

A photograph of a man from behind, wearing a dark blue suit jacket and a light blue shirt. He has his right hand tucked behind his back, with his index finger pointing towards the left. The background is a solid light blue color.

# Wirtschaftskriminalität in Deutschland 2010

Fokus Mittelstand



# Wirtschaftskriminalität in Deutschland 2010

## Fokus Mittelstand

# Inhaltsverzeichnis

Vorwort	3
Zusammenfassung der Ergebnisse	4
Einschätzungen und Erfahrungen mit Wirtschaftskriminalität	6
Aufdeckung – Kommissar Zufall hilft	11
Reaktion – Professionalisierung in der Aufklärung nötig	13
Vermeidung – Überschätzung der etablierten Kontrollmechanismen	17
Fokus Mittelstand – Paradigmenwechsel gefordert	22
Forensic – Wirtschaftskriminalität vermeiden und bekämpfen	27
Eckdaten der Studiendurchführung	28

# Vorwort

Seit nunmehr zehn Jahren erforscht KPMG das Phänomen Wirtschaftskriminalität. Zu Beginn alleine und später mit der Unterstützung eines renommierten Sozialforschungsinstituts begannen wir 1999 damit, im Abstand von circa drei Jahren die erste und zweite Führungsebene von Unternehmen verschiedenster Branchen nach ihren Erfahrungen mit Wirtschaftskriminalität und den von ihnen implementierten Präventions- und Aufdeckungsmaßnahmen sowie zum Umgang mit entdeckten Fällen zu befragen.

Dabei ist das Thema Wirtschaftskriminalität auf der Agenda der Vorstände, Geschäftsführer und Aufsichtsräte weiter nach oben gerückt. Eine steigende Anzahl von Unternehmen investiert verstärkt in Präventions- und Entdeckungsmechanismen, zum einen aus einer gestiegenen Sensibilität gegenüber dem Thema, zum anderen aus einer verbesserten Kenntnis über die Möglichkeiten und Grenzen der Verhinderung beziehungsweise Aufdeckung von wirtschaftskriminellen Handlungen. Zusätzlich befördert wurde das Thema durch die öffentliche Aufmerksamkeit bei wirtschaftskriminellen Handlungen und die daraus folgenden Reputationsschäden für Unternehmen, Führungskräfte und Aufsichtsorgane, die nicht zuletzt bemüht sind, das persönliche Risiko im Rahmen der immer strengeren Corporate-Governance-Anforderungen zu reduzieren.

Die Studienergebnisse zeigen aber auch deutlich, dass es an verschiedenen Punkten noch wesentlichen Verbesserungsbedarf gibt. Oftmals sind die Präventions- und Aufdeckungsmaßnahmen zu unspezifisch und erfassen etwa bei Datenanalysen sämtliche Bereiche und Mitarbeitergruppen. Neben den damit verbundenen potenziellen datenschutzrechtlichen Problemen wäre es deutlich effektiver und kostengünstiger, auf Basis typischer Verhaltens- und Betrugsmuster eine unternehmensspezifische Risikoanalyse durchzuführen und gezielt Sicherheitslücken durch Kontrollmaßnahmen zu schließen.

Das Kapitel „Fokus Mittelstand – Paradigmenwechsel gefordert“ (Seite 22) zeigt, dass das Thema Wirtschaftskriminalität von mittelständischen Unternehmen immer noch stiefmütterlich behandelt wird. Dabei bewegen mittelständische Unternehmen erhebliche Finanzvolumina, verfügen oft über technisch einmaliges Know-how, produzieren und vertreiben im Ausland, arbeiten mit einer Vielzahl von externen Partnern zusammen und sind aufgrund der Komplexität ihres Geschäftsmodells gegenüber der Wirtschaftskriminalität stark exponiert. Aus unserer Sicht muss zukünftig auch im Mittelstand die Auswahl geeigneter Strategien zur Bekämpfung der Risiken an Bedeutung gewinnen, ohne allerdings die gerade in familiengeführten Unternehmen oftmals betonte und gelebte Vertrauenskultur zu zerstören.

In diesem Sinne wünsche ich Ihnen eine interessante Lektüre.

Ihr

**Frank M. Hülsberg**

Leiter Forensic

# Zusammenfassung der Ergebnisse

## **Bedrohung durch Wirtschaftskriminalität steigt weiter**

Immer mehr deutsche Unternehmen sehen Wirtschaftskriminalität als Gefahr für die Wirtschaft. Der Trend ist in den letzten zehn Jahren eindeutig und beweist die steigende Wahrnehmung des Phänomens Wirtschaftskriminalität aufseiten der Privatwirtschaft. Von 2006 bis 2010 ist der Anteil der Unternehmen, die Wirtschaftskriminalität als ernsthaftes Problem für das Wirtschaftsleben betrachten, um weitere neun Prozentpunkte gestiegen und liegt nun bei 80 Prozent, bei Großunternehmen sogar bei 90 Prozent.

## **Adressierung des Themas ist in den Unternehmen angekommen**

Mit gestiegenem Problembewusstsein setzen sich Unternehmen zunehmend mit dem Phänomen Wirtschaftskriminalität auseinander und haben umfassendes internes Fachwissen in Bezug auf wirtschaftskriminelle Handlungsmuster aufgebaut.

In den letzten drei Jahren haben Unternehmen massiv in ihre Kontroll- und Aufklärungssysteme investiert. So setzen 91 Prozent der Unternehmen inzwischen im Rahmen der Aufklärungsarbeit auf interne Kräfte, wie die Interne Revision oder Task Forces, 2006 lag der Anteil nur bei 77 Prozent. Auch die Präventionssysteme wurden unter anderem durch die Überarbeitung von Berechtigungskonzepten und die Verbesserung interner Kontrollen deutlich optimiert.

## **Professionalisierung in der Reaktion zum Schutz vor Reputationsschäden nötig**

Unternehmen sollten sich bei der Bekämpfung von Wirtschaftskriminalität nicht ausschließlich auf die klassischen Unternehmensbereiche wie Einkauf und Vertrieb konzentrieren. Zwar findet sich hier weiterhin die größte Anzahl von Betrugsfällen, andere Geschäftsbereiche wie die Rechnungslegung oder das Kreditmanagement sind aber auf dem Vormarsch. Außerdem ist Wirtschaftskriminalität in letztgenannten Bereichen mit einem weitaus höheren Schadenspotenzial verbunden, vornehmlich auch durch einen potenziellen Reputationsverlust und die damit verbundenen negativen Folgen.

Das Hauptaugenmerk bei der Betrugs- und Korruptionsbekämpfung liegt bislang im Aufdecken und Aufklären wirtschaftskrimineller Handlungen. Auch wenn dies selbstverständlich von großer Bedeutung ist, vernachlässigen viele Unternehmen gleichzeitig die Reaktion auf konkrete Fälle sowie den nachhaltigen Umgang mit Verdachtsfällen. Dies steigert die Gefahr von Reputationsschäden.

## **Systeme wiegen Unternehmen in falscher Sicherheit**

Trotz des Aufbaus von Kontroll-, Aufklärungs- und Präventionsstrukturen bleibt viel zu tun. Denn auch wenn sich die meisten Unternehmen bei den eingeführten technischen Maßnahmen und präventiven Kontrollen sehr gut aufgestellt sehen, verlassen sich viele zu stark auf diese Systeme und passen

sie nicht an das sich verändernde Umfeld an. Prävention wird eher als „Rundumschlag“ betrieben, anstatt Verhaltens- und Betrugsmuster zu analysieren und auf dieser Basis die Maßnahmen intelligent zu konzeptionieren. Beispielsweise sollten besonders risikoreiche Geschäftsbereiche fokussiert betrachtet und Maßnahmen laufend angepasst werden.

**Compliance und Prävention –  
der Blick über den Tellerrand wird  
vernachlässigt**

Unternehmen sind in ihren wirtschaftlichen Aktivitäten nicht auf sich gestellt, sondern mit Kunden und Lieferanten zunehmend eng verzahnt. Wirtschaftskriminelle Handlungen innerhalb der Lieferkette sind daher häufig mit einem Risiko für das eigene Unternehmen verbunden. Die Umfrageergebnisse zeigen, dass die meisten Unternehmen diesen Risiken kaum proaktiv begegnen. So gaben lediglich 29 Prozent der Befragten an, Integritätskriterien in die Lieferantenbewertung beziehungsweise -entwicklung aufzunehmen. Auch führt mit

56 Prozent über die Hälfte der Unternehmen keine Analysen wirtschaftskrimineller Handlungen von verbundenen Unternehmen und Dienstleistern durch.

Wie prominente Skandale in diesem Jahr gezeigt haben, können Maßnahmen zur Prävention von wirtschaftskriminellen Aktivitäten auch Gefahren bergen. Insbesondere wenn Mitarbeiterdaten in eine Prüfung einbezogen werden, kann der Grat zum Gesetzesverstoß oft sehr schmal sein. Und wer Kontrollmaßnahmen nicht mit Blick auf den Datenschutz entwickelt, kann schnell über den gesetzlichen Rahmen treten. In Anbetracht der aktuellen Fälle ist es überraschend, dass 90 Prozent der befragten Unternehmen die von ihnen durchgeführte systematische Vorabprüfung zur Einhaltung gesetzlicher Anforderungen als gut beziehungsweise eher gut einschätzen. Offensichtlich haben viele Unternehmen die sich aus dem Spannungsfeld Kontrolle und Aufklärung versus Datenschutz ergebenden Gefahren noch nicht erkannt.

**Fokus Mittelstand – Zeit für einen Paradigmenwechsel**

Die Gefahr durch Wirtschaftskriminalität wird vom Mittelstand weiterhin stark unterschätzt. Die Unternehmen sehen sich wesentlich weniger gefährdet als Großunternehmen. Gleichzeitig überschätzen viele Unternehmen ihre Kenntnisse hinsichtlich wirtschaftskrimineller Handlungen. Dies wird besonders bei den immateriellen Vermögenswerten deutlich. Erst wenige mittelständische Unternehmen schützen ihr Know-how und ihre Innovationen in ausreichendem Maß. Problematisch ist zudem, dass „Vertrauen“ als Organisationsprinzip weit verbreitet ist. Die potenzielle Gefahr, die von eigenen Mitarbeitern ausgeht, wird vernachlässigt. Und schließlich sind die Unternehmen weit weniger gut auf den Ernstfall vorbereitet als große Unternehmen. Ein ausgereiftes Notfallmanagement oder gar etablierte Krisenteams sind selten zu finden.

# Einschätzungen und Erfahrungen mit Wirtschaftskriminalität

Das Thema Wirtschaftskriminalität ist im zurückliegenden Jahrzehnt zu einem immer stärker öffentlich diskutierten Phänomen geworden. Dabei hat sich dieser Trend seit dem Erscheinen der letzten Studie im Jahre 2006 noch einmal beschleunigt. Die mediale Aufarbeitung großer Korruptionsskandale und Kartellrechtsverstöße trug dazu wesentlich bei.

## Immer mehr Unternehmen sehen Wirtschaftskriminalität als ernsthaftes Problem.

Mit der verstärkten öffentlichen Aufarbeitung sowie den zunehmend empfindlicheren Strafen ist auch das Problembewusstsein bei privatwirtschaftlichen Unternehmen geschärft worden.

Dies zeigt auch das aktuelle Bundeslagebild zur Korruption des BKA: Der Anstieg der Korruptionsfälle im Bereich der Wirtschaft könnte möglicherweise

„in einer zunehmenden Sensibilität und Aufklärungsbereitschaft der Privatwirtschaft als Folge der in der Vergangenheit geführten öffentlichkeitswirksamen Korruptionsverfahren begründet sein“ (BKA: Korruption. Bundeslagebild 2008, Pressefreie Kurzfassung: 16).

Während schon in den Vorjahren eine große Mehrheit (1999: 69 Prozent, 2003 und 2006: je 71 Prozent, vgl. Abb. 1) angab, das Phänomen Wirtschaftskriminalität als ernsthaftes Problem für die Wirtschaft zu betrachten, ist der Anteil von 2006 auf 2010 um weitere neun Prozentpunkte gestiegen und liegt nun bei 80 Prozent, unter Großunternehmen sogar bei fast 90 Prozent. Über zwei Drittel (67 Prozent) der Umfrageteilnehmer glauben darüber hinaus, dass das Ausmaß wirtschaftskrimineller Handlungen in nächster Zeit weiter zunehmen wird.

Unternehmen sehen Wirtschaftskriminalität also immer mehr als ernsthafte Gefahr. Der Trend ist in den letzten zehn Jahren eindeutig.

Abb. 1: Wirtschaftskriminalität – ein Problem für die Privatwirtschaft?

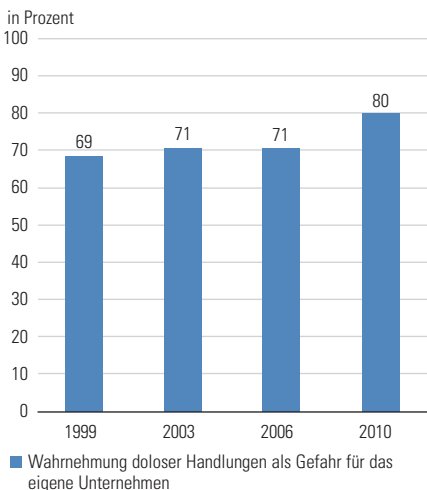
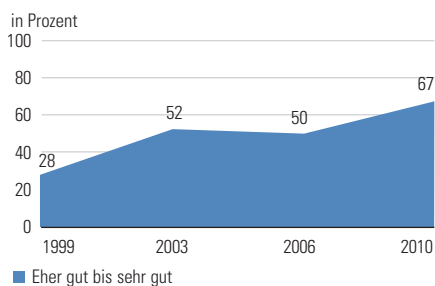


Abb. 2: Kenntnisse über wirtschaftskriminelle Handlungsmuster insgesamt



## In den letzten Jahren haben die meisten Unternehmen internes Fachwissen in Bezug auf wirtschaftskriminelle Handlungsmuster aufgebaut.

Mit dem gestiegenen Problembewusstsein haben sich Unternehmen in den letzten Jahren zunehmend mit dem Phänomen Wirtschaftskriminalität auseinandergesetzt und so internes Fachwissen in Bezug auf wirtschaftskriminelle Handlungsmuster aufgebaut (vgl. Abb. 2). So gaben in der aktuellen Umfrage 67 Prozent der Unternehmen

an, über „gute“ oder „eher gute“ Kenntnisse in diesem Bereich zu verfügen. In den Jahren 2003 und 2006 lag die Quote bei etwa 50 Prozent, 1999 sogar nur bei knapp 30 Prozent.

Die Umfrageergebnisse zeigen, dass ein wesentlicher Impuls für den Aufbau von Fachwissen die eigene Betroffenheit von wirtschaftskriminellen Handlungen (innerhalb der letzten drei Jahre) ist. So schätzten 78 Prozent der betroffenen Unternehmen ihre Kenntnisse als „gut“ oder „eher gut“ ein, unter den nicht betroffenen Unternehmen lag die Quote bei nur 60 Prozent (vgl. Abb. 3). Hieraus lässt sich vermuten, dass trotz der signifikant weiteren Verbreitung des wirtschaftskriminalistischen Fachwissens im Zeitablauf viele Unternehmen mit wirtschaftskriminellen Risiken nach wie vor eher reaktiv als proaktiv umgehen.

Des Weiteren bestätigen die Umfrageergebnisse die intuitive Vermutung, dass Großunternehmen über bessere Kenntnisse verfügen als der Mittelstand. Dieser sollte daher weiter in den Aufbau von internem Wissen investieren.

Dass dieser Wissensaufbau nicht auf die Geschäftsführung oder Abteilungen wie Recht, Interne Revision oder Compliance beschränkt sein sollte, belegt die hohe Bedeutung, die die Unternehmen einer Sensibilisierung der Mitarbeiter im Rahmen der Bekämpfung von Wirtschaftskriminalität beimessen. So vertreten 77 Prozent der Befragten die Auffassung, dass durch eine erhöhte beziehungsweise verbesserte Sensibilisierung wirtschaftskriminelle Handlungen hätten verhindert werden können (vgl. Abb. 4). Dies ist ein signifikanter Anstieg im Vergleich zu den Vorjahren: 2003 und 2006 äußerten 57 beziehungsweise 58 Prozent diese Meinung.

**Aufgrund des geschärften Problembewusstseins sowie der verbesserten Kontrollsysteme steigt die Anzahl der von Wirtschaftskriminalität „betroffenen“ Unternehmen (Kontrollparadoxon).**

Abb. 3: Kenntnisse über wirtschaftskriminelle Handlungsmuster, „nicht betroffene“ und „in den letzten drei Jahren von Wirtschaftskriminalität betroffene“ Unternehmen

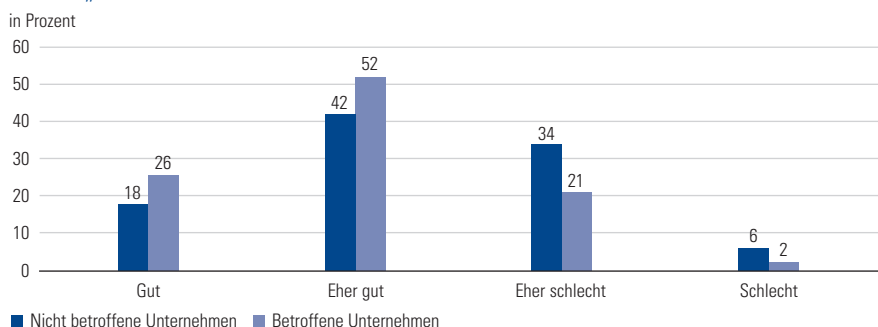
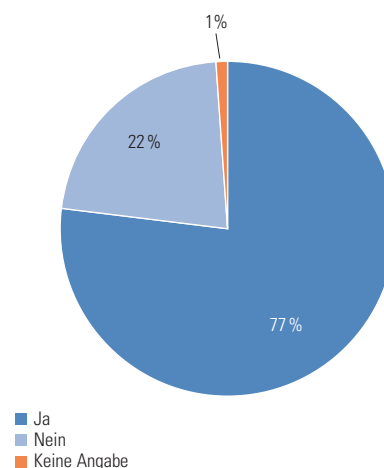


Abb. 4: Wirksamkeit erhöhter Sensibilität



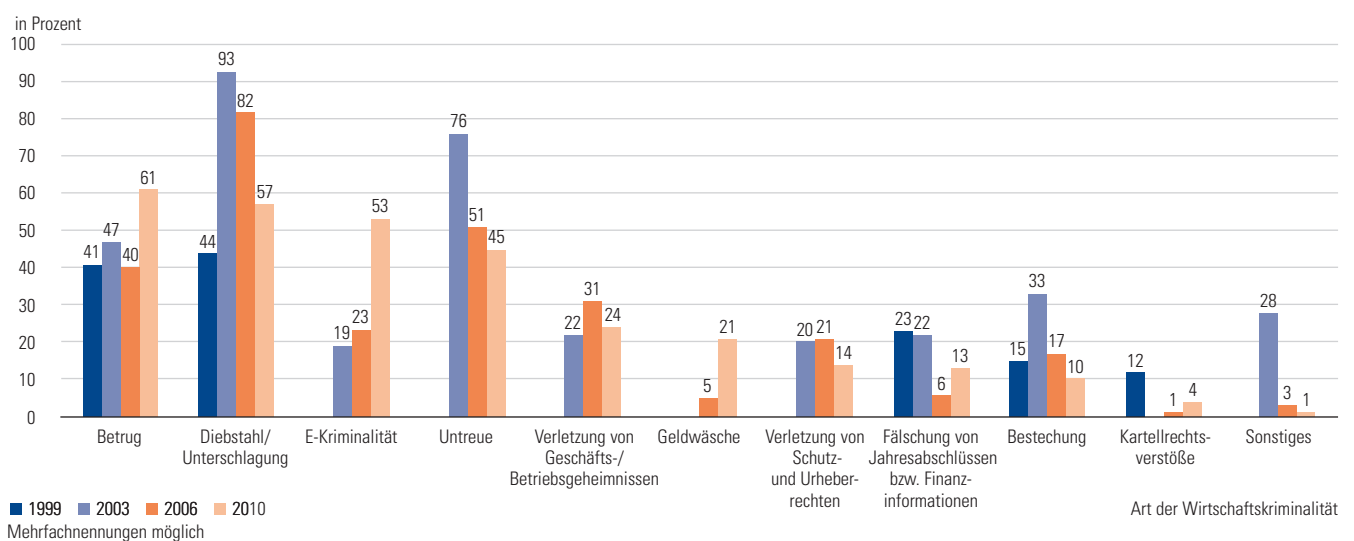
Wirtschaftskriminalität ist in Deutschland weit verbreitet. Dies zeigen die Ergebnisse der Umfrage sehr deutlich. So gaben insgesamt 37 Prozent der Befragten an, dass ihr Unternehmen in den vergangenen drei Jahren von wirtschaftskriminellen Handlungen betroffen war. Allerdings deuten diese Ergebnisse nicht unbedingt auf eine Zunahme der Wirtschaftskriminalität im Vergleich zu den Vorjahren hin. Stattdessen sind die Unterschiede im Zeitverlauf möglicherweise auf der Basis des Kontrollparadoxons zu erklären: Mit dem gestiegenen Bewusstsein einer verstärkten behördlichen Verfolgung und Sanktionierung sowie mit einer Verbesserung der Kontrollmaßnahmen werden mehr Fälle wirtschaftskrimineller Handlungen aufgedeckt. Dieses Phänomen ist in

der kriminologischen Forschung auch als „Kontrollparadoxon“ bekannt.

Wie in den Vorjahren sind die klassischen Vermögensschädigungen wie Diebstahl, Unterschlagung, Betrug und Untreue die am häufigsten auftretenden Delikte (vgl. Abb 5). Die Fälschung von Finanzinformationen sowie Formen des sogenannten Corporate Misconducts (zum Beispiel Bestechung, Kartellrechtsverstöße) sind vergleichsweise selten, steigen jedoch wieder an.

Auch wenn hier in den letzten Jahren keine deutliche Veränderung stattgefunden hat, zeigt die Umfrage doch wichtige Entwicklungen auf. So ist das Thema E-Kriminalität mit nun 53 Prozent (2006: 23 Prozent) auf dem Vormarsch

Abb. 5: Häufigkeiten und Arten von Wirtschaftskriminalität



(vgl. Abb. 5). Auch von Geldwäsche (2010: 21 Prozent, 2006: 5 Prozent) sowie der Fälschung von Jahresabschlüssen beziehungsweise Finanzinformationen (2010: 13 Prozent, 2006: 6 Prozent) sind wieder deutlich mehr Unternehmen betroffen als noch vor drei Jahren.

Die Analyse der Bereiche, die durch Wirtschaftskriminalität betroffen waren, zeigt eine starke Verschiebung zu den Bereichen Finanz- und Rechnungswesen sowie zum Kreditgeschäft, wie Abb. 6 zeigt. Aus diesen Ergebnissen lässt sich ableiten, dass wirtschaftskriminelle Handlungen in der Unternehmenshierarchie weiter nach oben wandern. Denn um die Kontrollen in diesen Bereichen zu umgehen, ist meist eine gehobene Stellung sowie gutes Fachwissen notwendig. Auch an dieser Stelle müssen die Ergebnisse allerdings mithilfe des schon diskutierten Kontrollparadoxons relativiert werden. Nicht zuletzt aufgrund neuer regulatorischer Anforderungen wie des Sarbanes-Oxley Act (SOX) haben namentlich Großunternehmen die prozessinhärenten Kontrollen in den letzten Jahren dokumentiert und verbessert. Auch die Erfahrung von KPMG zeigt, dass es in der Vergangenheit öfter zu wirtschaftskriminellen Handlungen, zum Beispiel im Bereich des Finanz- und Rechnungswesens, gekommen ist. Diese werden aber durch systematisierte interne Kontrollsysteme inzwischen häufiger aufgedeckt.

Abb. 6: Von Wirtschaftskriminalität betroffene Unternehmensbereiche

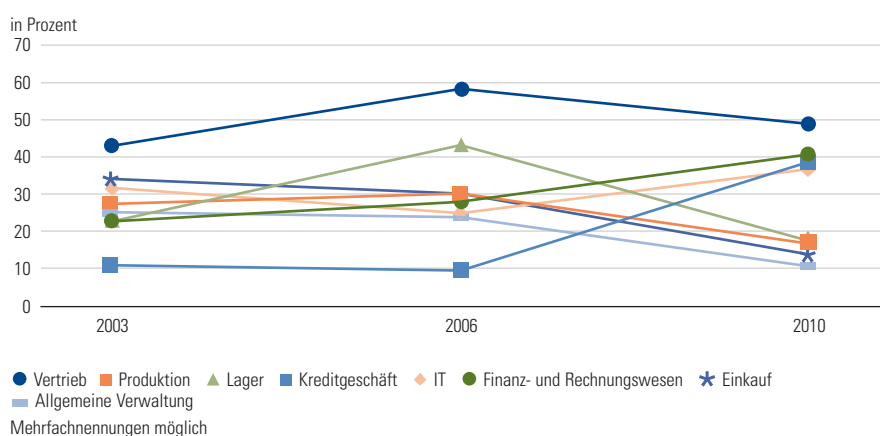
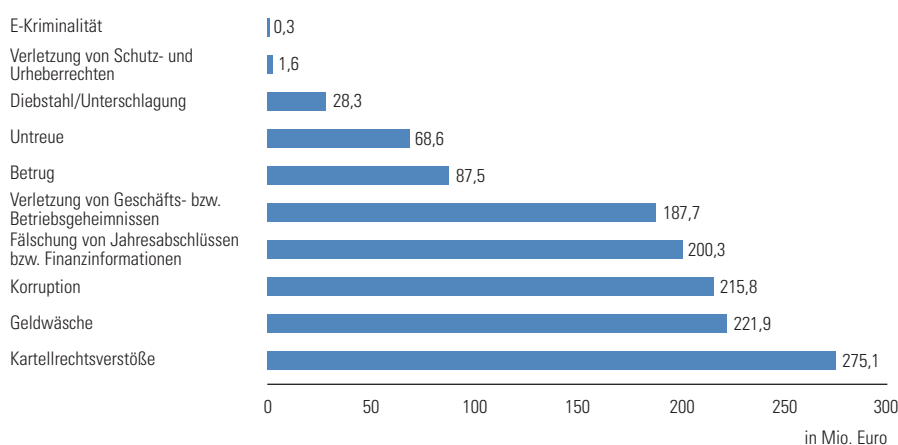


Abb. 7: Durchschnittliche Schäden durch die verschiedenen Delikttypen



**Auch wenn Kartellrechtsverstöße, Geldwäsche, Korruption und Jahresabschlussfälschung vergleichsweise selten auftreten, sind diese Formen der Wirtschaftskriminalität aufgrund ihres hohen Schadenspotenzials besonders riskant.**

Von einer Betrachtung der reinen Auftrittshäufigkeit kann nicht auf die Bedeutung der unterschiedlichen Arten der Wirtschaftskriminalität für Unternehmen geschlossen werden.

Auf jeweils durchschnittlich über 200 Millionen Euro schätzen die jeweils betroffenen Unternehmen den ihnen in den letzten drei Jahren entstandenen Schaden durch Kartellrechtsverstöße, Geldwäsche, Korruption und die Fälschung von Jahresabschlüssen beziehungsweise Finanzinformationen. Das mit diesen vergleichsweise selten auftretenden Arten wirtschaftskrimineller Handlungen verbundene Risiko ist somit beachtlich. Dies muss bei der Gestaltung von Präventions- und Kontrollmaßnahmen beachtet werden.

Neben unmittelbaren finanziellen Schäden stellen Reputationsschäden ein sehr großes Risiko dar. Die mediale Berichterstattung über aktuelle Fälle ist gut im Gedächtnis. Von den befragten Unternehmen schätzt allerdings nur circa ein Viertel (24 Prozent) das sich aus Reputationsschäden ergebende Risiko als hoch oder sehr hoch ein, knapp die Hälfte (48 Prozent) hält es für niedrig oder sehr niedrig. Bei einer genaueren Analyse der Ergebnisse zeigt sich, dass Unternehmen, die in der Vergangenheit

von wirtschaftskriminellen Handlungen betroffen waren, eine deutlich höhere Risikosensibilität in Bezug auf Reputationsschäden haben: Während 55 Prozent der nicht betroffenen Unternehmen das Reputationsrisiko für niedrig oder sehr niedrig halten, teilen diese Einschätzung nur 38 Prozent der betroffenen Unternehmen. Dieses Ergebnis legt nahe, dass die bisher nicht betroffenen Unternehmen das Reputationsrisiko im Allgemeinen unterschätzen.

Die tatsächlich hohe Bedeutung des Reputationsrisikos wird auch durch die Umfragen von Transparency International gestützt (vgl. Global Corruption Barometer 2009). Diese ergaben, dass die Hälfte der Befragten mehr Geld ausgeben würde, um von einem „ehrlichen“ („corruption-free“) Unternehmen zu kaufen. Die Aussage der Kunden ist eindeutig.

# Aufdeckung – Kommissar Zufall hilft

Die Aufdeckung wirtschaftskrimineller Handlungen muss von oberster Priorität sein, denn ohne ein möglichst hohes Aufdeckungsrisiko für die Beteiligten sowie eine adäquate Sanktionsstruktur ist eine effektive Präventionsarbeit kaum darstellbar. Auch ermöglicht die Analyse begangener Straftaten die Verbesserung des internen Kontrollsystems.

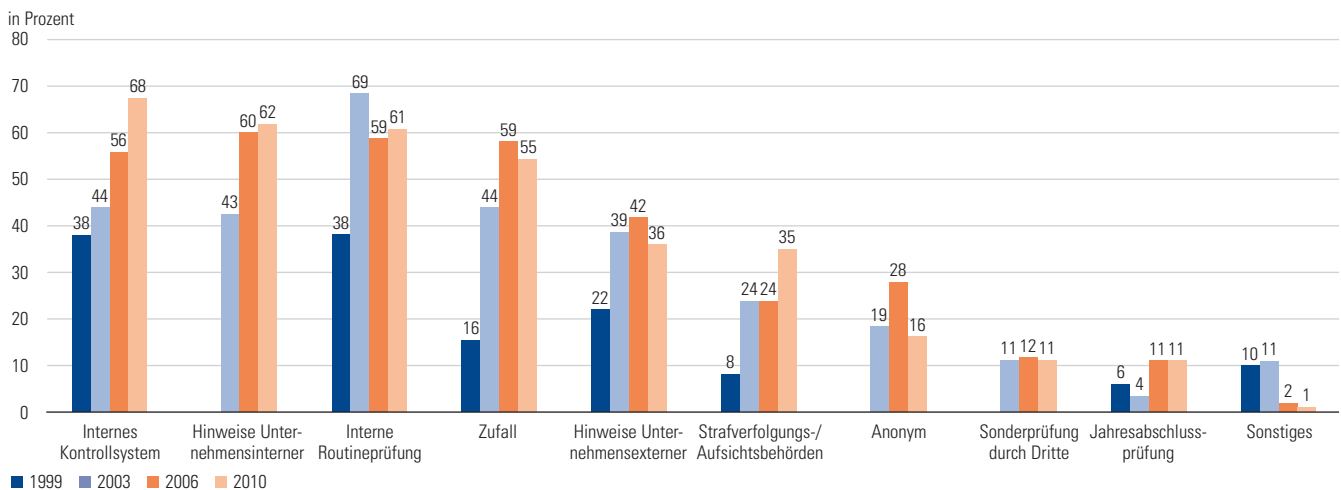
**Wirtschaftskriminalität wird in erster Linie über interne Kontroll- und Hinweisgeber-systeme aufgedeckt, aber auch der „Kommissar Zufall“ spielt weiterhin eine bedenklich große Rolle.**

Um die Effektivität der Aufdeckungsstrukturen zu beurteilen, sind die Kanäle, über die Unternehmen von wirtschaftskriminellen Handlungen erfahren, von großem Interesse. Die Umfrageergebnisse zeigen, dass unternehmens-

interne Hinweise aus dem internen Kontrollsystem (68 Prozent) sowie aus internen Routineprüfungen (61 Prozent) die wesentlichen Quellen von Hinweisen auf wirtschaftskriminelle Handlungen sind. Von großer Bedeutung sind außerdem Hinweise „Unternehmensinterner“, im Englischen „Whistleblower“ genannt (62 Prozent).

Bedenklich ist allerdings, dass „Kommissar Zufall“ weiterhin eine wichtige Rolle im Rahmen der Aufdeckung wirtschaftskrimineller Handlungen spielt (55 Prozent). Die Quote hat sich im Vergleich zu 2006 (59 Prozent) nicht signifikant verringert. Berücksichtigt man zusätzlich die Hinweise durch Unternehmensexterne (36 Prozent) sowie die Aufdeckungen von Strafverfolgungs- und Aufsichtsbehörden (35 Prozent), wird deutlich, dass die Unternehmen bei der systematischen Aufdeckung noch erhebliche Defizite haben.

Abb. 8: Aufdeckung von wirtschaftskriminellen Handlungen\*



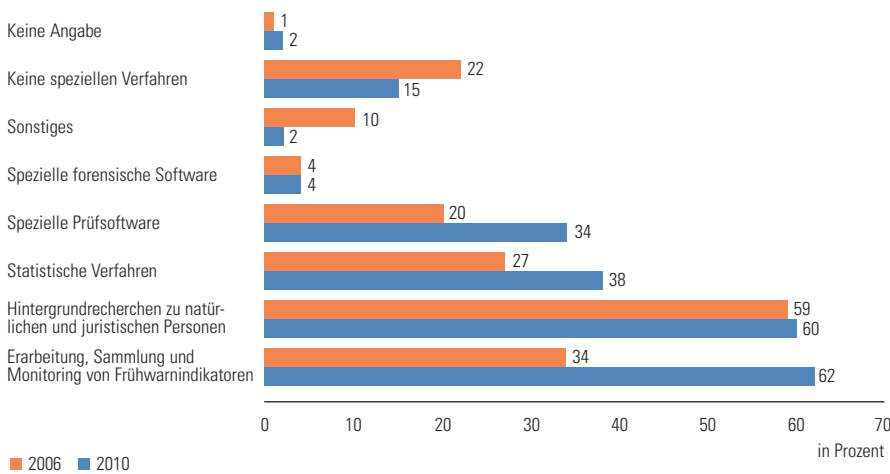
\* Unternehmen, bei denen Wirtschaftskriminalität aufgetreten ist (Mehrfachnennung möglich)

Die Ergebnisse zeigen, dass zwar bei vielen Unternehmen die internen Kontrollmechanismen grundsätzlich gut funktionieren. Jedoch ist die Bedeutung von externen und internen Hinweisgebern, die Informationen besitzen, die sich den Kontrollen und Systemen entziehen, weiterhin essenziell für die Aufdeckung von Wirtschaftskriminalität. Investitionen in Whistleblowing-Systeme sowie Ombudsmänner sind somit von großer Bedeutung.

**Im Rahmen der Aufdeckungsarbeit setzen Unternehmen ein erweitertes Spektrum an Instrumenten ein, IT-gestützte Verfahren werden allerdings nach wie vor zu wenig genutzt.**

Bei der Frage nach den im Rahmen der Aufdeckungsarbeit eingesetzten Verfahren zeigt sich, dass die Unternehmen im Vergleich zu 2006 tendenziell ein breiteres Spektrum an Instrumenten nutzen. Insbesondere Monitoringsysteme unter Einbeziehung von Frühwarnindikatoren („Red Flags“) haben mit einer Nennungshäufigkeit von 62 Prozent deutlich an Bedeutung gewonnen (2006: 34 Prozent). Auch statistische Verfahren sowie spezielle Prüfsoftware sind mit inzwischen 38 Prozent beziehungsweise 34 Prozent (2006: 27 Prozent beziehungsweise 20 Prozent) etablierter Bestandteil des Instrumentariums (vgl. Abb. 9). Bedenkt man jedoch, dass die Durchführung analytischer Prüfungshandlungen bei den heute üblichen Datenmengen meist nur durch den intelligenten Einsatz von spezieller IT-Prüfsoftware möglich ist, muss die Verbreitung dieser Verfahren bisher als zu gering eingestuft werden.

Abb. 9: Eingesetzte Verfahren zur Aufdeckung wirtschaftskrimineller Handlungen



# Reaktion – Professionalisierung in der Aufklärung nötig

**In den letzten drei Jahren haben viele Unternehmen in den Aufbau von internen Aufklärungskapazitäten investiert.**

Bei der Aufklärung wirtschaftskrimineller Handlungen setzen die meisten Unternehmen auf interne Kräfte, wie die Revision oder Task Forces (91 Prozent). Im Vergleich zu 2006 (77 Prozent) lässt sich hieraus ein deutlicher Aufbau interner Kapazitäten ablesen. Untersuchungen durch externe Spezialisten haben dagegen an Bedeutung verloren (2010: 25 Prozent, 2006: 40 Prozent) (vgl. Abb. 10).

Die Bedeutung der Strafverfolgungsbehörden in der Aufklärung wirtschaftskrimineller Handlungen ist im Vergleich zu 2006 in etwa gleich geblieben (2010: 54 Prozent, 2006: 56 Prozent). Dieses Ergebnis überrascht, wenn man die wachsende Bedeutung der Strafverfolgungsbehörden im Rahmen der Aufdeckung wirtschaftskrimineller Handlungen bedenkt (2010: 35 Prozent, 2006: 24 Prozent; siehe Kapitel „Aufdeckung“ ab S. 11).

**„In der Praxis hat sich gezeigt, dass eine frühzeitige Anzeige an die Staatsanwaltschaft nicht immer erfolgversprechend ist – zur Aufnahme von Ermittlungen erwarten die Behörden oftmals, dass das Unternehmen schon eigene Erkenntnisse vorlegen kann.“**

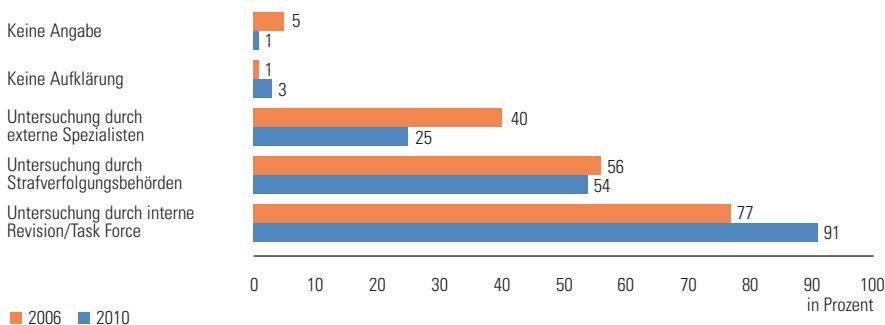
Hauke Hintze, KPMG  
Rechtsanwaltsgesellschaft mbH

Die Tatsache, dass Unternehmen im Rahmen der Aufklärung immer mehr auf die Kapazitäten der Strafverfolgungsbehörden zurückgreifen, zeigt zudem, dass Unternehmen zum Teil einen proaktiven Umgang mit den Behörden pflegen. Die Behörden werden nicht nur als „Gegner“ gesehen, sondern im Rahmen der Aufklärung als Kooperationspartner gesucht. Dies ist grundsätzlich eine erfreuliche Entwicklung, doch muss an dieser Stelle auf die starke Belastung der behördlichen Stellen hingewiesen werden. Auch wenn Unternehmen weiterhin die Kooperation suchen sollten, ist es nicht empfehlenswert, den Aufbau interner Ressourcen zu vernachlässigen.

**Unternehmen beurteilen ihre Erstreaktion auf wirtschaftskriminelle Handlungen zunehmend selbstkritisch. Besonders die Beweissicherung wird als Schwachstelle gesehen.**

Von den 170 von Wirtschaftskriminalität betroffenen Unternehmen dieser Umfrage vermutet ein Drittel der Unternehmen Versäumnisse bei der Erstreaktion (32 Prozent). Im Vergleich zu 2006 (unter 20 Prozent) ist dies ein signifikanter Anstieg. Als Schwachstelle wird derzeit dabei in erster Linie die Beweissicherung (2010: 45 Prozent, 2006: 28 Prozent) gesehen (vgl. Abb. 11). Auch bei der unverzüglichen Information der verantwortlichen Stellen sehen viele Umfrageteilnehmer Versäumnisse (44 Prozent). Unternehmen scheinen folglich zwar verstärkt interne Kapazitäten aufgebaut zu haben (siehe Abb. 10), ihnen fehlt es aber an Fachwissen beziehungsweise Notfallreaktionsplänen

Abb. 10: Aufklärung der wirtschaftskriminellen Handlungen in Unternehmen



im Rahmen der Beweissicherung sowie der Krisenkommunikation mit internen und externen Stellen.

**Immer mehr Unternehmen erkennen die Bedeutung eines Notfallmanagements, die Strukturen sind aber weiterhin defizitär.**

Die Ergebnisse zeigen, dass viele Unternehmen ihre Reaktion auf wirtschaftskriminelle Handlungen zu positiv bewerten: Während zwei Drittel der Unternehmen, bei denen Wirtschaftskriminalität aufgetreten ist, angeben, immer zeitnah und angemessen auf wirtschaftskriminelle Handlungen reagiert zu haben, offenbarten sich gleich-

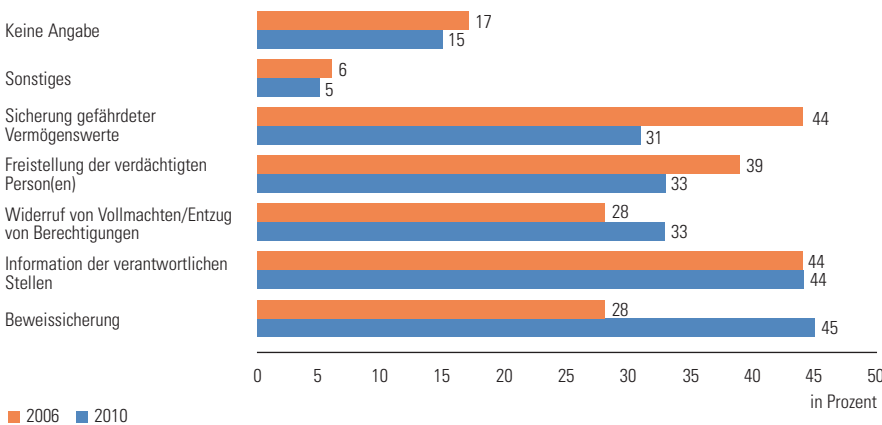
zeitig weit verbreitete Defizite im Bereich des Notfallmanagements.

Dabei zeigt sich im Vergleich zu 2006, dass immer mehr Unternehmen die Bedeutung eines Notfallmanagements erkannt haben. So gaben 2006 nur gut 30 Prozent der kleinen und mittelständischen Unternehmen (bis 500 Millionen Euro Jahresumsatz) und 55 Prozent der Großunternehmen (mehr als 500 Millionen Euro Jahresumsatz) an, Ad-hoc-Maßnahmen im Vorfeld definiert zu haben. Im Jahr 2010 verfügten 46 Prozent der familien- und inhabergeführten Unternehmen und fast 70 Prozent der restlichen befragten Unternehmen über derartige Strukturen.

Beim Notfallmanagement zeigen diese Ergebnisse aber trotz der Verbesserungen erhebliche Versäumnisse. Besonders kritisch: Nur die Hälfte der Unternehmen verfügt über ein ausgebildetes Krisenmanagementteam. Spezielle Schulungen und Krisensimulationen zur Fortbildung erhält davon nur ein Drittel der Teams.

Um Reputationsschäden zu vermeiden, ist dabei auch die Erarbeitung eines externen und internen Kommunikationskonzepts für Krisensituationen von herausragender Bedeutung. Die Ergebnisse zeigen, dass besonders die externe Kommunikation bei vielen Unternehmen nicht ausreichend vorbereitet wird.

Abb. 11: Versäumnisse bei der Erstreaktion auf wirtschaftskriminelle Handlungen



So gaben 35 Prozent der Unternehmen, die über ein Notfallmanagement verfügen, an, keine Abläufe für die externe Kommunikation definiert zu haben. Der Umgang mit Verdachtsfällen und die Reaktion auf konkrete Fälle hat demnach teilweise noch erhebliches Verbesserungspotenzial.

### Fast alle Unternehmen sanktionieren Wirtschaftskriminalität, zivilrechtliche und strafrechtliche Konsequenzen werden aber nur von der Hälfte der Unternehmen gezogen.

Ein wichtiger Faktor im Rahmen der Präventionsarbeit ist neben der Erhöhung der Aufdeckungswahrscheinlichkeit die konsequente und hierarchieunabhängige Sanktionierung wirtschaftskrimi-

neller Handlungen. So ist festzustellen, dass die überwiegende Mehrheit der betroffenen Unternehmen Sanktionen vorgenommen hat (vgl. Abb. 12). Dabei sind weiterhin arbeitsrechtliche Konsequenzen die weitaus am häufigsten ergriffene Maßnahme, wobei im Vergleich zu 2006 ein leichter Rückgang zu verzeichnen ist. Die Bedeutung zivilrechtlicher und strafrechtlicher Konsequenzen ist mit gut 50 Prozent weitestgehend unverändert. Wie schon 2006 lässt sich feststellen, dass im Sinne einer gesellschaftlichen Generalprävention gegen wirtschaftskriminelle Handlungen strafrechtliche Maßnahmen häufiger erwogen werden sollten. Die Botschaft muss klar sein: Wirtschaftskriminalität lohnt sich nicht!

### Die meisten Unternehmen nehmen wirtschaftskriminelle Fälle zum Anlass, Verbesserungen der Präventions- und Kontrollstrukturen durchzuführen. Die Defizite in diesen Bereichen zeigen aber, dass die Erkenntnisse nicht konsequent umgesetzt werden.

Ein weiterer Aspekt im Nachgang zu der Aufklärung einer Tat ist – im Sinne einer „lernenden Organisation“ – die Optimierung der Präventionsstrukturen. Dabei ist die Aufnahme bekannt gewordener Fälle essenziell

Abb. 12: Ergriffene Sanktionen

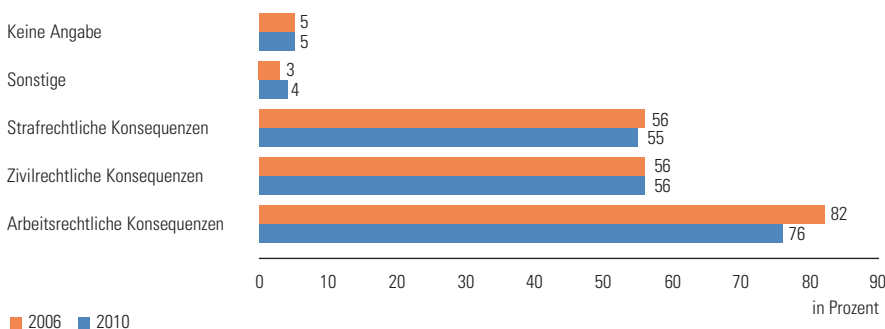
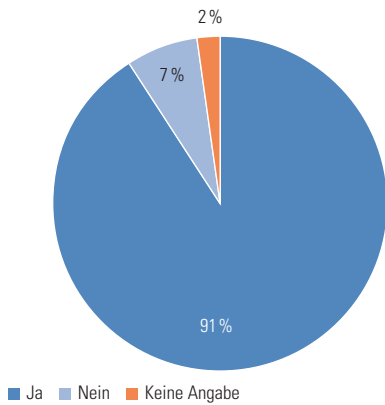


Abb. 13: Analyse entdeckter wirtschaftskrimineller Handlungen



für die Erkennung und Behandlung von wirtschaftskriminellen Handlungsmustern. Erfreulich ist daher, dass 84 Prozent der betroffenen Unternehmen bekannt gewordene Fälle bereits zentral und systematisch erfassen (Fraud Reporting).

Neben der zentralen und systematischen Erfassung ist die Ursachenforschung für die Verbesserung der Organisation essenziell. 91 Prozent der Unternehmen, bei denen Wirtschaftskriminalität aufgetreten war, gaben an, wirtschaftskriminelle Handlungen hinsichtlich der Ursachen sowie der Frühwarnindikatoren zu analysieren (vgl. Abb. 13).

Die große Anzahl der Unternehmen, die wirtschaftskriminelle Handlungen systematisch erfassen und die Ursachen analysieren, scheint im Sinne einer lernenden Organisation darauf hinzudeuten, dass die Unternehmen auch hinsichtlich ihrer Kontroll- und Präventionssysteme gut gegen Wirtschaftskriminalität gerüstet sind. Die Erfahrung lehrt aber, dass dies nicht unbedingt der Fall ist. Offensichtlich lassen viele Unternehmen die sich aus der Ursachenforschung ergebenden Verbesserungspotenziale ungenutzt.



# Vermeidung – Überschätzung der etablierten Kontrollmechanismen

**„Compliance Management ist mehr als Korruptionsbekämpfung und unternehmensinterne Wettbewerbsaufsicht. Compliance Management bedeutet vor allem Vorbeugung.“**

Frank M. Hülsberg, KPMG AG  
Wirtschaftsprüfungsgesellschaft

## Die meisten Unternehmen haben ihre Präventionssysteme in den letzten drei Jahren verbessert.

Unternehmen werden in Bezug auf die Wirksamkeit ihrer eigenen Präventionsmaßnahmen gegen Wirtschaftskriminalität immer selbstbewusster. So empfand 2010 weniger als ein Fünftel der Unternehmen ihre Präventionsmaßnahmen als defizitär (Abb. 14).

Die Investitionen in Präventionsmaßnahmen können als Reaktion auf die hohe Bedeutung gewertet werden, die dem Faktor „Gelegenheit“ als begünstigendem Element von Wirtschaftskriminalität zugemessen wird. „Gelegenheit“ wird durch unzureichende Organisation und ineffiziente Kontrollsysteme geschaffen (Abb. 15).

Neben „Gelegenheit“ fördern die Faktoren „Motivation“ und „Rechtfertigung“ wirtschaftskriminelle Handlungen. Diese drei Faktoren bilden das sogenannte „Fraud Triangle“ oder auch Kriminalitätsrisikomodell, das bereits in den 1940er-Jahren in den USA entwickelt wurde und weiterhin im Rahmen der Systematisierung krimineller Ursachen hilfreich ist. Nach diesem Modell tritt Wirtschaftskriminalität dann auf, wenn alle drei Faktoren gleichzeitig erfüllt sind. Es muss also eine Gelegenheit zur Tat geben, der Täter muss eine Motivation für die Tat haben und er muss die Tat im Nachgang vor sich selbst rechtfertigen können, das heißt das schlechte Gewissen neutralisieren.

Die Umfrageergebnisse zeigen deutlich, dass die meisten Unternehmen ihre

Präventionssysteme in den letzten drei Jahren erheblich verbessert haben. Die Überarbeitung von Berechtigungskonzepten sowie von Richtlinien und Verfahrensanweisungen, die Verbesserung der internen Kontrollen und die Beauftragung von Verantwortlichen spielen eine große Rolle. Auch das Thema „Compliance“ ist auf der Agenda deutlich nach oben gerückt: 74 Prozent der Unternehmen gaben an, eine Compliance-Funktion eingerichtet zu haben (vgl. Abb. 16).

Das große Selbstbewusstsein der befragten Unternehmen in Bezug auf ihr Präventionssystem steht teilweise im Kontrast zu den weiteren Ergebnissen.

## Der hohe Anteil von Einzeltätern und die damit vergleichsweise geringe Bedeutung von Absprachen zwischen Mitarbeitern deuten auf signifikante Defizite hinsichtlich der Funktionstrennung und des Vieraugenprinzips hin.

Zwar gaben 85 Prozent der Unternehmen an, ihr Kontrollsystem verbessert zu haben, tatsächlich zeigen die Umfrageergebnisse aber weiterhin signifikante Defizite. Besonders deutlich wird dies bei der Frage, inwieweit es im Rahmen wirtschaftskrimineller Aktivitäten zu Absprachen zwischen Mitarbeitern kam. So gaben 71 Prozent der Unternehmen (die in den letzten drei Jahren betroffen waren) an, dass es in keinem Fall zu Absprachen zwischen Mitarbeitern kam. Wirtschaftskriminelle Handlungen von Einzeltätern deuten darauf hin, dass grundlegende Kontrollprin-

Abb. 14: Ausreichende Präventionsmaßnahmen

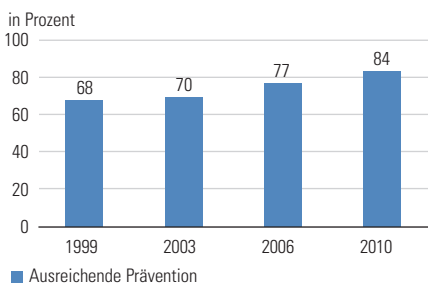
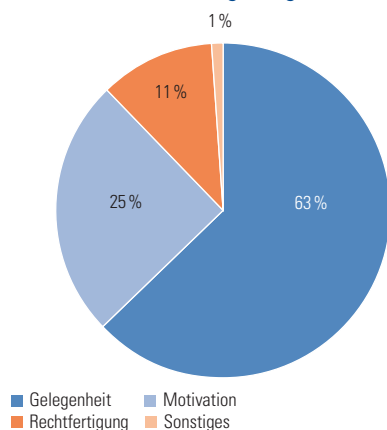


Abb. 15: Umstände, die Wirtschaftskriminalität begünstigen



zipien, wie Funktionstrennung oder das Vieraugenprinzip, verletzt wurden, da ansonsten immer mehrere Personen in eine kriminelle Handlung involviert sein müssten.

### Immaterielle Vermögensgegenstände werden bei der Risikoanalyse und im Präventionssystem vernachlässigt.

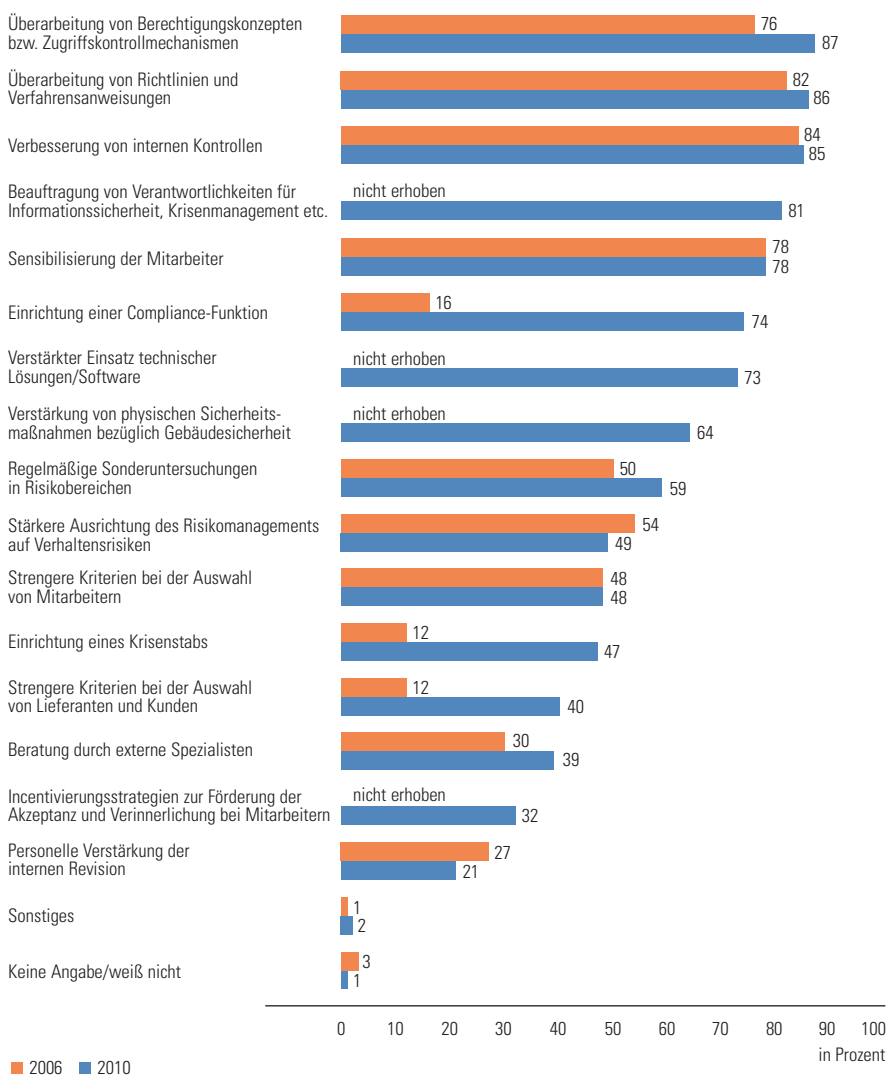
Ausgangspunkt einer zielgerichteten Prävention muss immer die strukturierte Erfassung und Analyse des eigenen Risikos sein. Insofern ist es erfreulich, dass die Mehrheit der Unternehmen dies umsetzen: Zwei Drittel (67 Prozent) der Umfrageteilnehmer gaben an, eine systematische Risikoerfassung und -bewertung durchzuführen.

Die Umfrageergebnisse zeigen aber auch deutlich, dass im Fokus dieser Maßnahmen physische Werte stehen. Nur circa ein Drittel aller befragten Unternehmen gab an, die Risiken für intellektuelles Eigentum zu analysieren. Dies zeigt, dass der Schutz physischer Werte als selbstverständlich erachtet wird, während immaterielle Vermögensgegenstände vernachlässigt werden (vgl. Abb. 17).

Dieses Ergebnis deckt sich damit, dass nur 25 Prozent der Unternehmen technische Schwachstellen als große Bedrohung für ihr Unternehmen empfinden. Auch schätzt über die Hälfte der Umfrageteilnehmer die Wahrscheinlichkeit eines Verstoßes gegen den Informationsschutz als niedrig ein.

Mit der seit Jahren wachsenden Bedeutung immaterieller Vermögensgegenstände für den Unternehmenserfolg und den gleichzeitig steigenden Möglichkeiten der Industriespionage haben

Abb. 16: Ergriffene Maßnahmen zur Risikominimierung



viele Unternehmen an dieser Stelle eine gefährlich offene Flanke: Der Schaden durch die Verletzung von Geschäfts- oder Betriebsgeheimnissen belastet Unternehmen im Durchschnitt in dreistelliger Millionenhöhe. Diese Ergebnisse decken sich mit den Ergebnissen einer aktuellen Studie der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW). Danach haben 74 Prozent der Firmen schützenswertes Know-how, lediglich 32 Prozent verfügen jedoch über ein Konzept zu dessen Schutz.

Alarmierend ist daher, dass nur die Hälfte der befragten Unternehmen in den letzten drei Jahren verstärkt Maßnahmen zur Verhinderung des Verlustes von sensiblen Informationen ergriffen hat. Nur 43 Prozent der Umfrageteilnehmer verfügen über ein Schutzkonzept für vertrauliche Unterlagen.

**Obwohl sich die Unternehmen der Bedeutung sensibilisierter Mitarbeiter im Rahmen der Präventionsarbeit bewusst sind, werden langfristige Maßnahmen zum Wissensaufbau sowie die gezielte Auswahl von Mitarbeitern vernachlässigt.**

Gut zwei Drittel der Umfrageteilnehmer glauben, dass durch eine erhöhte beziehungsweise verbesserte Sensibilität der Mitarbeiter für das Thema Wirtschaftskriminalität eine Verhinderung wirtschaftskrimineller Handlungen möglich ist. So ist die Verbreitung von Verhaltenskodizes seit 2006 sprunghaft angestiegen und liegt jetzt bei 81 Prozent (vgl. Abb. 18). Fast alle dieser Unternehmen (90 Prozent) gaben des Weiteren an, dass die relevanten Mitarbeiter diese Verhaltensgrundsätze erhalten hätten und zur Einhaltung verpflichtet wurden.

Abb. 17: Systematische Erfassung und Bewertung des Risikos für ...

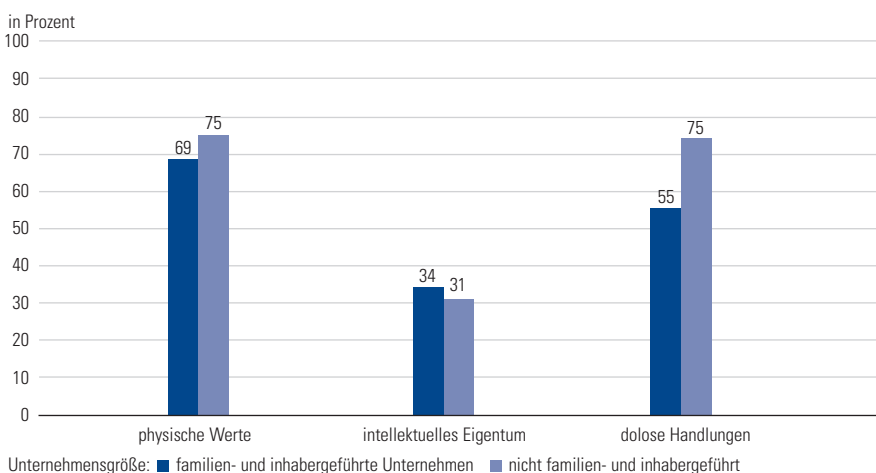
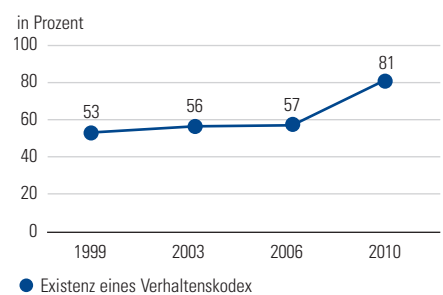


Abb. 18: Existenz eines Verhaltenskodex



**„Compliance ist daher primär eine Haltung, die es bei jedem Einzelnen im Unternehmen auszuprägen gilt. Sie entsteht aus dem Bewusstsein, was rechtens und was legitim ist, und lebt von der klaren Vorgabe der Führung, dass Erfolg in diesem Unternehmen nur das ist, was mit integren Mitteln auf eine integre Art und Weise erzielt wird. Ein wirksames Compliance Management setzt bei diesen Parametern an und ist damit Werte- und Risikomanagement zugleich.“**

Dr. Annette Kleinfeld  
Geschäftsführung Dr. Kleinfeld CEC  
GmbH & Co. KG  
Corporate Excellence Consultancy

Doch auch wenn Selbstverpflichtung und Verhaltenskodex wichtige erste Schritte sind, reichen sie nicht aus, um Mitarbeiter langfristig für kritische Fragestellungen zu sensibilisieren. Nur ein kontinuierlicher Wissensaufbau sowie eine Operationalisierung von grundsätzlichen Verpflichtungen werden langfristig zu einer Vermeidung beziehungsweise signifikanten Verringerung wirtschaftskrimineller Aktivitäten führen. Jedoch boten nur 33 Prozent der betroffenen Unternehmen Ethiktrainings beziehungsweise -schulungen an. Auch haben nur 36 Prozent dieser Unternehmen Integritätskriterien in die Zielvereinbarung von Führungskräften aufgenommen. Des Weiteren lassen sich nur etwa 30 Prozent der Unternehmen den Erhalt der Grundsätze schriftlich bestätigen – eine notwendige Maßnahme, um die Compliance-Anstrengungen entsprechend zu dokumentieren.

Unternehmen waren Mitarbeiter oder Management, also Unternehmensinterne, in die Straftaten involviert. Auch schätzen 69 Prozent der Befragten die Bedrohung durch eigene Mitarbeiter als mittel bis hoch ein. Trotz der hohen potenziellen Gefahr aus den eigenen Reihen und des in den meisten Unternehmen gut ausgeprägten Bewusstseins der notwendigen Sensibilisierung, wird neben der Schulung auch die Personalauswahl vernachlässigt. So setzt mit 48 Prozent nicht einmal die Hälfte der Unternehmen auf eine strenge Mitarbeiterauswahl, was der eigenen Bedrohungseinschätzung entgegenläuft.

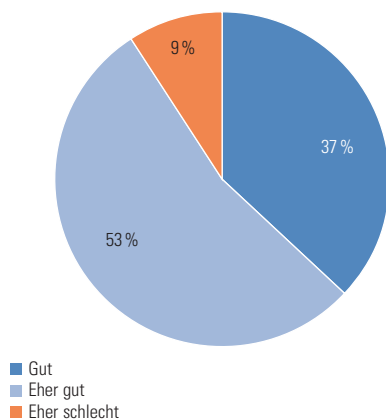
### Überraschend viele Unternehmen sehen sich im Spagat zwischen Datenschutz und Kontrolle gut aufgestellt.

Dabei ist sich der größte Teil der Befragten der mit diesen Defiziten verbundenen Risiken durchaus bewusst: 74 Prozent der Unternehmen gaben an, dass gesetzliche und moralische Standards häufig deshalb verletzt würden, weil Verhaltensgrundsätze beziehungsweise Richtlinien nicht ernst genug genommen werden. Damit muss die Frage aufgeworfen werden, ob für viele Unternehmen die Einhaltung ethischer Standards nicht eher ein Lippenbekenntnis als ein tatsächlich angestrebtes Ziel ist.

Alle Maßnahmen zur Prävention von wirtschaftskriminellen Aktivitäten können aber auch Gefahren bergen. So werden Mitarbeiter, aber auch Aufsichtsgremien oder Externe (wie zum Beispiel Journalisten) zum Opfer der Prävention, wenn Überwachungsmaßnahmen sich außerhalb des gesetzlichen Rahmens, zum Beispiel des Bundesdatenschutz- oder Telekommunikationsgesetzes, bewegen. Dieses Spannungsfeld ist seit den jüngsten Datenskandalen im öffentlichen Bewusstsein sehr präsent. In Anbetracht dieser Fälle ist es überraschend, dass 90 Prozent der befragten Unternehmen die von ihnen durchgeführte systematische Vorabprüfung zur Einhaltung gesetzlicher Anforderungen

Ob Untreue, Diebstahl, Korruption oder die Verletzung von Geschäfts- oder Betriebsgeheimnissen, in den meisten

Abb. 19: Systematische Vorabprüfung gesetzlicher Anforderungen



**„Die zunehmende Berichterstattung über Datenschutzverstöße durch einige prominente Unternehmen hat das Thema Datenschutz verstärkt in das öffentliche Interesse gerückt. Die aktuellen Fälle zeigen: Unternehmen müssen die Konzeption und Umsetzung unternehmensweiter Compliance- und Datenschutz-Management-Prozesse klar an den Anforderungen des Datenschutz- und Betriebsverfassungsgesetzes ausrichten.“**

Frank M. Hülsberg, KPMG AG  
Wirtschaftsprüfungsgesellschaft

als gut beziehungsweise eher gut einschätzen (vgl. Abb. 19). Offensichtlich haben viele Unternehmen die sich aus dem Spannungsfeld „Kontrolle und Aufklärung versus Datenschutz“ ergebenden Gefahren noch nicht erkannt.

### Nur wenige Unternehmen bemühen sich um die Compliance in der gesamten Lieferkette.

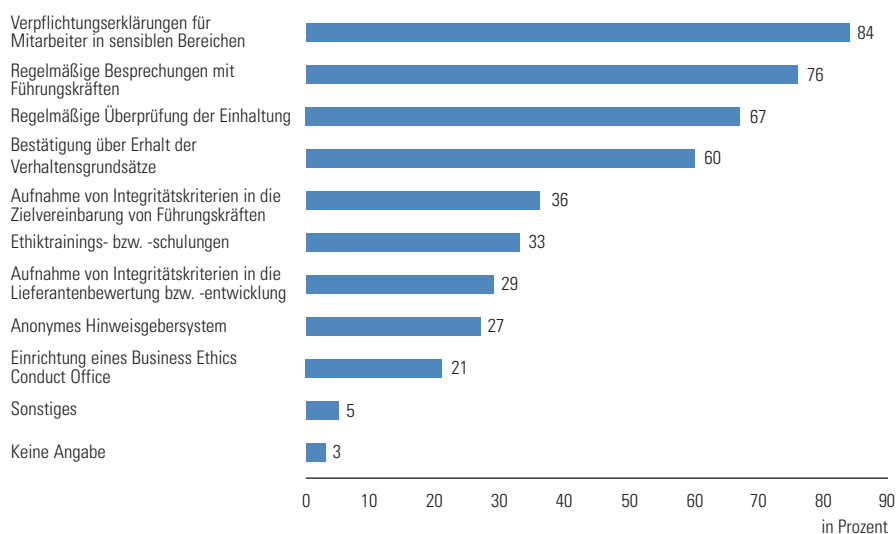
Unternehmen sind in ihren wirtschaftlichen Aktivitäten nicht auf sich gestellt, sondern in der Regel in eine Lieferantenkette eingebunden. Wirtschaftskriminelle Handlungen innerhalb dieser Lieferantenkette sind häufig mit einem Risiko für das eigene Unternehmen verbunden. Besticht zum Beispiel ein Subunternehmer eine Regierung, um einen Bauauftrag zu erhalten, kann dieses Vergehen durchaus mit dem Auftraggeber in Verbindung gebracht werden. Die

Compliance-Bemühungen dürfen sich daher nicht auf das eigene Unternehmen beschränken, sondern sollten die gesamte Lieferkette mit einbeziehen.

Insbesondere auch angesichts der Reichweite des Foreign Corrupt Practices Act (FCPA) und der vor diesem Hintergrund bekannt gewordenen Beispiele mit Strafzahlungen teilweise in mehrstelliger Millionenhöhe erscheint die Vernachlässigung dieser Aspekte nahezu fahrlässig.

Trotzdem zeigen die Umfrageergebnisse hier bei dem größten Teil der Unternehmen signifikante Defizite. So gaben lediglich 29 Prozent der Befragten an, Integritätskriterien in die Lieferantebewertung aufzunehmen. Auch führt mit 56 Prozent über die Hälfte der Unternehmen keine Analysen wirtschaftskrimineller Handlungen von verbundenen Unternehmen und Dienstleistern durch.

Abb. 20: Verbreitung von Integritätskriterien



# Fokus Mittelstand – Paradigmenwechsel gefordert

Wer die mediale Berichterstattung zum Thema Wirtschaftskriminalität verfolgt, könnte zu dem Schluss kommen, dass Wirtschaftskriminalität vor allem Großunternehmen betrifft. Ob Korruption oder Datenmissbrauch, bisher machten Konzerne mit solchen spektakulären Verfahren die negativen Schlagzeilen.

Dies bedeutet aber nicht, dass Wirtschaftskriminalität nicht auch den Mittelstand betrifft. Im Gegenteil: Der Mittelstand ist mit seiner Innovationskraft ein bedeutender Wirtschaftsmotor Deutschlands – und das bietet Angriffsfläche: Immer wieder sind es kleine und mittelgroße Unternehmen über alle Branchen hinweg, die dank hervorragendem Know-how ganze Industriezweige mit neuen Technologien revolutionieren. Damit sind sie eine attraktive Zielscheibe.

Gleichzeitig setzen viele kleine und mittelgroße Unternehmen auf das Prinzip Vertrauen und fürchten den mit starren Kontrollen verbundenen Bürokratismus. Dies ist nur allzu verständlich, denn insbesondere ihre Flexibilität ist für mittelständische Unternehmen häufig ein wesentlicher Erfolgsfaktor. Jedoch machen sie sich damit angreifbar, denn die Erfahrung zeigt, dass Vertrauen oft ausgenutzt wird.

## Mittelstandsdefinition

Aus diesem Grund wollten wir in der diesjährigen Studie gezielt den deutschen Mittelstand zu seinem Umgang mit dem Thema Wirtschaftskriminalität befragen. Eine Analyse der im Mittelstand etablierten Präventions-, Kontroll- und Aufklärungsmaßnahmen ist jedoch nur auf der Basis einer Abgrenzung dieser Unternehmensgruppe möglich. Diese Trennlinie ist nicht immer eindeu-

tig, denn ein großer Teil der sogenannten mittelständischen Unternehmen produziert und vermarktet seine Produkte weltweit und nutzt die gleichen komplexen Finanzierungsstrukturen wie Großkonzerne. Wer derart exponiert agiert, kann nicht alleine aufgrund von Kennzahlen kategorisiert werden.

Aus diesem Grund wird im Rahmen dieser Studie die Abgrenzung auf der Basis der Eigentümer- und Führungsstruktur vorgenommen. Als Mittelstand wird definiert, wer inhaber- oder familiengeführt ist. Trotz der großen Vielfalt dieser Unternehmen bedingt die Einheit aus Führung und Eigentum nach unserer Erfahrung eine spezielle Führungskultur. So unterschiedlich die Geschäftsaktivitäten der in dieser Gruppe untersuchten Unternehmen sind, in Bezug auf die Ausgestaltung von Präventions-, Kontroll- und Aufklärungsmaßnahmen weisen sie eine hohe Homogenität aus. Von den 300 in die Studie einbezogenen Unternehmen waren 127 inhaber- oder familiengeführt.

## Viele mittelständische Unternehmen glauben weiterhin, dass sie weniger gefährdet sind als Großunternehmen.

„Wirtschaftskriminalität? Das ist was für die Großen!“ Unsere Umfrage zeigt, dass dies weiterhin über die Hälfte der mittelständischen Unternehmen denkt: 56 Prozent der Umfrageteilnehmer vertreten die Meinung, dass ihr eigenes Unternehmen weniger gefährdet ist als ein Großunternehmen. Besonders signifikant ist der Unterschied bei der Einschätzung von möglichen Reputationsschäden: Nur 14 Prozent der mittelständischen Unternehmer sehen dies als eine Gefahr für

ihr Unternehmen, unter Großunternehmen liegt die Quote bei 32 Prozent.

Diese Einschätzung lässt sich mit dem bereits erwähnten Fokus der Medien auf Wirtschaftskriminalität bei Großunternehmen erklären. Angesichts der insgesamt gestiegenen öffentlichen Wahrnehmung sowie der medialen Berichterstattung ist aber absehbar, dass sich dies ändern wird. Selbst wenn ein mittelständisches Unternehmen nicht mit einem Korruptionsskandal auf der Titelseite der nationalen Tageszeitungen Schlagzeilen macht, eine Schädigung der Reputation kann auch im kleinen Kreis auf Branchen- oder regionaler Ebene, zum Beispiel unter Lieferanten und Kunden, große Risiken bergen.

## Viele mittelständische Unternehmen überschätzen ihre eigenen Fähigkeiten und Kenntnisse über wirtschaftskriminelles Handeln.

59 Prozent der mittelständischen Unternehmen bewerten ihre eigenen Fähigkeiten und Kenntnisse bezüglich wirtschaftskrimineller Handlungen als gut beziehungsweise eher gut. Außerdem halten 76 Prozent von ihnen die implementierten Präventionsmaßnahmen für ausreichend. Die Einschätzung der eigenen Kenntnisse sowie der Präventionsmaßnahmen ist im Vergleich zu Großunternehmen etwas weniger selbstsicher – hier sind es 73 beziehungsweise 90 Prozent. Zieht man aber die tatsächliche Qualität der Aufdeckungs-, Kontroll- und Präventionssysteme in Betracht (siehe unten), offenbaren mittelständische Unternehmen hier eine deutliche Überschätzung der eigenen Kenntnisse und Strukturen.

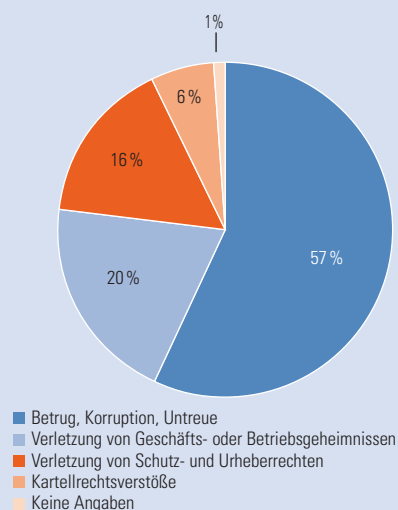
„Klassische Vermögensdelikte“ treten im Mittelstand weiterhin am häufigsten auf.

#### Praxisbeispiel 1: „Vertriebskorruption“

Ein Lagermitarbeiter entwendet einen DVD-Player; der eigentlich einem Kunden zugedachte Rabatt verschwindet in der Tasche des Vertriebsmitarbeiters: Diese „klassischen“ Vermögensdelikte machen bei mittelständischen Unternehmen nach wie vor den größten Teil der wirtschaftskriminellen Handlungen aus. Während die Umfrageergebnisse bei Großunternehmen eine deutliche Verschiebung von Wirtschaftskriminalität in die Unternehmensbereiche Finanz- und Rechnungswesen sowie zum Kreditgeschäft widerspiegeln, stehen bei mittelständischen Unternehmen weiterhin die „klassischen“ Bereiche Lager und Vertrieb im Vordergrund. Delikte wie Diebstahl, Unterschlagung, Untreue und Betrug sind weiterhin die von betroffenen mittelständischen Unternehmen am häufigsten genannten Deliktarten (57 Prozent, vgl. Abb 21).

Quelle: Sichere Geschäfte? Wirtschaftskriminalität – Risiken für mittelständische Unternehmen; Hrsg. BDI/KPMG; 2009

Abb. 21: Größte Bedrohung für Mittelstand aus ...



Die sich aus dem Verlust von immateriellen Vermögensgegenständen ergebenden Risiken werden trotz negativer Erfahrungen weiterhin unterschätzt, die Kontrollmechanismen sind unzureichend.

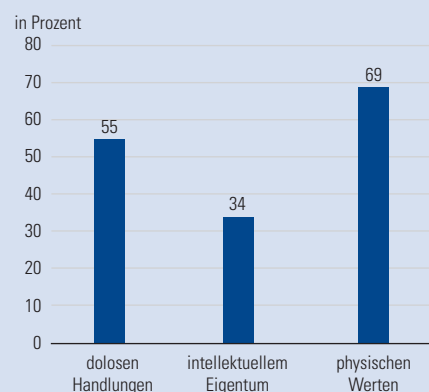
Auch wenn Schäden an materiellen Vermögensgegenständen empfindlich sein können, existenzbedrohend sind sie meist nicht. Ganz anders sieht es bei dem Verlust immaterieller Vermögensgegenstände aus: Der Erfolg vieler deutscher mittelständischer Unternehmen basiert auf dem Erfindergeist ihrer Ingenieure, Chemiker oder Physiker. Oft sind Schlüsseltechnologien die wichtigste Geschäftsgrundlage. Gelangen Formeln oder Rezepturen in die Hände der Konkurrenz, kann dies auch etablierte Traditionsunternehmen ins Straucheln bringen. Gleichzeitig sind die Zeiten vorbei, in denen Konstruktionspläne und Modelle aufgrund ihrer schier physischen Größe schwierig zu entwenden waren. Heute liegt alles digital vor. Selbst die komplexesten Pläne passen auf einen USB-Stick und damit in jede Westentasche.

Deshalb ist es auch nicht erstaunlich, dass die Verletzung von Geschäfts- und Betriebsgeheimnissen inzwischen auch im Mittelstand bei Weitem kein Einzelfall mehr ist. Im Gegenteil: Die Umfrageergebnisse zeigen, dass der Datendiebstahl für mittelständische Unternehmen ein größeres Problem darstellt als für Großunternehmen. So war in den letzten drei Jahren fast ein Drittel von ihnen hiervon betroffen, unter Großunternehmen war es „nur“ ein Fünftel. Trotz dieser negativen Erfahrungen wird die Gefahr des Verlustes immaterieller Werte von mittelständischen Unternehmen weiterhin unterschätzt. So sehen nur 20 beziehungsweise 16 Prozent die Verletzung von Geschäfts- und Betriebsgeheimnissen sowie von Schutz- und

Urheberrechten als größte Bedrohung für deutsche mittelständische Unternehmen (vgl. Abb. 21).

Angesichts dieses mangelnden Problembewusstseins besteht ein immer noch unzureichender Schutz der immateriellen Vermögenswerte. Zwar nannten die mittelständischen Unternehmen die Überarbeitung von Berechtigungskonzepten beziehungsweise Zugriffskontrollmechanismen als am meisten durchgeführte Maßnahme zum Schutz vor Wirtschaftskriminalität (85 Prozent). Diese Einzelmaßnahmen jedoch werden nicht in ein Gesamtkonzept eingebettet, ihre Effektivität ist damit zweifelhaft. So gab nur ein gutes Drittel an, über ein Schutzkonzept für vertrauliche Informationen zu verfügen, bei Großunternehmen hat inzwischen bereits die Hälfte derartige Strukturen implementiert. Auch eine systematische Erfassung und Bewertung des mit dem Verlust von intellektuellem Eigentum verbundenen Risikos wird nur von einem Drittel der befragten mittelständischen Unternehmen durchgeführt. Für physische Werte tun dies fast zwei Drittel der Befragten – Lager und Produktionshallen stehen also trotz geringerer existenzbedrohender Risiken weiterhin im Fokus.

Abb. 22: Systematische Erfassung und Bewertung von ... im Mittelstand



**Praxisbeispiel 2:**

Seit Jahrzehnten arbeitet der Ingenieur bei einem süddeutschen Maschinenbauer. Zahlreiche wichtige Entwicklungen gehen auf das Konto des fleißigen und zuverlässigen Mitarbeiters. „Einer unserer besten Männer“, ist der geschäftsführende Inhaber, Enkelsohn des Unternehmensgründers, überzeugt. Dank des großen Respekts und Vertrauens für seine Arbeit und seine Person hat der Ingenieur weitreichende Zugriffsrechte; Kontrollen gibt es keine. Schon vor Jahren hätte er die Gelegenheit gehabt, Firmeninterna an ausländische Konkurrenten zu verkaufen. Seit dem Markteintritt in China nehmen dubiose Angebote zu. Aber der Mitarbeiter sieht hierfür keinen Anlass, denn seine Bezahlung ist gut und seine Loyalität zur Firma hoch.

Dann erkrankt unerwartet ein Familienmitglied schwer. Die Kosten für Medikamente und Pflege übersteigen die vorhandenen Mittel der Familie. Zeitgleich bekommt der Mitarbeiter auf einer internationalen Messe ein extrem attraktives Angebot für die Weitergabe eines Patentes. Nach einigen schlaflosen Nächten lässt sich der Ingenieur auf den Deal ein, die Konstruktionspläne überreicht er auf einem USB-Stick. Kurz darauf laufen im Fernen Osten die Maschinen an und wenige Monate später hält der Geschäftsführer die Plagiate in der Hand. Die Geschäftsgrundlage des Traditionsunternehmens ist zerstört.

### Mittelständische Unternehmen setzen stark auf das Prinzip Vertrauen, die Kontrollstrukturen sind unausgereift.

Dem Vertrauen kommt als Organisationsprinzip in mittelständischen Unternehmen traditionell eine bedeutende Rolle zu. Denn die mit einem engen Kontroll-

netz oft verbundenen bürokratischen Strukturen hemmen einen der wichtigsten Erfolgsfaktoren deutscher mittelständischer Unternehmen im globalen Wettbewerb: die Flexibilität. Auf der Basis von Vertrauen kann Verantwortung delegiert werden, für Mitarbeiter entstehen Spielräume, die wiederum schnelle und einzelfallbezogene Entscheidungen ermöglichen (siehe Sichere Geschäfte? Wirtschaftskriminalität – Risiken für mittelständische Unternehmen; Hrsg. BDI/KPMG; 2009).

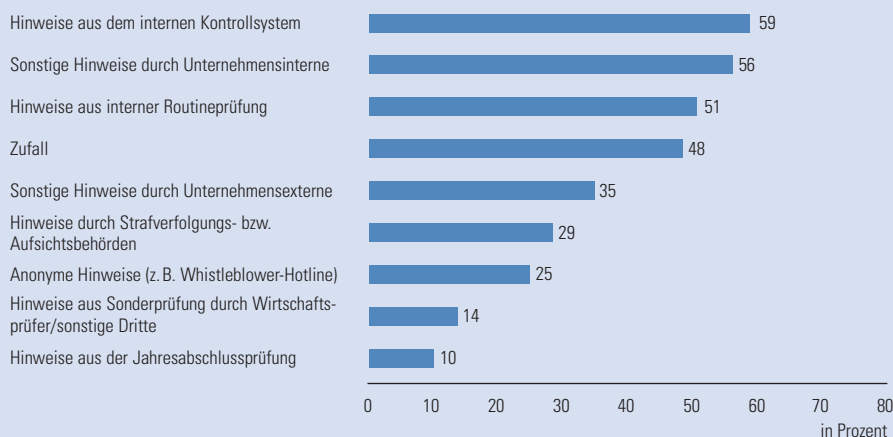
Verbunden mit dem Vertrauensprinzip ist aber zwangsläufig das Risiko, dass Spielräume zum Nachteil des Unternehmens ausgenutzt werden. Für Mitarbeiter entsteht die Gelegenheit zum Vertrauensmissbrauch. Dabei scheinen sich die mittelständischen Unternehmen dieses Risikos durchaus bewusst zu sein: 69 Prozent der mittelständischen Umfrageteilnehmer schätzen die Gelegenheit als wichtigste Ursache für wirtschaftskriminelle Handlungen ein. Auch spielen Absprachen von Mitarbeitern mit Unternehmensexternen im Mittelstand eine deutlich größere Rolle: Während bei Großunternehmen 60 Prozent angaben, dass es in keinem Fall zu derartigen Absprachen gekommen sei, lag diese Quote bei mittelständischen Unternehmen nur bei 38 Prozent. 18 Prozent geben sogar an, dass es in 80 bis 100 Prozent der Fälle von Wirtschaftskriminalität zu Absprachen zwischen Mitarbeitern und Externen kam.

Trotz des offenbar vorhandenen Problembewusstseins setzen mittelständische Unternehmen weiterhin auf das Prinzip Vertrauen: Die Umfrageergebnisse zeigen, dass bei diesen Unternehmen das interne Kontrollsystem vergleichsweise schwach ausgeprägt ist. So haben zwar in etwa gleich viele mittelständische wie große Unternehmen Verpflichtungserklärungen für Mitarbeiter in sensiblen

Bereichen eingeführt, regelmäßig überprüft werden diese aber deutlich seltener. Ähnlich sieht es in der Lieferkette aus: Integritätskriterien für Lieferanten etablierten mit 40 Prozent zwar fast doppelt so viele mittelständische Unternehmen wie Großunternehmen, eine regelmäßige Risikoeinschätzung wirtschaftskrimineller Handlungen durch verbundene Unternehmen und Dienstleister führt aber nicht einmal ein Drittel durch. Auch Verfahren zur Erarbeitung, Sammlung und zum Monitoring von Frühwarnindikatoren oder Hintergrundrecherchen zu natürlichen und juristischen Personen setzt jeweils weniger als die Hälfte der mittelständischen Unternehmen ein.

Bei der Aufdeckung wirtschaftskrimineller Handlungen spielt bei mittelständischen Unternehmen der „Kommissar Zufall“ eine noch bedeutendere Rolle als bei Großunternehmen: Während 74 Prozent der Großunternehmen Hinweise aus dem internen Kontrollsystem als Quelle für die Aufdeckung wirtschaftskrimineller Handlungen nannten, waren es bei mittelständischen Unternehmen nur 59 Prozent. Auch gibt mit 22 Prozent ein durchaus signifikanter Teil der mittelständischen Unternehmen an, keine speziellen Verfahren zur Aufdeckung wirtschaftskrimineller Handlungen einzusetzen, bei Großunternehmen liegt der Anteil unter 10 Prozent. Auffällig ist außerdem, dass anonyme Hinweise (Whistleblowing) und Hinweise aus Sonderprüfungen die einzigen Quellen sind, die im Mittelstand von größerer Bedeutung als bei Großunternehmen sind. Insgesamt kann man festhalten: Zwar hat der Mittelstand durchaus in Instrumente wie Whistleblowing-Hotlines investiert, umfassende systematische Kontroll- und Aufdeckungsmaßnahmen existieren dagegen nicht.

Abb. 23: Wodurch sind Sie erstmals auf begangene wirtschaftskriminelle Handlungen aufmerksam geworden?



## Aufklärung liegt in der Hand interner Ressourcen.

Zur Aufklärung von wirtschaftskriminellen Straftaten greifen nur 15 Prozent der mittelständischen Unternehmen auf externe Kräfte zurück. Dieses Ergebnis deutet darauf hin, dass die mittelständischen Unternehmen stark auf die in den letzten Jahren aufgebauten internen Kräfte setzen. Fraglich ist allerdings, ob diese neuen Kapazitäten die Risiken tatsächlich ausreichend abdecken, denn erfahrungsgemäß gibt es Verbesserungspotenzial an speziellem Fachwissen sowie bei den eingesetzten Ressourcen. Somit muss die Frage aufgeworfen werden, ob sich vor allem mittelständische Unternehmen im Rahmen der Aufklärungsarbeit nicht in einer trügerischen Sicherheit wähnen. Dies könnte unter anderem daran liegen, dass sich die öffentliche Berichterstattung bisher vor allem auf Großunternehmen konzentrierte. Mit der insgesamt gestiegenen öffentlichen Wahrnehmung von Wirtschaftskriminalität dürfte sich dies – selbst wenn selbstverständlich Großunternehmen weiterhin verstärkt im Fokus stehen werden – ändern.

## Der Mittelstand ist schlecht auf eintretende Fälle und Verdachtsmomente vorbereitet.

Hundertprozentige Sicherheit kann aber auch das beste Kontrollsystem nicht bieten, Wirtschaftskriminalität wird niemals ganz ausgeschlossen werden können. Umso wichtiger sind Strukturen, die den Umgang mit kritischen Situationen managen.

Die Umfrageergebnisse zeigen, dass mittelständische Unternehmen hier schlecht aufgestellt sind. So verfügt nicht einmal die Hälfte (46 Prozent) der befragten Unternehmen über schriftlich geregelte Abläufe und Ad-hoc-Maßnahmen, also ein Notfallmanagement für den Fall der Fälle. Nur 39 Prozent der mittelständischen Unternehmen verfügen über ein entsprechend ausgebildetes Krisenmanagementteam, von diesen geben wiederum nur 29 Prozent der Befragten an, dieses Team regelmäßig zu trainieren. Das ist riskant, denn besteht ein Erstverdacht oder ein bestätigter Fall, muss sehr schnell agiert werden, insbesondere wenn der Vorfall öffentlichkeitswirksam ist. Ohne

eine entsprechende Vorbereitung kann viel falsch gemacht werden. So kann die falsche Kommunikationsstrategie gewählt oder ungewollt Beweise vernichtet werden. Eine professionelle Vorgehensweise ist im Rahmen der Schadensbegrenzung von größter Bedeutung.

Dennoch halten 71 Prozent der mittelständischen Unternehmen – und damit 7 Prozentpunkte mehr als bei den befragten Großunternehmen – ihre Reaktion auf Verdachtsmomente für immer zeitnah und angemessen.

### Fazit

Mit der Globalisierung und der einhergehenden internationalen Vernetzung und Digitalisierung agieren mittelständische Unternehmen längst in einem ähnlich komplexen Umfeld wie Großunternehmen und sind damit – trotz geringerer Medienpräsenz – den gleichen Risiken ausgesetzt. Diesen Risiken müssen sie in der Regel mit schlanken Unternehmensstrukturen begegnen. Daraus ergibt sich für den Mittelstand ein zusätzliches Spannungsfeld zwischen der effektiven und effizienten Eindämmung von Wirtschaftskriminalität und ihrer Flexibilität in Organisation und Geschäftsbetrieb.

Die Studienergebnisse zeigen, dass viele mittelständische Unternehmen den Handlungsbedarf grundsätzlich erkannt haben. Ob Whistleblower-Systeme, Ethikrichtlinien oder Integritätserklärungen für die Lieferantenkette – die ersten Schritte in die richtige Richtung wurden gegangen. Die Umfrageergebnisse zeigen aber auch, dass Vorkehrungen für Wirtschaftskriminalität bisher meist Einzelmaßnahmen sind. Es fehlt an einer strukturierten Vorgehensweise auf der Basis einer fundierten Risikoanalyse. So erklärt sich, dass zentrale Risiken, wie der Verlust von Betriebs- oder Geschäftsgeheimnissen, trotz negativer Erfahrungen weiterhin unterschätzt werden. Mittelständische Unternehmen müssen sich dieser Gefahren stärker bewusst werden und diesen mit strukturierten Präventions-

Aufklärungs- und Kontrollmaßnahmen begegnen. Dies mag einem Paradigmenwechsel gleichkommen, denn mit jeder zusätzlichen Kontrolle wird das lang gepflegte Vertrauensprinzip infrage gestellt. Doch genau hier ermöglicht ein geplantes und strukturiertes Vorgehen, die Gratwanderung zwischen Kontrollsystemen und Flexibilität erfolgreich zu meistern. Wem Schwachstellen und Risiken bekannt sind, der kann gezielt vorgehen und muss nicht willkürlich Kontrollmaßnahmen implementieren: Kontrolle wo nötig, Vertrauen wo möglich.

# Forensic – Wirtschaftskriminalität vermeiden und bekämpfen

Der Bereich Forensic von KPMG besitzt umfassende fachliche Expertise über wirtschaftskriminelle Handlungen, die, verknüpft mit einem breit gefächerten Erfahrungsschatz, eine praktische Ausrichtung bei der Analyse, Aufdeckung und Beratung wirtschaftskrimineller Sachverhalte in Unternehmen und Behörden bietet. Unserem multidisziplinär aufgestellten Team gehören deutschlandweit über 100 Fachleute an. Neben Wirtschaftsprüfern, Steuerberatern und Compliance-Spezialisten sind dies Psychologen, Datenschutzfachleute sowie ehemalige Kriminalbeamte, Staats- und Rechtsanwälte.

Auf der Basis langjähriger Forensic-Erfahrungen hat KPMG ein Dienstleistungsangebot entwickelt, das sich an den Bedürfnissen unserer Mandanten orientiert. Dabei bieten wir Ihnen sowohl professionelle Unterstützung bei der Aufklärung und Adressierung wirtschaftskrimineller Straftaten als auch einen umfassenden konzeptionellen Ansatz zur Prävention und Früherkennung von wirtschaftskriminellen und vermögensschädigenden Handlungen. Sprechen Sie uns an!

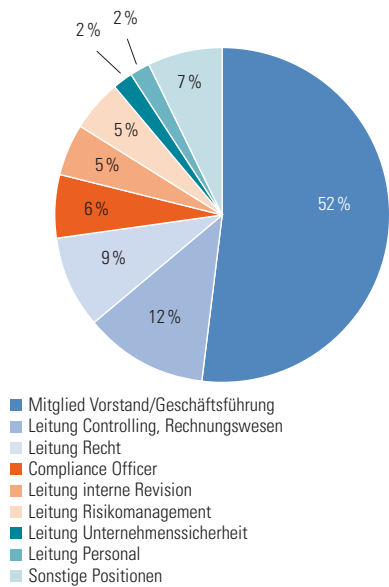
Wir helfen Ihnen bei:

Prävention	Aufdeckung	Aufklärung und Adressierung
<ul style="list-style-type: none"> <li>• Identifikation und Beurteilung von Wirtschaftskriminalitätsrisiken (Fraud and Misconduct Risk Assessment)</li> <li>• Verhaltensstandards und interne Richtlinien</li> <li>• Risikobeurteilungen bezüglich Mitarbeitern, Lieferanten etc. (Integrity Due Diligence)</li> <li>• Kommunikationsstrategien und Training</li> <li>• Prozessspezifische Anti-Fraud-Kontrollen</li> <li>• Datenschutz im Compliance Management</li> </ul>	<ul style="list-style-type: none"> <li>• Hotlines und Hinweisgebersysteme (Whistleblowing)</li> <li>• Regelmäßige Prüfungen und Überwachungsmaßnahmen</li> <li>• Proaktive forensische Datenanalyse</li> </ul>	<ul style="list-style-type: none"> <li>• Handlungskonzepte zur Adressierung von Verdachtsfällen (Incident Management and Response Plan)</li> <li>• Leitlinien zur Durchführung von forensischen Sonderuntersuchungen</li> <li>• Gestaltung und Durchsetzung von Sanktionsmaßnahmen</li> <li>• Empfehlungen zu notwendigen Abhilfemaßnahmen</li> </ul>

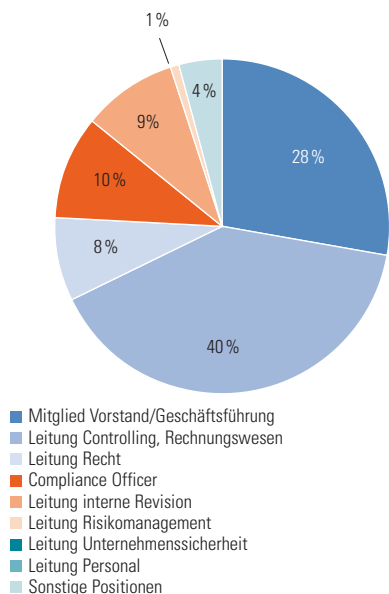
# Eckdaten der Studiendurchführung

Abb. 24: Welche Position nehmen Sie in Ihrem Unternehmen ein?

Familien-/Inhabergeführte Unternehmen



Große Unternehmen



Wie auch in der letzten Umfrage im Jahr 2006 haben wir ein international renommiertes Sozial- und Marktforschungsinstitut, die TNS Emnid in Bielefeld, mit der Durchführung der Befragung beauftragt. Der Fragebogen wurde von uns konzeptioniert und die Mitarbeiter von TNS Emnid umfassend eingewiesen. Die persönliche Befragung hat sich dabei bewährt, da viele Umfrageteilnehmer insbesondere aufgrund der Komplexität und Sensibilität des Themas einen direkten Gesprächspartner wünschen. Insgesamt wurden branchenübergreifend 300 Führungskräfte befragt.

Die Struktur des für die Umfrage konzeptionierten standardisierten Fragebogens orientierte sich an den für die Bekämpfung von Wirtschaftskriminalität besonders zentralen Themenbereichen. Wie auch in den Vorjahren haben wir mit dem Aufbau des Fragebogens daher wieder einen „80/20-Ansatz“ verfolgt: Die von uns vorgegebenen Auswahlmöglichkeiten zu einer Antwort decken die erfahrungsgemäß wichtigsten beziehungsweise häufigsten 80 Prozent der möglichen Antworten ab. Für die verbleibenden 20 Prozent blieb die Möglichkeit, individuelle Antworten zu geben.

Um insbesondere auch Unterschiede abhängig von der Unternehmensgröße festzustellen, wurden Unternehmen unterschiedlicher Größenklassen befragt. Es wurde hier eine repräsentative und nach Branchen und Umsatzzahlen stratifizierte Stichprobe ausgewählt.

In der von uns durchgeführten Auswertung wurden die Unternehmen auf der Basis ihres Umsatzes befragt. Für eine

Analyse des Mittelstands war eine Abgrenzung dieser Unternehmensgruppe nötig. Diese Trennlinie war nicht immer eindeutig zu ziehen, denn ein großer Teil der sogenannten mittelständischen Unternehmen produziert und vermarktet seine Produkte weltweit und nutzt die gleichen komplexen Finanzierungsstrukturen wie Großkonzerne. Daher konnte der Mittelstand nicht allein aufgrund von Kennzahlen kategorisiert werden, sondern wurde auf Basis der Eigentümer- und Führungsstruktur abgegrenzt. Als Mittelstand wurden die Unternehmen definiert, die inhaber- oder familiengeführt sind. Denn trotz der großen Vielfalt bedingt die Einheit aus Führung und Eigentum nach unserer Erfahrung eine spezielle Führungskultur. Von den 300 befragten Unternehmen waren nach dieser Definition 127 mittelständisch geprägt.

Die Fragebögen wurden jeweils von Führungskräften beantwortet, die im Rahmen ihres Verantwortungsbereichs die größte Nähe oder den besten Überblick über das Thema Wirtschaftskriminalität haben. Dies war entweder ein Mitglied der Geschäftsführung oder aber der Leiter der relevanten Fachabteilung.

# Ansprechpartner

KPMG AG  
Wirtschaftsprüfungsgesellschaft

**Frank M. Hülsberg**  
Leiter Forensic Deutschland  
Barbarossaplatz 1a  
50674 Köln  
T +49 221 2073-1678  
fhuelsberg@kpmg.de

Autorenteam: Stefan Weiss, Petra Lichtenau, Uwe Klapproth, Eva Maria Lucke

© 2010 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2010 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Germany. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.