sollte. Sichergestellt werden kann dies durch ein sog. Rollenkonzept, in dem jedem Nutzer die für seine Tätigkeit notwendigen Rechte eingeräumt werden. Es versteht sich von selbst, dass sog. *Super-User-* und *Administratorrechte* nur einem ausgewählten Personenkreis zugänglich gemacht werden dürfen.
Diese Funktionen gewähren Zugang zu Systembefehlen, die Eingriffe in das System und in den Buchungsstoff gewähren, ohne eine Spur zu hinterlassen. Gleiches gilt für den Befehl „Erase“, der wie früher das Radieren, Daten spurlos löscht. Die Öffnung des Systems muss auf der einen Seite möglich sein, um ungeplante Fehler oder Stillstände/ Blockaden auflösen zu können. Auf der anderen Seite ist auf die nachträgliche Dokumentation penibel Wert zu legen, um nicht das Abschlusstestat aufs Spiel zu setzen.
Um generell Unbefugten den Zugang zu den Unternehmenssystemen zu erschweren, sollte das individuelle Password regelmäßig gewechselt und eine Mindestlänge von 8 Stellen besitzen. Das Password sollte sowohl aus Buchstaben, Zahlen und Sonderzeichen bestehen und regelmäßig gewechselt werden. Der Wechsel kann dann noch systemmäßig überwacht bzw. eingefordert werden.
Remote-Zugriffe auf das Unternehmensnetzwerk sind besonders sensibel, wenn sie nicht über gesicherte Leitungen geführt werden. Den besten Schutz gewähren SMART-Cards, die ihren Private-Key hardwaremäßig auf der Karte verdrahtet haben. Damit kann ein verschlüsselter Dialog nicht von Dritten ausgespäht werden, weil nur der Public Key softwaremäßig vorhanden ist.
Eine weitere Möglichkeit der Sicherheit in der Remote-Kommunikation ist die Nutzung des *https-Modes*. Im Online-Banking wird dieser Modus von der Bank über ihren Server dem Netz mitgeteilt und über den Browser des Kunden bestätigt. Notwendig ist ein Zertifikat, das wiederum von einer zertifizierten Stelle vergeben wurde und dann in allen gebräuchlichen Browsern akzeptiert wurde. Da durch Vortäuschung eines Servers, der ebenfalls über ein Zertifikat verfügen muss, Bankkunden getäuscht werden können, wurde auf Smartcards oder Handy umgestellt, die dann die iTAN erzeugen können bzw. die die iTAN auf einem anderen Kommunikationsweg mitgeteilt bekommen.

4.2. Verarbeitungskontrollen

Ziel der Verarbeitungskontrollen ist es, dass erfasste Daten *zuverlässig, zeitnah, vollständig und formell und materiell* verarbeitet werden, Fehler durch Abstimmsysteme erkannt und bereinigt, und Folgevorgänge aufgrund der vereinbarten Verarbeitungslogik „angestoßen“ werden.
Durch Vollständigkeitskontrollen wird sichergestellt, dass alle eingegebenen Datensätze in den nächsten Programmschritten auch verarbeitet werden. Müssen Datensätze wegen

fehlender Informationen zunächst zurückgehalten werden, weiß das System, wie viele Datensätze in die „Wartedatei“ geschrieben wurden und gibt entsprechenden Statistiken zur Verarbeitung heraus.
Die Programmlogik schließt normalerweise Weiterverarbeitungen wegen formeller Fehler aus, materielle Fehler/ Beispiel müssen durch entsprechend gestaltete Plausibilitätschecks schon bei der Eingabe abgefangen werden.

Beispiel	Bei einer Internet-Bestellung möchte ein Kunde „1“ Fernseher bestellen. Das entsprechende Eingabefeld ist als numerisch gekennzeichnet (formelle Prüfung), so dass Buchstaben wie „Ein“ oder Sonderzeichen “-1-„ nicht eingegeben werden können oder einen Fehleraufruf zur Folge haben. Wird jedoch irrtümlich statt der „1“ eine „10“ eingegeben, so erfolgt normalerweise aus formalen Gründen keine Fehlermeldung, da das Feld ja numerisch definiert ist. Eine Plausibilitätsprüfung macht sich zunutze, dass es extrem unwahrscheinlich ist, dass ein Endkunde trotz eines tollen Angebots gleich 10 Fernseher auf einmal bestellen wird und weist die Bestellung ab. Um den seltenen Fall eines tatsächlich handelnden Wiederverkäufers mit abzudecken und den Umsatz damit zu retten, kann das Feld auf ein Callcenter verweisen, wo nach Kreditprüfung dann die Bestellung aufgenommen wird.

Nicht akzeptierte Eingaben bzw. abgewiesene Datensätze während der Verarbeitung müssen zeitnah wieder der Verarbeitung zugeführt werden, um unnötige Kosten zu vermeiden. Diese Aufarbeitung der Warte- Fehlerlisten-Datensätze sollte von den zuständigen Stellen der Fachseiten als Sonderaufgabe organisiert werden, um Folgefehler zu vermeiden.
In den heute gebräuchlichen Dialogsystemen werden Änderungen an den Daten durch die Nutzer sofort durchgeführt. Trotzdem müssen Sicherheiten vom Systemdesigner vorgesehen sein, die bei Verarbeitungsproblemen (*Überlastungen, Abbrüchen, Deadlock-Konflikten*[27]) einen Restart ermöglicht und den Aufsetzpunkt allen Nutzern mitteilt. Moderne Systeme erlauben diese Restarts, da sie durch interne Meldungen während der Verarbeitung in festen Rhythmen den Status der Verarbeitung festschreiben (Audit Trails).
Zusätzlich enthalten Audit Trails auch den *Versionsstand,* mit der Daten einer bestimmten Periode erfasst wurden. Änderungen der Software, die dann doch nichtfunktioniert haben, können wieder eliminiert werden, die Software wird wieder eine Version zurückgesetzt. Wichtig in diesem Zusammenhang ist die Regelung der Verantwortung, dass das IT-System Teil eines Geschäfts-Prozesses ist, den eine Fachseite zu verantworten hat. Änderungen an der IT-Software bedürfen somit der Genehmigung der Fachseite, die zusätzlich die erfolgreiche Änderung in einer neuen Version durch ihr o.k. dokumentiert.

4.3. IT-Kontrollen im Vertrieb

Im Vertrieb sind für entsprechende Werbeaktionen Stamm- und Bewegungsdaten von Kunden und Interessenten relevant.
Da es sich immer um personengebundene Daten handelt, kommt der Datenschutz ins Spiel und damit die schriftliche Einwilligung der Interessenten, dass das Unternehmen die Daten auch zu werblichen Zwecken nutzen darf. Die brandaktuelle Diskussion um die Nutzung von historischen Facebook-Daten zeigt exemplarisch den Unterschied im Datenschutz zwischen Deutschland/ Europa und den USA. Auch die Diskussion um die Veröffentlichung

[27] *Überlastungen* eines Systems kündigen sich in der Regel schon mit stark ansteigenden Antwortzeiten an. *Abbrüche* sind Verarbeitungsprobleme, die von den Systemspezialisten beseitigt werden müssen. Diese Eingriffe sollten immer dokumentiert werden, um nicht die ordnungsgemäße Verarbeitung aufs Spiel zu setzen. *Deadlock* beschreibt einen Konflikt, bei z.B. zwei Nutzer auf das gleiche Konto oder dieselbe Tabelle Änderungen vornehmen wollen. Ist ebenso möglich beim Adressabgleich zweier Server, die gleichzeitig Änderungsmeldungen erhalten und sich nicht synchronisieren können. Dies kann dann zum kompletten Abbruch der Verarbeitung führen, weil die Cache der Server mit Verwaltungsdaten überlaufen.

fotografierter Google-Straßenabschnitte mit einer Vielzahl von Einsprüchen zeigt deutlich die Sensibilität des Datenschutzthemas in Deutschland.
O² hat die gerade geplante Nutzung von Mobilitätsprofilen seiner Kunden zu kommerziellen Zwecken wegen großer Proteste aus der Öffentlichkeit (wenigstens fürs Erste) aufgegeben
Dass Facebook- und Google-Daten eine hohe Relevanz für die werbetreibende Industrie darstellen, lässt sich anhand der immer noch sehr hohen Streuverluste[28] von über 90 % in Zeitungsbeilagen belegen. Das heißt, dass die hohen Beilagekosten nur in weniger als 10% zu Umsatz führen, lässt jeden Vertriebler nach Möglichkeiten Ausschau halten, die Effektivität von Werbeaktionen zu erhöhen. Das personalisierte Internet würde diese Quoten deutlich erhöhen[29]. Es muss jedoch das Einverständnis des Nutzers eingeholt werden. Dieser hat dann einer Kommunikation mit Gleichgesinnten („Freunde") ein Interesse (Community), nicht jedoch immer daran, mit Junkmails und Werbebanner-Einblendungen zu Themen beglückt zu werden, die er als persönliche Vorlieben in Facebook u.a. Community-Website eingestellt hatte[30].
Über ein sog. Matching (Abgleich unterschiedlicher Dateien über einen identischen Schlüssel) lässt sich im Unternehmen eine Sicherheit darüber herstellen, dass nur Kunden, eingewilligte Interessenten und nicht auf der „Robinson-Listen" Verzeichnete für die Mailingaktion ausgewählt werden.
Dass unrechtmäßig angeschaffte und zum Kauf angebotene Kundendaten eine Anzeige bei den Strafverfolgungsbehörden zur Folge haben mit vorheriger Information des geschädigten Wettbewerbers, versteht sich unter ehrbaren Kaufleuten als Selbstverständlichkeit und wird der Vollständigkeit halber hier nur am Rande erwähnt.
Mit IT-Analysetools lassen sich z.B. in der Kundendatenbank[31] diverse Analysen durchführen, die das Kaufverhalten des Kunden mit der Unternehmensstrategie besser in Abstimmung bringen könnten. Zu denken sind an Analysen

- in Stammkunden und Neukunden,
- Groß-, Mittel- und Kleinkunden,
- hohe bis niedrige Deckungsbeiträge je Kundengruppe
- Sortiments- und Produktvorlieben
- Zahlungsverhalten
- Regionale Verdichtung eigener Kunden im Vergleich zu den Ballungsräumen
- Kaufkraft, Alter, Branchenzugehörigkeit etc.

So sinnvoll alle diese Analysen sind, immer ist zu beachten, dass die Compliance-Belange erfüllt werden, um ein rechtmäßiges Handeln des Unternehmens sicherzustellen.

5. Zusammenfassung

Ein Unternehmen kann auch im Vertrieb einige Vorkehrungen treffen, um sich vor den unerlaubten Handlungen seiner Mitarbeiter und Manager zu schützen.
Im Red Flag Dreieck von Gelegenheit, Motiv und Rechtfertigung besitzt der Punkt Gelegenheit die größten Handlungsoptionen für ein Unternehmen. Aber auch am Punkt Motiv und Rechtfertigung eines potentiellen Täters lässt sich im Unternehmen arbeiten. Im Vordergrund stehen hier der Vorgesetzte und die Führungskultur im Unternehmen.
Zusätzlich sind Personalabteilung und Fachvorgesetzter bei Neueinstellungen gefordert, mit der notwendigen Sachkunde und dem geforderten Dokumentennachweis.

---

[28] Sind der Teil einer Werbeaktionen, der ohne Response (Antwort) eines potenziellen Kunden verpufft.
[29] Tatsächlich stellt z. B. Google seinen Kunden eine Clicksystematik zur Verfügung, mit der sich alle vorher besuchten Websites des Nutzers rückwärts von der Unternehmensseite analysieren lassen. Die Transparenz des Entscheidungsprozesses vor dem Kauf wird hierdurch sehr transparent.
[30] Facebook bestreitet zurzeit die Eigentumsrechte an historischen und gelöschten Daten der Nutzer. Nach Auffassung des Autors wird sich diese Position auf jeden Fall in Deutschland nicht halten lassen.
[31] Natürlich können mit Hilfe dieser Tools auch aus anderen Datenbanken unter dem Stichwort „Big Data" und Data Mining eine Vielzahl sinnvoller Analysen durch geführt werden.

Die USP ist auch heute noch für die Unternehmen ein hohes Gut, dass von den Unternehmen auf den Märkten z.T. erbittert verteidigt wird. In der „Produktentwicklung“ werden anhand von vielen praktischen Fällen Möglichkeiten angeboten, sich gegen Angriffe ihrer USP legal zu schütze. Diese umfasst zusätzlich zum gebotenen Patent- und Gebrauchsmusterschutz die Etablierung einer Geheimhaltungsrichtlinie, die die zulässige Außenkommunikation regelt und die Felder der schützenwerten Vermögenswerte im Unternehmen beschreibt.
Die Nutzung von SMART-Cards und andere Möglichkeiten sicherer Kommunikation außerhalb der Unternehmensräume werden beschrieben.
Red Flags wie schleichender Kundenverlust, Nachahmerprodukte u.a. werden mit möglichen Gegenmaßnahmen wie Anzeigen bis hin zum Marktrückzug und Aufgabe von Kooperationen erläutert.
Innerhalb der Preispolitik wird versucht, etwas Transparenz in den Markt von Absatzmittlern hineinzubringen. Die Reputationsrisiken aufgrund von unerlaubten Handlungen werden an einer Reihe praktischer Fälle diskutiert. Der Werbeprozess beschäftigt sich von der Planung bis hin zur Vergabe einzelner Leistungen im Werbeobjekt. Durch Gestaltung der entsprechenden Verträge und Aufbau einer eigenen Kompetenz wird versucht, diesen Unternehmensbereich etwas zu entmystifizieren und den Einkauf von Werbeleistung auf dieselbe professionelle Stufe wie übrige Güter und Dienstleistungen zu stellen. Das Thema Geschenke inkl. Einladungen zu Events wird ebenfalls beleuchtet.
Im Vertrieb wird das Zusammenspiel von Umsatz und Provision ebenso beleuchtet wie die Auftragskontrolle und auffällige Umsatz- und Bezahlungsmuster von Kunden. Abhilfen wie Massendatenanalysen und intensive Diskussion einer sinnvollen Vertriebsprovision werden dargestellt .Red Flags im Vertrieb wie hohe Auftragsstornos, Retouren und Sondergutschriften werden im Einzelnen diskutiert und Maßnahmen zur Abhilfe besprochen.
IT-Controls haben den manuellen Aufwand in den Unternehmen stark reduziert und werden deshalb verstärkt eingesetzt. Diese Controls besitzen nicht die Möglichkeit der Fehlerkorrektur, sondern geben nur Hinweise auf Fehler und Probleme, die dann vom Management in Aktionen umgesetzt werden. Man unterscheidet bei den IT-Controls in Zugangs- und Verarbeitungskontrollen. Zugangskontrollen regeln, dass nur Berechtigte die Möglichkeit erhalten, auf IT-Systeme zuzugreifen. Verarbeitungskontrollen stellen die Vollständigkeit, Richtigkeit, Zeitnähe und in gewissem Umfange auch inhaltliche Plausibilität der Verarbeitung sicher.
Durch die Möglichkeit der Massendatenanalyse gibt es heute die Chance, mit mächtigen Dateianalyse-Programmen wie ACL und IDEA auch im Compliance-Bereich systematisch auf die Suche nach Red Flags zu gehen.
Soweit personenbezogene Daten betroffen sind, sollten Sozialpartner und Datenschutz vorab in Kenntnis gesetzt werden.
Für alle Datenbanken bestehen heutzutage viele Möglichkeiten von Hypothesentests, vom Benford-Test hin zu auffälligen Mustern bei den Bewegungsdaten. Mit der Internen Revision steht dem Unternehmen eine prozessunabhängige Instanz zur Verfügung. Diese kann das Unternehmen für seine Zwecke immer dann einsetzen, wenn Doppelarbeiten zwischen CO und IR vermieden werden sollen sowie Fach-Wissen und intime Unternehmens- und Prozesskenntnis benötigt werden.

Literaturverzeichnis

I. Einschlägige Gesetze und Vorschriften

Abschlussprüferrichtlinie (8. EU-Richtlinie),EU
Aktiengesetz (AktG),D
Betriebsverfassungsgesetz;D
Bilanzrechtsmodernisierungsgesetz (BilMoG), D
Bundesdatenschutzgesetz, D
Deutscher Corporate Governance Kodex (DCGK), D
Foreign Corruption Practises Act (FCPT), USA
Gesetz gegen den unlauteren Wettbewerb (UWG), D
Gesetz zur Kontrolle und Transparenz in Unternehmen (KonTraG), D

Handelsgesetzbuch (HGB), D
MaRisk, D
SarbanesOxley Act (SOX),USA
Telekommunikationsgesetz (TKG), D

II. Empfehlenswerte Bücher und Studien

DIIR-Standard Nr. 5: Standard zur Prüfung des Anti-Fraud-Management-Systems durch die Interne Revision, Frankfurt a.M., 24.5.2012

Ernst&Young: 10. Global Fraud Survey: Korruption, Das Risiko der Anderen, Stuttgart, 2008

Kotler/ Kartajaya/ Setiawan: Die neue Dimension des Marketings: Vom Kunden zum Menschen ,campus, Frankfurt a.M, 2010: Die Autoren stellen Marketing in Dienst der Nachhaltigkeit und belegen, dass nachhaltig wirtschaftende Unternehmen auf Dauer zu größeren Erfolgen fähig sein, weil sie als akzeptierter Teil der Gesellschaft wahrgenommen werden.

Kotler: Marketingmanagement: Strategien für wertschaffendes Handeln, 12. Auflage, Pearson Studium, München, 2007: Das Standardwerk des Marketings, unverzichtbar für jeden, der sich mit Markting beschäftigen will.

Kregel, Peemöller: Grundlagen der Internen Revision, Erich Schmidt Verlag, Berlin, 2010: Die Autoren stellen im ersten Band der Handbuchreihe den aktuellen Stand der Internen Revision dar. Das Nachschlagewerk ist sowohl für den an Interner Revision Interessierten wie auch den Fachmann ein wertvoller Ratgeber. Es besticht durch seine aktuellen wissenschaftlichen und berufsständischen Grundlagen als auch durch seine vielen praktischen Beispiele und Handlungsempfehlungen.

IdW: PS 980: Prüfung des Compliance Management Systems, Düsseldorf, 2011: Der Prüfungsstandard fasst die Prüfungsschwerpunkte der Prüfung des Compliance Management Systems mit den Komponenten Einrichtung, Ausgestaltung und Überwachung zusammen und grenzt ihn gegenüber dem Risikomanagement und IKS-Prüfungen ab. CMS-Prüfungen sind Prüfungen der Corporate Governance eines Unternehmens als Prophylaxe zur Gesetzeskonformität. Die Wirksamkeit eines CMS leidet besonders dann, wenn Regelverstöße im Unternehmen ohne Konsequenzen bleiben.

IdW: PS 210: Zur Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung., Düsseldorf, 2006: In diesem Standard wird auf die abschlussrelevanten Red Flags detailliert hingewiesen.

IFAC, New York, USA: ISA 240: Der Prüfungsstandard erläutert die Verantwortung des Abschlussprüfers beim Auffinden von Fraud-Fällen im Abschluss. Dieser Standard fasst die Fraud-Verantwortlichkeit enger als der deutsche PS 210, der alle Gesetzesverstöße in einem Unternehmen erfasst und im Hinblick auf die Abschlussrelevanz bewertet.

KPMG: Studie „Wirtschaftskriminalität in Deutschland 2010, Fokus Mittelstand,“, 2010

McCarthy: *Basic Marketing: A Managerial Approach*, 1960: Das Basiswerk des Marketings, das dann von Philip Kotler weiter entwickelt wurde.

Sykes& Matza:Techniques of Neutralization: A Theory of Delinquency (1957 - mit David Matza); deutsche Übersetzung: Techniken der Neutralisierung. Eine Theorie der Delinquenz. In: Kriminalsoziologie. F. Sack und R. König. Frankfurt am Main, Akademische Verlagsgesellschaft, 1968.: Bahnbrechender Ansatz eines studierten Soziologen und Kriminologen, der mit dem Neutralisierung fünf Techniken beschreibt, mit dem Straftäter ihre Verantwortung an der kriminellen Handlung leugnen bzw. auf andere verlagern.

III. Interessante Internetlinks

Stichwort	**Link**
ACL	www.acl.com
Apple-Samsung	http://www.stern.de/digital/telefon/gegenklage-gegen-apple-samsung-schlaegt-zurueck-1729438.html
Benford-Analyse	www.i-analyzer.de/resources/Benford_Betrugsaufdeckung.pdf
Daimler-Bestechungsskandal	www.sec.gov/news/press/2010/2010-51.htm
Deutsche Institut für Interne Revision e.V.	www.diir.de
Ehrbarer Kaufmann	www.veek-hamburg.de
Fraudprophylaxe	http://www.acfe.com/resources/view.asp?ArticleID=253
IDEA	www.audicon.net
Microsoft	http://news.cnet.com/8301-10784_3-9880256-7.html
Mitarbeiterbefragungen	www.tns-infratest.com/marketing_tools/**trim**.asp

Patente und Gebrauchsmuster	www.dpma.de
Institut of Internal Auditors, Altamonte, USA	www.theiia.org
Transparency International	www.transparency.de
Vereitelter Sprengstoffanschlag in Berlin, September 2011	www.morgenpost.de
War Room als Teil des Manager-Cockpits	www.patrick-georges.net