KPMG

Im Spannungsfeld

Wirtschaftskriminalität in Deutschland 2020

Studie

17. August 2020

Unternehmen im Spannungsfeld

Liebe Leserinnen und Leser,

Wirtschaftskriminalität stellt Unternehmen fortwährend vor große Herausforderungen. Sei es die punktgenaue Allokation und Finanzierung von Präventionsmaßnahmen, die Frage der effektiven, aber auch rechtmäßigen Untersuchungsmaßnahmen oder die Reaktion auf auffällig gewordene Geschäftspartner und Mitarbeiter. Der Umgang mit Wirtschaftskriminalität, ihrer Risikoeinschätzung und Vorbeugung sowie der revolvierenden Verbesserung der Prozesse, Kontrollen und Maßnahmen ist eines der wesentlichen Governancethemen in der modernen Unternehmenswirklichkeit. Auf der Agenda einer jeden Geschäftsleitung und eines jeden Aufsichtsgremiums nimmt das Thema stetig mehr Raum ein. Ganze Abteilungen beschäftigen sich mit ihrer Analyse, Prävention, Aufdeckung und Aufklärung und auf nationaler wie auch internationaler Ebene gleichen sich die Rahmenbedingungen für wirksame Compliance-Management-Systeme einerseits und Sanktionsmechanismen andererseits immer mehr an.

Die Welt wird immer komplexer. Dies gilt auch mit Blick auf Wirtschaftskriminalität, einem sich stetig wandelnden Phänomen. In den sogenannten Nuller-Jahren haben wir vermehrt gegen Korruption gekämpft, danach für den Datenschutz, es schlossen sich die verschiedensten Delikte im Finanzsektor an und selbst die Corona-Krise hat eigene Fraud-Szenarien zum Vorschein gebracht. Die mit der neuen Situation einhergehenden Veränderungen der Prozess- und Geschäftsabläufe wie Home-Office oder Remote Working, eine dadurch bedingte Abweichung von etablierten Prozessen, hieraus resultierende fehlende oder unregelmäßigere Kontrollen und gegebenenfalls auch Zeit- und Erfolgsdruck, zum Beispiel bei der Bearbeitung von Kreditanträgen oder aufgrund von Arbeitsüberlastung wegen personeller Engpässe, bieten, verbunden mit der einhergehenden Verunsicherung von Bürgern, Mitarbeitern, Unternehmen und Märkten, einen idealen Nährboden für betrügerische Aktivitäten. Bei Phishing-Mails, betrügerischen Webseiten, Fake President-Angriffen, Kredit- und Subventionsbetrug sowie dem Einsatz von Finanzagenten ist seit März 2020 eine starke Zunahme zu verzeichnen.

Hinzu kommen immer neue regulatorische Anforderungen. So hat sich zum Beispiel im Januar 2020 das Geldwäschegesetz geändert und sieht nun neue Anforderungen an das geldwäschebezogene Risikomanagement vor. Das US Department of Justice und das US Office of Foreign Assets Control haben in entsprechenden Guidances ihre Vorstellungen zur Ausgestaltung eines Compliance-Programms vorgegeben. In Deutschland befindet sich zudem die Diskussion um ein Verbandssanktionengesetz in vollem Gange. Sieht der Entwurf dieses Gesetzes auf der einen Seite zwar Bußgelder von bis zu 10 Prozent des weltweiten Konzernvorjahresumsatzes vor, so zeigt er auf der anderen Seite Wege auf, das Bußgeld zu mindern. Nach den Vorgaben des Gesetzes durchgeführte interne Ermittlungen führen zu einer Reduzierung des Bußgeldrahmens um die Hälfte. Compliance-Maßnahmen können sich ebenfalls bußgeldmindernd auswirken.

Somit bleibt es auch in Zukunft dabei, dass sich Wirtschaftskriminalität nicht nur selbst dynamisch entwickelt, sondern auch denjenigen, die davon betroffen sind oder sich damit befassen, in höchstem Maße Flexibilität abverlangt.

In diesem Sinne wünsche ich Ihnen eine spannende und erkenntnisreiche Lektüre.

Ihre
Barbara Scheben
Head of Forensic Deutschland

Inhalt

Executive Summary

Risikoeinschätzung und Betroffenheit deutscher Unternehmen bleiben weiterhin konstant.

» Die überwiegende Mehrheit (78 Prozent) der befragten Unternehmen schätzt das generelle Risiko deutscher Unternehmen, von wirtschaftskriminellen Handlungen betroffen zu sein, als hoch oder sehr hoch ein. Mit zunehmender Unternehmensgröße wächst auch das wahrgenommene Risiko.

» Die durch Wirtschaftskriminalität verursachten Kosten steigen. Vor allem große Unternehmen (30 Prozent) verzeichnen häufiger Schäden in Höhe von mehr als 1 Millionen Euro.

» Im Vergleich zu der vorangegangenen Studie machen Unternehmen seltener Externe für wirtschaftskriminelle Handlungen verantwortlich (2020: 47 Prozent; 2018: 61 Prozent).

» Das Risiko, von Wirtschaftskriminalität betroffen zu sein, hält mehr als jedes zweite Unternehmen (52 Prozent), das sein Schutzniveau selbst als unzureichend einschätzt, für hoch oder sehr hoch. Unter denen mit gutem oder sehr gutem Schutz sind es lediglich 28 Prozent beziehungsweise 15 Prozent.

Die Tendenz eines präventiven Ansatzes zur Vermeidung von Wirtschaftskriminalität ist weiterhin erkennbar. Externe Unterstützung im Umgang mit wirtschaftskriminellen Handlungen ist bereits bei der Mehrheit der Unternehmen üblich oder zumindest beabsichtigt.

» Verhaltensgrundsätze und Leitbilder im Unternehmen sind erneut das bevorzugte Mittel der Wahl, was Präventionsmaßnahmen betrifft. Acht von zehn Unternehmen vertrauen darauf.

» Mehr als jedes zweite Unternehmen (56 Prozent) vertraut bei unternehmensinternen Sachverhaltsaufklärungen oder Untersuchungen wirtschaftskrimineller Handlungen auf externe Unterstützung.

» Die Fortführung der Geschäftsbeziehung mit Tätern wirtschaftskrimineller Handlungen wird zunehmend an Bedingungen geknüpft (2020: 46 Prozent, 2018: 44 Prozent). Vor allem die unabhängige Prüfung des Compliance-Management-Systems (CMS) durch Dritte gewinnt im Hinblick auf die Fortsetzung der Geschäftsbeziehung an Bedeutung.

Über die Hälfte der deutschen Unternehmen ist mit dem Thema Sanktionen und Embargos nicht vertraut, obwohl bei Verstößen gravierende Bußgelder erwartet werden.

» Für nahezu vier von fünf der befragten Unternehmen bedeutet ein Sanktions- und Embargoverstoß einen enormen Reputationsschaden (79 Prozent).

» Risiken, gegen Sanktionen und Embargos zu verstoßen, sehen vor allem große Unternehmen. 25 Prozent dieser Gruppe stufen sie als hoch oder sehr hoch ein.

» Auch die erwarteten Auswirkungen im Falle eines entdeckten Verstoßes werden von großen Unternehmen (nach Umsatz) kritischer wahrgenommen – hier geben 70 Prozent an, mit gravierenden Bußgeldern zu rechnen.

» Fast jedem zweiten kleinen Unternehmen (42 Prozent) fehlt es an hinreichenden Handreichungen und Richtlinien dazu, wie sie sich sanktions- und embargokonform verhalten können.

» Mehr als jedes dritte der umsatzstarken Unternehmen sieht einen Bedarf an Sanktions- und Embargo-Compliance lediglich für Unternehmen des Finanzsektors (36 Prozent). Vor allem mittlere Unternehmen teilen diese Ansicht deutlich seltener (13 Prozent).

Der Einsatz digitaler Compliance-Werkzeuge nimmt zu. Dies führt bei einem Großteil der Unternehmen zu einer Effizienzsteigerung der Compliance-Einheit und wirkt auch präventiv.

» Große Unternehmen setzen vor allem bei Compliance-Reporting und Due Diligence-Prüfungen Dritter (79 beziehungsweise 60 Prozent) auf digitale Werkzeuge, kleine und mittelgroße Unternehmen häufig im Vertragsmanagement (41 und 55 Prozent).

» Die überwiegende Mehrheit nennt Effizienzsteigerungen (79 Prozent) sowie die Stärkung der Prävention von Wirtschaftskriminalität (71 Prozent) als Gründe für die Digitalisierung im Compliance-Umfeld.

» Die größte Herausforderung für ein digitales Compliance-Umfeld stellt der Mangel an Ressourcen dar. Dies teilen selbst große Unternehmen mit; von ihnen benennen knapp zwei Drittel (65 Prozent) diesen Aspekt als Hemmnis im Hinblick auf die Digitalisierung.

1. Risikoprofil, Betroffenheit und Kosten von Wirtschaftskriminalität

Risikoeinschätzung und Betroffenheit deutscher Unternehmen bleiben weiterhin konstant.

1.1 Allgemeine Risikowahrnehmung und Betroffenheit

Wie bereits in der Studie von 2018 lässt sich auch in der diesjährigen Befragung eine hohe Diskrepanz zwischen Selbst- und Fremdwahrnehmung der Risiken wirtschaftskrimineller Handlungen feststellen. So schätzen die Befragten das Risiko, von Wirtschaftskriminalität betroffen zu sein, für ihr eigenes Unternehmen grundsätzlich deutlich geringer ein als für andere deutsche Unternehmen (30 gegenüber 78 Prozent).

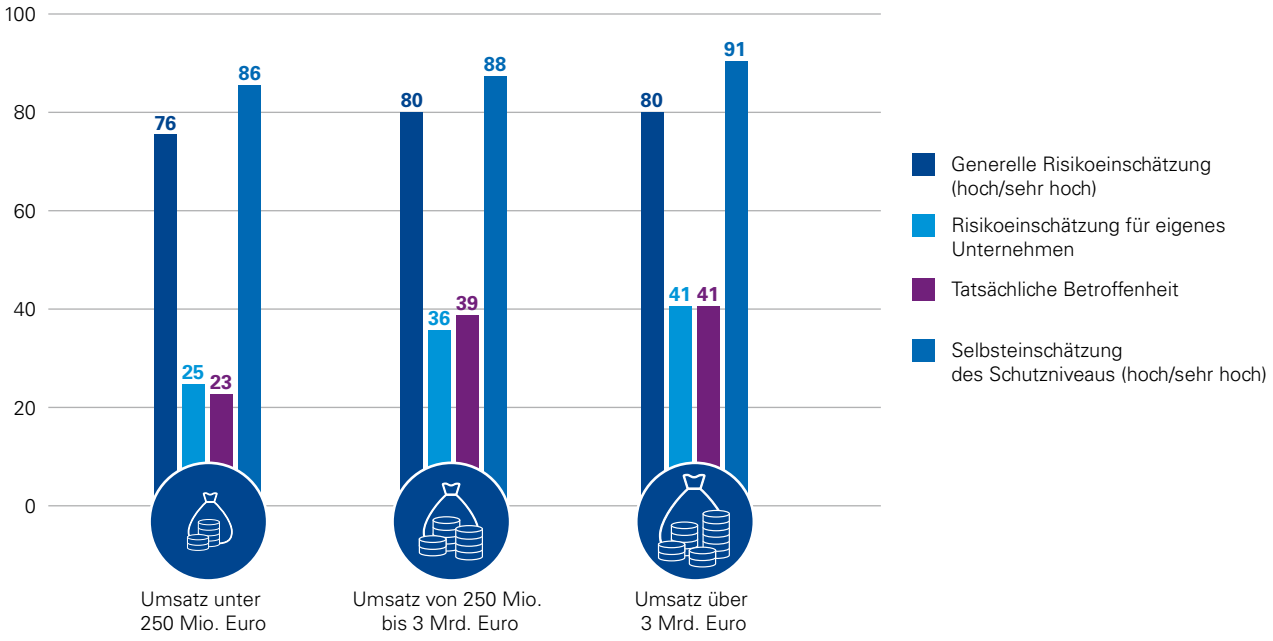
In Bezug auf die Bewertung des generellen Risikos für deutsche Unternehmen sind kaum Unterschiede zwischen den Größenklassen auszumachen. Im Hinblick auf die Risikoeinschätzung für das eigene Unternehmen jedoch zeichnet sich ab, dass kleine Unternehmen die Gefahr, selbst von wirtschaftskriminellen Handlungen oder Compliance-Verstößen betroffen zu sein, grundsätzlich niedriger einstufen als mittlere oder große.

Dies heißt allerdings nicht, dass sich kleine Unternehmen auch für besser geschützt halten, denn: Zwar bezeichnen immerhin 86 Prozent von ihnen das eigene Schutzniveau als gut oder gar sehr gut (Letzteres: 11 Prozent), doch bei den großen Unternehmen fällt diese Einschätzung noch optimistischer aus – 91 Prozent halten ihren Schutz für gut oder sehr gut (Letzteres: 20 Prozent). Auch im Allgemeinen besitzen die Befragten ein großes Vertrauen in ihr eigenes Schutzniveau. Dies zeigt sich insbesondere darin, dass lediglich 12 Prozent der Befragten dieses als schlecht bewerten.

Für die vorliegende Studie sind die befragten Unternehmen in die Kategorien groß, mittel und klein eingeteilt. Unternehmen mit einem Umsatz von über 3 Milliarden Euro oder mit mehr als 500 Mitarbeitern gelten hierbei als groß, mittlere Unternehmen sind die mit einem Umsatz zwischen 250 Millionen und 3 Milliarden Euro oder mit 101 bis 500 Mitarbeitern, und Unternehmen, die diese Schwellenwerte nicht erreichen, gelten als klein. Sofern es zwischen Unternehmen derselben Kategorie größere Unterschiede beim Umsatz oder bei der Mitarbeiterzahl gibt, wird dies gesondert erwähnt.

Es überrascht zudem nicht, dass Unternehmen, die ein positives Bild von ihrem Schutzniveau haben, das Risiko, von wirtschaftskriminellen Handlungen betroffen zu sein, grundsätzlich deutlich seltener als hoch oder sehr hoch einstufen als diejenigen, die sich selbst keine sonderlich geeigneten Schutzvorkehrungen attestieren (28 gegenüber 52 Prozent).

Abbildung 1: Vergleich Risikoeinschätzung, Betroffenheit und Einschätzung des eigenen Schutzes im Hinblick auf Wirtschaftskriminalität



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Trotz des grundsätzlich als hoch wahrgenommenen Schutzniveaus des eigenen Unternehmens ist die allgemeine Betroffenheit gemäß den Ergebnissen der aktuellen Umfrage nur unwesentlich gesunken (2020: 30 Prozent; 2018: 32 Prozent). Dabei liegt die Betroffenheitsrate bei nach eigener Einschätzung sehr gut gegen Wirtschaftskriminalität geschützten Unternehmen unter der Rate der Unternehmen, die sich selbst als schlecht geschützt einstufen (17 gegenüber 34 Prozent). Dies deutet darauf hin, dass diese Unternehmen also nicht nur gefühlt, sondern auch tatsächlich besser gewappnet sind, was für den Wert präventiver Maßnahmen spricht.

Die Zahlen zeigen grundsätzlich, dass mit zunehmender Größe des Unternehmens die Betroffenheitsrate steigt. Eine möglicherweise höhere Attraktivität sowie eine höhere Komplexität der Unternehmensstruktur könnten dies erklären. Jedoch sollte in diesem Zusammenhang auch das sogenannte Kontrollparadoxon berücksichtigt werden: Dieses besagt, dass ausgeprägtere Kontrollmaßnahmen zu einer vermehrten Aufdeckung wirtschaftskrimineller Handlungen führen, wohingegen viele Verstöße in Unternehmen mit weniger ausgeprägten Kontrolltätigkeiten unerkannt bleiben.

Mithin ist bei kleinen Unternehmen – also bei denen, die oftmals über einen weniger starken Schutz verfügen – schlichtweg das Dunkelfeld größer als bei großen Unternehmen, da sie nicht über die erforderlichen Maßnahmen und Mittel zur Aufdeckung wirtschaftskriminellen Handelns verfügen (siehe Abschnitt 2.6).

Im Kontext allgemeiner Risikowahrnehmung und Betroffenheit fällt schließlich ein weiterer Aspekt ins Auge: Unternehmen, die in den vergangenen zwei Jahren bereits von Wirtschaftskriminalität betroffen waren, schätzen das Risiko, künftig mit solchen Vorfällen konfrontiert zu werden, mehrheitlich (51 Prozent) als hoch oder sehr hoch ein. Nur ein Fünftel der Unternehmen, die bislang noch nicht von Wirtschaftskriminalität betroffen waren, teilt diese Einschätzung.

Hinsichtlich einer etwaigen künftigen Veränderung des Risikos für das eigene Unternehmen, mit Wirtschaftskriminalität konfrontiert zu werden, gleichen die Ergebnisse im Wesentlichen denen von 2018: Nahezu jeder dritte Befragte ist der Meinung, dieses Risiko werde in den kommenden zwei Jahren zunehmen. Nur 6 Prozent gehen von einem sinkenden Risiko aus.

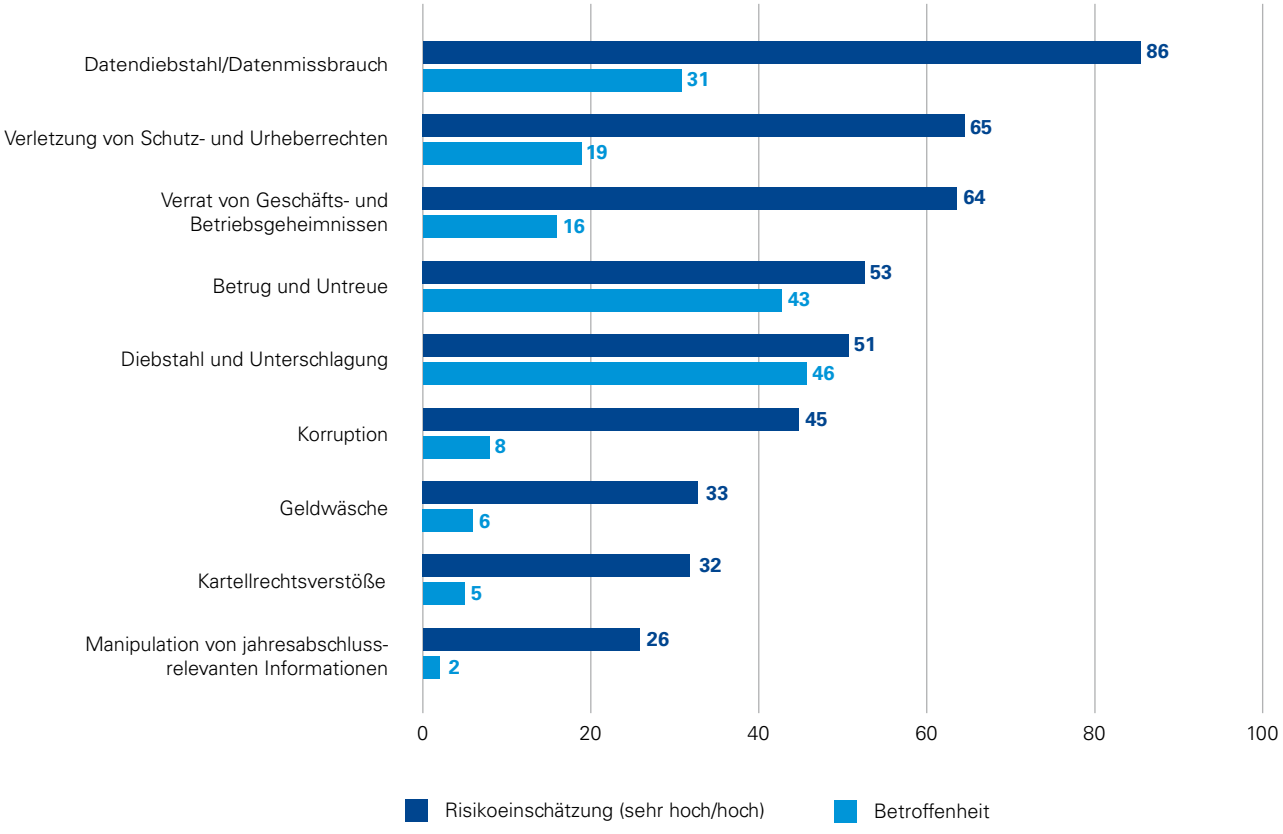
1.2 Deliktsspezifische Risikowahrnehmung und Betroffenheit

Die deliktsspezifische Einschätzung der Betroffenheit ähnelt der aus der Untersuchung vor zwei Jahren.

Datendelikte bereiten den Befragten nach wie vor die größten Sorgen – 86 Prozent bezeichnen das Risiko, von entsprechenden Verstößen betroffen zu sein, als hoch oder sehr hoch, wobei „sehr hoch" hier vergleichsweise häufig genannt wird (29 Prozent). Dies gilt unabhängig von Mitarbeiterzahl, Umsatzstärke und auch Selbstbewertung der unternehmensinternen Schutzmaßnahmen.

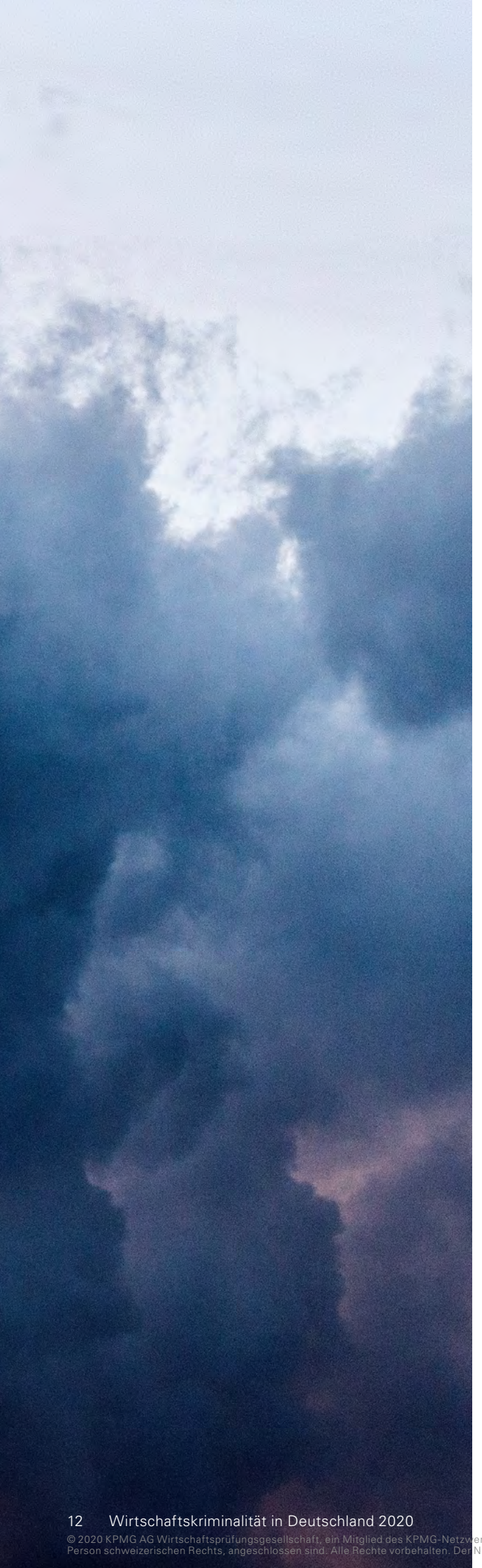
Betroffen von Datendelikten war in den vergangenen zwei Jahren knapp ein Drittel der Unternehmen (31 Prozent). Dass Risikoeinschätzung und Betroffenheit derart divergieren – 86 gegenüber 31 Prozent –, könnte auf die enorme mediale Präsenz dieser Thematik angesichts der EU-Datenschutz-Grundverordnung und auch auf Cybercrime-Fälle sowie Hackerangriffe zurückzuführen sein, die in jüngerer Vergangenheit Wellen geschlagen haben. Während die Zahl derer, die den eigenen Angaben zufolge von derartigen Delikten betroffen waren, sich gegenüber 2018 nicht verändert hat (jeweils 31 Prozent), geben 2020 deutlich mehr Unternehmen als zuvor an, das Risiko eines Datendeliktes als sehr hoch einzuschätzen (2020: 29 Prozent; 2018: 21 Prozent). Dies verdeutlicht die immense Bedeutung des Themenfelds Datenschutz in Zeiten, in denen die Menge der verarbeiteten Daten in den Unternehmen stetig zunimmt. Mit der Digitalisierung geht auch eine größere Bereitschaft einher, zunehmend Daten sensibler Kategorien zu verarbeiten – für die besondere Schutzvorkehrungen erforderlich sind.

Abbildung 2: Risikoeinschätzung im Vergleich zur tatsächlichen Betroffenheit



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent



Eine ähnliche Medienpräsenz erfuhr in jüngerer Vergangenheit das Thema Geldwäsche. Trotz neuer regulatorischer Anforderungen sehen die Unternehmen das darin innewohnende Risiko allerdings als geringer an. Knapp zwei Drittel der befragten Unternehmen (64 Prozent) schätzen das Risiko, betroffen zu sein, als niedrig oder sogar sehr niedrig ein.

» Mit Inkrafttreten der 5. EU-Geldwäscherichtlinie wird der Verpflichtetenkreis noch einmal erweitert. Geldwäsche trifft weit mehr Unternehmen als nur den Finanzsektor. «

Nach Branchen aufgeschlüsselt tritt bei der Risikowahrnehmung in Bezug auf Geldwäsche ein deutlicher Unterschied zutage, und zwar zwischen Unternehmen des Finanzsektors und Unternehmen anderer Branchen. Dies deckt sich mit den Erkenntnissen aus der Studie des Jahres 2018, jedoch ist die Trennlinie mittlerweile sogar noch breiter geworden: 75 Prozent der Unternehmen des Finanzsektors benennen das Risiko, von Geldwäsche betroffen zu sein, als hoch oder sehr hoch. Im Jahr 2018 waren dies 60 Prozent. In anderen Branchen gilt dies für lediglich 30 Prozent der Unternehmen (2018: 27 Prozent).

43 Prozent der betroffenen Unternehmen nennen Delikte im Bereich Betrug und Untreue – hier insbesondere umsatzstarke Unternehmen (kleine Unternehmen: 39 Prozent; große Unternehmen: 71 Prozent). Im Vergleich zur vorangegangenen Studie ist die durchschnittliche Betroffenheit jedoch um 15 Prozentpunkte gesunken (2020: 43 Prozent; 2018: 58 Prozent).

60 Prozent der befragten Unternehmen, die ihre internen Sicherungsmaßnahmen als sehr gut bewerten, gaben an, in der Vergangenheit von Betrug und Untreue betroffen gewesen zu sein. Dies liegt 17 Prozentpunkte über dem Durchschnitt aller Deliktsarten. Ursächlich hierfür könnte ebenfalls das Kontrollparadoxon sein.

Die Aktualität und Allgegenwart betrügerischer Taten hat sich erst kürzlich wieder eindrucksvoll offenbart, nämlich im Rahmen der Corona-Krise. Manche Kriminelle haben den Drang nach Finanzstabilität sowie einer schnellen Schadenregulierung erkannt und ausgenutzt. Durch das Abweichen von Regelprozessen und routinemäßigen Kontrollen ergeben sich für Betrüger günstige Gelegenheiten.

Auch die Gefahr, sogenannten Fake President-Angriffen zum Opfer zu fallen, ist im Zusammenhang mit der Corona-Krise aus den zuvor genannten Gründen und insbesondere auch im Hinblick auf die Verlagerung der Arbeitstätigkeit ins Home-Office gestiegen. Hierbei nehmen Betrüger per E-Mail oder telefonisch Kontakt mit Mitarbeitern auf, geben sich als Unternehmensleitung aus und veranlassen, dass sie Zahlungen auf bestimmte Konten vornehmen, die diesen Betrügern zuzuordnen sind.

» Fake President-Angriffe nutzen das Abweichen von Regelprozessen aus. Dies war jüngst in der Corona-Pandemie durch eine Zunahme der Fälle wieder zu sehen. «

Betrachtet man die Risikoeinschätzung und die tatsächliche Betroffenheit für Delikte im Bereich Betrug und Untreue, aber auch für Diebstahl und Unterschlagung, liegen diese entgegen dem Trend der Divergenz, der sich bei den anderen abgefragten wirtschaftskriminellen Delikten zeigt, nah beieinander (Betrug und Untreue: 53 zu 43 Prozent; Diebstahl und Unterschlagung: 51 zu 46 Prozent). Es fällt jedoch auf, dass diese Delikte trotz der hohen Betroffenheitszahlen eine vergleichsweise niedrigere Risikowahrnehmung verzeichnen als Deliktsarten, die bei Unternehmen deutlich seltener aufgetreten sind, wie beispielsweise die Verletzung von Schutz- und Urheberrechten (Betroffenheit: 19 Prozent; Risikowahrnehmung: 65 Prozent hoch/sehr hoch). Die Ursache könnte darin liegen, dass Betrug und Untreue sowie Diebstahl und Unterschlagung vermeintlich „alltäglicher" sind und somit für Unternehmen greifbarer und leichter kalkulierbar wirken.

In der diesjährigen Befragung gaben 8 Prozent der Unternehmen an, von Korruption betroffen gewesen zu sein. Dies bestätigt den Trend einer rückläufigen Betroffenheit, der sich bereits in den vorhergehenden Studien abzeichnete (2018: 13 Prozent; 2016: 16 Prozent). Bemerkenswert ist allerdings, dass umsatzstarke Unternehmen, die in der Befragung aus 2018 mit 11 Prozent am wenigsten betroffen waren, nun mit einer Betroffenheitsrate von 18 Prozent Spitzenreiter sind. Die prozentuale Verteilung bei mittleren und kleinen Unternehmen präsentiert sich jedoch genau gegenläufig, also mit einem Rückgang. Mit Blick auf Kartellverstöße sind besonders umsatzstarke Unternehmen am seltensten betroffen. Gaben 2016 noch 21 Prozent der Unternehmen mit einem Umsatz von 3 Milliarden Euro oder mehr an, Verstöße gegen das Kartellrecht zu verzeichnen, waren es 2018 lediglich 6 Prozent, und seither konnte die Zahl sogar noch halbiert werden (2020: 3 Prozent). Der Eindruck, dass mittelgroße Unternehmen am stärksten von solchen Vorfällen betroffen sind, lässt sich auch in diesem Jahr wieder bestätigen: 2018 gaben 11 Prozent der mittleren Unternehmen an, mit solchen Fällen konfrontiert gewesen zu sein, 2020 waren es 8 Prozent.

Verletzungen von Schutz- und Urheberrechten werden von deutschen Unternehmen weiterhin als sehr riskant eingestuft (hoch/sehr hoch: 65 Prozent). Vor allem vor dem Hintergrund der Produkt- und Markenpiraterie ist das Bedürfnis, die eigenen Erzeugnisse zu schützen, für Unternehmen essenziell. Dies zeigt sich insbesondere darin, dass auch 60 Prozent der Unternehmen mit sehr guten Schutzmaßnahmen gegen wirtschaftskriminelle Handlungen das Risiko von Delikten dieser Art als hoch beziehungsweise sehr hoch einschätzen. Darüber hinaus ist auch die allgemeine Betroffenheit bei dieser Deliktsart von 13 Prozent auf 19 Prozent gestiegen.

» Als vermeintliche Alltagsdelikte finden Betrug und Untreue, aber auch Diebstahl und Unterschlagung in der Risikowahrnehmung von Unternehmen wenig Beachtung – ein gefährlicher Trugschluss! «

Die von 2016 auf 2018 verschärfte Sorge ob solcher Risiken im verarbeitenden Gewerbe hat sich in diesem Jahr nicht bestätigt. Vielmehr glich sich die Risikowahrnehmung über die Branchen hinweg immer mehr an, sodass sich die Angaben nach Branche lediglich mit wenigen Prozentpunkten unterscheiden. Unternehmen des verarbeitenden Gewerbes bewerten das Risiko in 66 Prozent der Fälle als hoch oder sehr hoch (2018: 71 Prozent), Unternehmen aus der Handels- und Dienstleistungsbranche sehen dies ähnlich (Handel: 65 Prozent, Dienstleistung: 64 Prozent), was einen leichten Anstieg der Zahlen im Vergleich zur vorangegangenen Studie bedeutet.

Was die Verletzung von Geschäftsgeheimnissen betrifft, ist ein zunehmendes Risikobewusstsein zu erkennen (2020: 64 Prozent, 2018: 60 Prozent). Sowohl mittlere als auch große Unternehmen stufen dieses Risiko sogar vermehrt als sehr hoch ein. Insgesamt ist auch die Betroffenheit dieser Deliktsart von 10 Prozent auf 16 Prozent gestiegen.

Als grundsätzlich deutlich geringer nehmen Unternehmen – unabhängig von Branche und Größe – die Gefahr der Manipulation von jahresabschlussrelevanten Informationen wahr. 71 Prozent gaben an, das Risiko sei niedrig oder gar sehr niedrig. Die Zahl der Betroffenen hat sich gegenüber 2018 sogar mehr als halbiert (von 5 auf 2 Prozent).

1.3 Kosten

Unter Gesamtschaden ist die Gesamtheit aller im unmittelbaren Zusammenhang mit wirtschaftskriminellen Handlungen abgeflossenen Vermögenswerte, entgangenen Gewinne, Ermittlungs- und Folgekosten sowie etwaigen Bußgelder, Geldstrafen und eventuellen Gewinnabschöpfungen zu verstehen.

Zur Darstellung der Studienergebnisse sind im Folgenden Bandbreiten angegeben, in die sich die Schadenssummen einordnen lassen (25- und 75-Prozent-Quantil um den Median). Sonstige Auffälligkeiten werden separat genannt.

Knapp jedes fünfte Unternehmen konnte bei der diesjährigen Umfrage den aus wirtschaftskriminellen Handlungen resultierenden monetären Schaden nicht in Zahlen angeben (18 Prozent). In der Studie des Jahres 2018 gab noch jedes sechste Unternehmen an, zu den entstandenen Kosten keine Angabe machen zu können (16 Prozent). Somit lässt sich der zuvor festgestellte Trend, dass Unternehmen vermehrt in der Lage sind, den Schaden zu beziffern und deliktsspezifisch einzuordnen, nicht bestätigen. Vor allem bei den Deliktsarten Korruption (2020: 39 Prozent, 2018: 11 Prozent), Verletzung von Geschäftsgeheimnissen (2020: 35 Prozent, 2018: 13 Prozent) sowie Geldwäsche (2020: 35 Prozent, 2018: 12 Prozent) bestehen diesbezüglich Defizite. Die Quantifizierung deliktsspezifischer Schäden ist jedoch eine wichtige Voraussetzung für ein effektives Risikomanagement, denn nur auf einer solchen Grundlage lassen sich die unternehmensindividuelle Gefährdungslage zutreffend einschätzen und angemessene Gegenmaßnahmen ergreifen.

Ein besonders großer Anteil der befragten Unternehmen, die ihren Schaden beziffern konnten, verzeichnete einen Gesamtschaden zwischen 100.000 und 180.000 Euro. Allerdings traten auch Schäden von bis zu 400.000 Euro (75-Prozent-Quantil) in nicht unerheblichem Maße auf. Im Vergleich zur vorigen Studie stieg die Anzahl der Unternehmen, die einen Schaden in Höhe von 1 Million Euro oder mehr zu Protokoll gaben, leicht an (2020: 10 Prozent, 2018: 7 Prozent). Angesichts der wirtschaftlichen Dimension ihres Geschäfts überrascht es nicht, dass insbesondere große Unternehmen Gesamtschäden im siebenstelligen Bereich verzeichnen. In 30 Prozent der Fälle bewegten sich die Schäden in dieser Größenordnung (2018: 13 Prozent).

» 10 Prozent der Unternehmen gaben an, einen Schaden von 1 Million Euro oder mehr erlitten zu haben. «

Abbildung 3: Gesamtschaden durch Wirtschaftskriminalität in den vergangenen zwei Jahren

	Gesamt	Umsatz unter 250 Mio. Euro	Umsatz von 250 Mio. bis 3 Mrd. Euro	Umsatz über 3 Mrd. Euro
Unter 10.000 Euro	4	9	0	0
10.000 bis 99.999 Euro	27	35	24	3
100.000 bis 999.999 Euro	42	38	46	48
1 Mio. Euro oder mehr	10	4	13	30
Keine Angabe	18	16	20	21

Quelle: KPMG, Deutschland, 2020

Angaben in Prozent, Rundungsdifferenzen möglich

Bereits 2018 gaben die Studienteilnehmer an, die höchsten Kosten seien ihnen aufgrund von Kartellrechtsverstößen entstanden – ein Bild, das auch die diesjährige Studie wiedergibt. Mehrheitlich geben die Unternehmen an, wegen derartiger Vergehen einen Schaden zwischen 50.000 und 500.000 Euro erlitten zu haben (2018: 100.000 bis 500.000 Euro).

Ähnlich starke finanzielle Auswirkungen hatten Korruptionsfälle auf deutsche Unternehmen (62.500 bis 475.000 Euro).

Vergleichsweise gering fallen dagegen die angegebenen Schäden aufgrund von Datendiebstahl oder -missbrauch aus (20.000 bis 150.000 Euro). Im Hinblick auf das offiziell ausgesprochene „Ende der Kulanz" deutscher Datenschutzbehörden sind Unternehmen dennoch besonders gut beraten, ihre Schutzmaßnahmen zu überprüfen und gegebenenfalls anzupassen, um die Gefahr von Datenschutzverstößen in den eigenen Reihen zu minimieren. Zudem sei darauf hingewiesen, dass die Daten, die in diese Studie eingeflossen sind, erhoben wurden, bevor die Nachrichten über die ersten Millionenbußgelder in Deutschland, die wegen Verstößen gegen die DSGVO verhängt wurden, an die Öffentlichkeit gelangten.

Neben den monetären Schäden sind bei solchen Vorkommnissen auch Reputationsschäden und Vertrauensverlust infolge der medialen Berichterstattung unter Umständen gravierende Begleiterscheinungen. Insgesamt bleibt hier abzuwarten, wie sich der Trend im Laufe der nächsten Jahre fortsetzen wird.

Der durchschnittliche Anteil der Ermittlungs- und Folgekosten am Gesamtschaden beläuft sich auf 22 Prozent und fällt damit ähnlich ins Gewicht wie in der vorangegangenen Studie (seinerzeit 19 Prozent). Mit Blick auf die unterschiedlichen Deliktsarten lässt sich festhalten, dass Verstöße aus dem Bereich Betrug und Untreue in der diesjährigen Studie den größten Zuwachs verzeichnen. So wird im Rahmen von Betrug und Untreue mehr als ein Drittel der Summe für Ermittlungs- und Folgekosten aufgebracht, was einen deutlichen Anstieg bedeutet (2020: 35 Prozent, 2018: 21 Prozent). Auffällig gering fällt dagegen der deliktsspezifische Anteil dieser Kosten im Bereich der Verletzungen von Schutz- und Urheberrechten aus. Schlug er 2018 mit 25 Prozent noch vergleichsweise deutlich zu Buche, ist er seither auf 9 Prozent geschrumpft.

Abbildung 4: Kategoriespezifischer Anteil der Ermittlungs- und Folgekosten an den Gesamtschäden

Quelle: KPMG, Deutschland, 2020

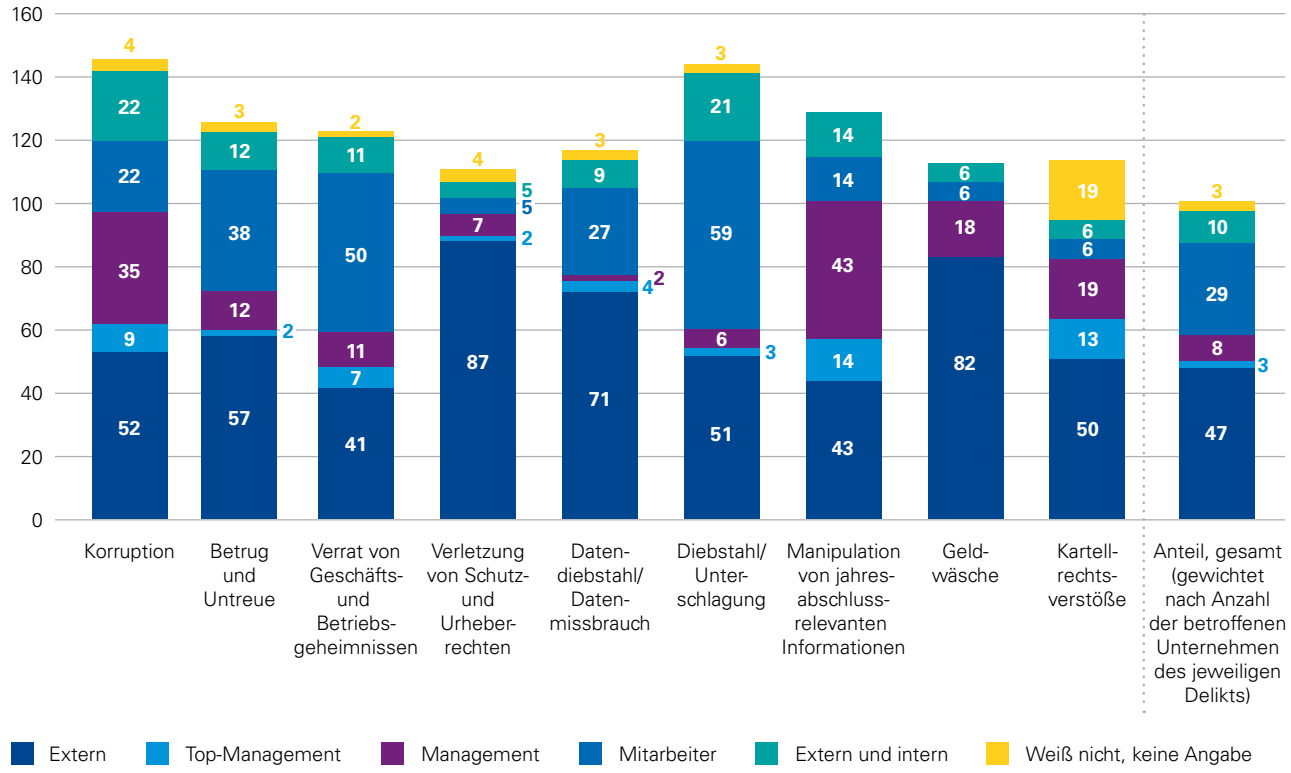
Angaben in Prozent

1.4 Täterherkunft

Externe, nicht zum jeweiligen Unternehmen gehörende Personen spielen bei wirtschaftskriminellen Handlungen derzeit eine kleinere Rolle als interne, was vor zwei Jahren noch deutlich anders aussah. Den Umfrageergebnissen zufolge lag die Beteiligung Externer in dieser Studie bei 47 Prozent, während sich dieser Wert 2018 auf 61 Prozent belief. In 10 Prozent der Fälle haben externe und interne Täter bei der Begehung wirtschaftskrimineller Handlungen zusammengewirkt.

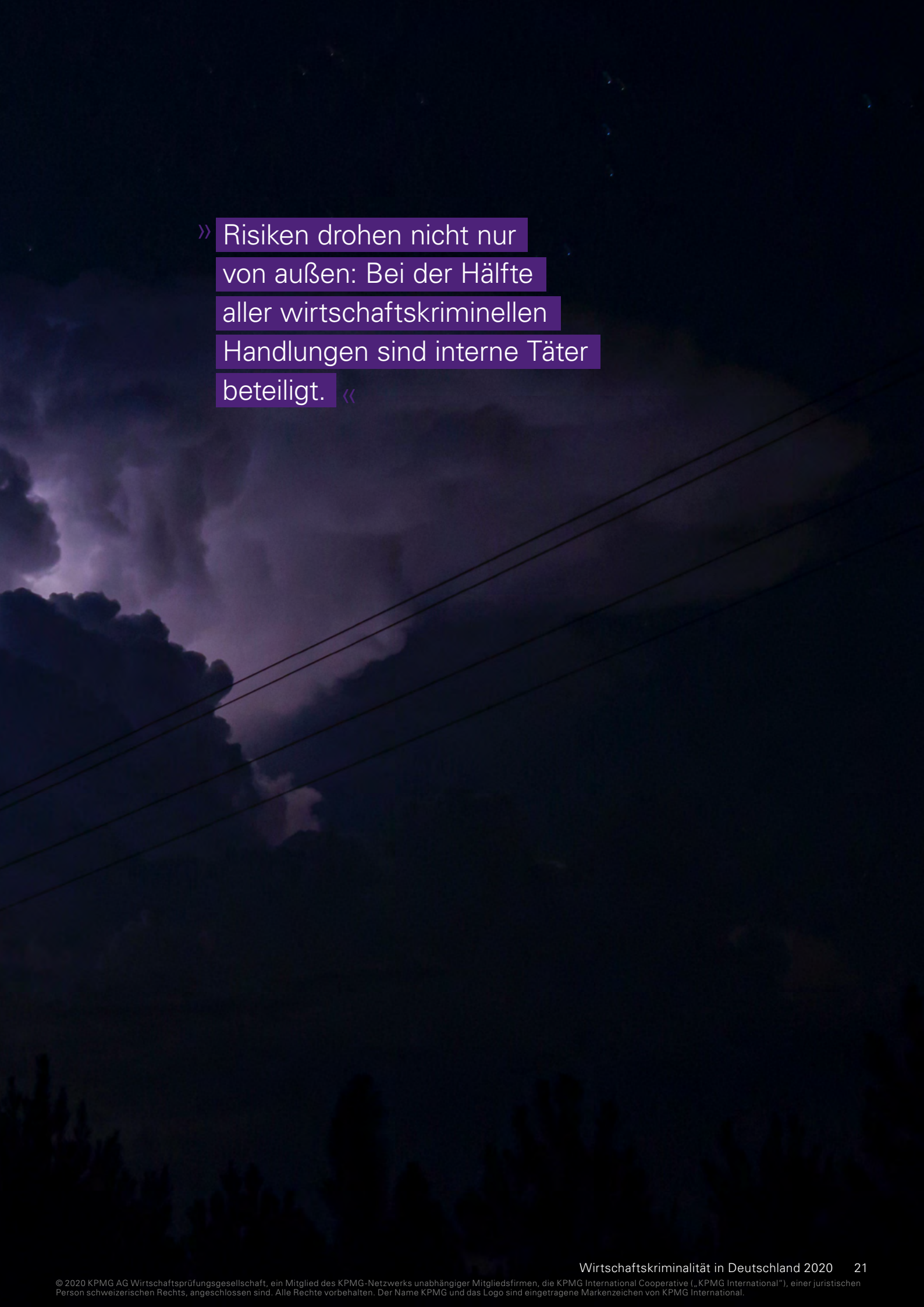
Für Geldwäschedelikte (82 Prozent) und Delikte im Hinblick auf die Verletzung von Schutz- und Urheberrechten (87 Prozent) werden mehrheitlich externe Täter angegeben. Für Deliktsarten wie Manipulation jahresabschlussrelevanter Informationen (71 Prozent), Diebstahl und Unterschlagung sowie Verletzung von Geschäftsgeheimnissen (jeweils 68 Prozent) sind es mehrheitlich interne Täter.

Abbildung 5: Täterherkunft



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent; Werte über 100 Prozent ergeben sich daraus, dass auch die Tatbegehung durch ein Zusammenwirken interner und externer Täter abgefragt wurde



» Risiken drohen nicht nur von außen: Bei der Hälfte aller wirtschaftskriminellen Handlungen sind interne Täter beteiligt. «

Die Gruppe derer, die Fälle nicht eindeutig einer Tätergruppe zuordnen können, umfasst 3 Prozent der Unternehmen. Die einzige Ausnahme bilden hier Kartellrechtsverstöße, bei denen immerhin knapp jeder Fünfte (19 Prozent) keine Angaben zum Täterkreis macht.

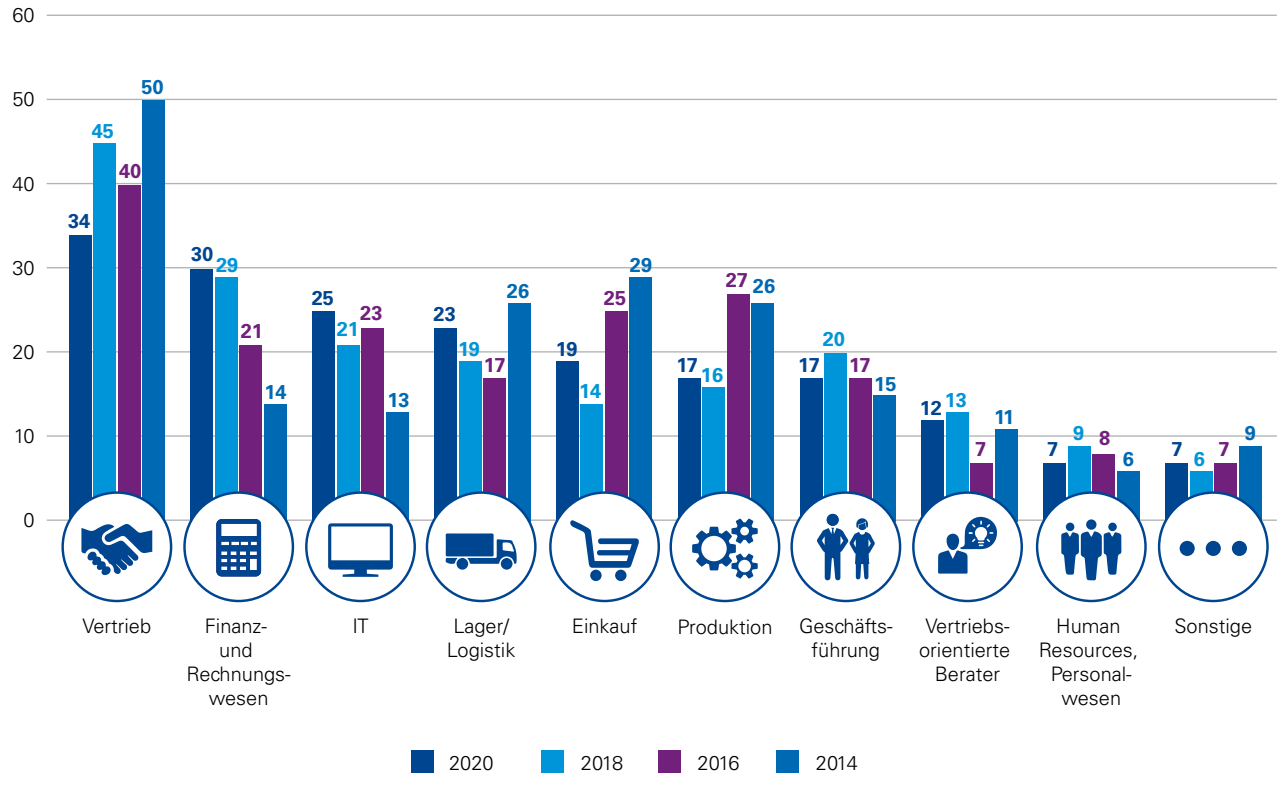
Einen aufschlussreichen Blick hinter die Kulissen bieten die Antworten auf die Frage nach den internen Tätern: Insgesamt wurde mehr als jedes vierte der allein durch interne Täter verübten Delikte von Mitgliedern der Managementebene begangen (28 Prozent) – davon 8 Prozent durch Mitglieder des Top-Managements.

Betrachtet man die Delikte im Einzelnen, zeigt sich, dass hinter Verstößen gegen das Kartellrecht (13 Prozent) oder der Manipulation jahresabschlussrelevanter Informationen (14 Prozent) häufig Personen aus dem Top-Management stehen. Letzteres Delikt (43 Prozent) sowie auch Korruption (35 Prozent) werden jedoch überwiegend von Mitarbeitern der mittleren Managementebene verübt.

1.5 Bereichsbezogene Betroffenheit

Wie schon die Vorgängerstudie zeigte, stellt der Vertrieb den am häufigsten von Wirtschaftskriminalität betroffenen Unternehmensbereich dar, doch ist hier ein nennenswerter Rückgang zu verzeichnen: Von 45 Prozent im Jahr 2018 auf 34 Prozent in der diesjährigen Studie. Damit ist dort die Abweichung mit Abstand am größten. Die Betroffenheit der übrigen Bereiche unterscheidet sich im Vergleich zu der Studie aus 2018 lediglich um maximal 5 Prozentpunkte.

Abbildung 6: Betroffene Bereiche im Jahresvergleich



Quelle: KPMG, Deutschland, 2020

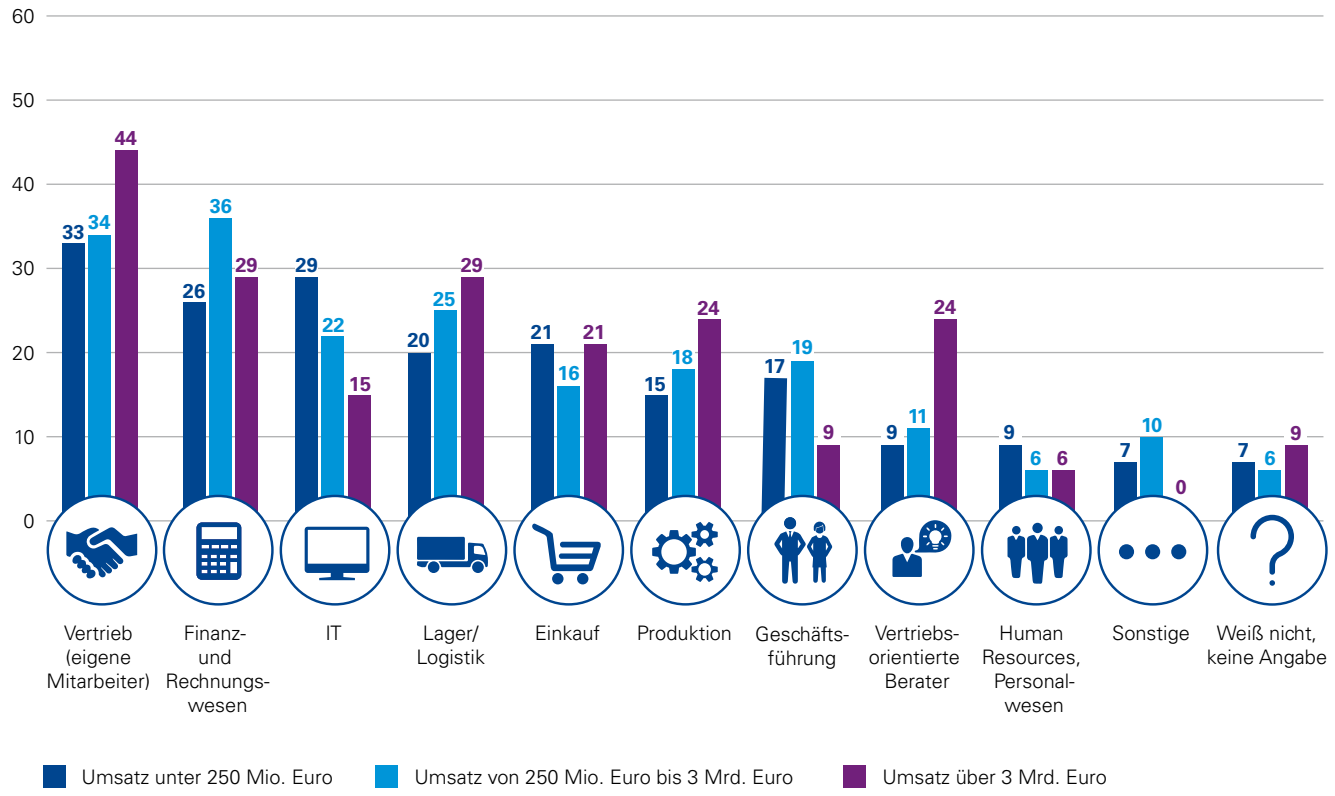
Angaben in Prozent

Der Trend der vorangegangenen Studien, wonach das Finanz- und Rechnungswesen zunehmend von Wirtschaftskriminalität betroffen war, setzt sich in diesem Jahr fort, auch wenn der Anstieg nun lediglich bei einem Prozentpunkt liegt. Dieser Bereich ist nach dem Vertrieb (34 Prozent) der am meisten betroffene (30 Prozent). Den prozentual größten Zuwachs verzeichnete der Bereich Einkauf (von 14 auf 19 Prozent), wobei dieser Anstieg vor allem auf die Betroffenheit dieses Bereichs bei Handelsunternehmen zurückzuführen ist, die sich nahezu verdoppelt hat (von 14 auf 29 Prozent).

Bei einem näheren Blick auf die verschiedenen Unternehmensgrößen (nach Umsatz) zeigt sich vor allem bei kleineren Unternehmen eine positive Entwicklung. Hier ist im Vergleich zu den Angaben in der Studie des Jahres 2018 in vielen Bereichen eine rückläufige Betroffenheit zu verzeichnen: Waren in der vorherigen Studie noch sieben der neun untersuchten Unternehmensbereiche zu mindestens 20 Prozent betroffen, sind es in diesem Jahr nur noch fünf.

Große Unternehmen benennen zumeist den Vertrieb als Ausgangspunkt wirtschaftskrimineller Handlungen (2020: 44 Prozent; 2018: 39 Prozent), wohingegen bei mittleren Unternehmen am häufigsten das Finanz- und Rechnungswesen im Fokus steht (2020: 36 Prozent; 2018: 29 Prozent).

Abbildung 7: Betroffene Bereiche nach Umsatz



Quelle: KPMG, Deutschland, 2020

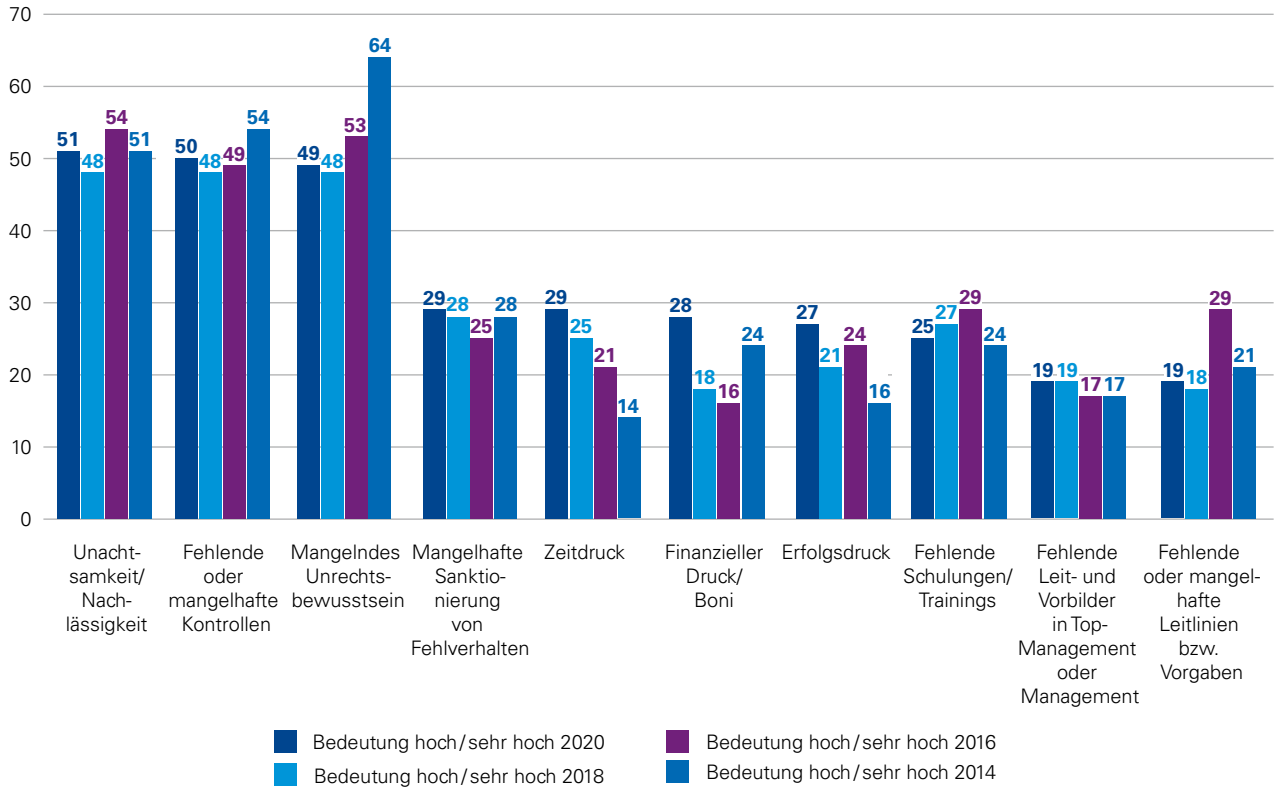
Angaben in Prozent

1.6 Risikofaktoren

Unachtsamkeit oder auch Nachlässigkeit ist für Unternehmen die bedeutsamste Ursache für die Begehung von wirtschaftskriminellen Handlungen, dicht gefolgt von fehlenden oder mangelhaften Kontrollen sowie mangelndem Unrechtsbewusstsein. Dies zeigte sich bereits in der Studie aus 2018, hat sich seither allerdings sogar noch verstärkt.

Grundsätzlich ist zu konstatieren: Je größer das Unternehmen (nach Mitarbeiterzahl), desto häufiger sehen diese Unternehmen die einzelnen Faktoren als risikobehaftet an. Demnach ist der Faktor Mensch für die Bewertung der Risikofaktoren ausschlaggebend.

Abbildung 8: Risikofaktoren für Begehung einer wirtschaftskriminellen Handlung



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Betrachtet man die Faktoren Zeitdruck (2020: 29 Prozent; 2018: 25 Prozent; 2016: 21 Prozent) sowie finanzieller Druck (28, 18 und 16 Prozent) über die Jahre hinweg, zeigt sich: Ihre Bedeutung für das Begehen von Wirtschaftskriminalität hat in der Gesamtheit der befragten Unternehmen konstant zugenommen. Insbesondere gilt dies für den finanziellen Aspekt, der im Vergleich zur vorangegangenen Studie eine Zunahme um 10 Prozentpunkte erfahren hat. Hier ließe sich die Frage vertiefen, ob sich Unternehmen einem erhöhten Leistungsdruck ausgesetzt sehen, der dazu verleitet, Ziele unter Inkaufnahme von Regelverstößen zu erreichen.

Mehr als jedes vierte Unternehmen (29 Prozent) sieht ein Risiko darin, dass Fehlverhalten mangelhaft sanktioniert wird. Als riskant bezeichneten diesen Aspekt 2018 insbesondere kleine Unternehmen (42 Prozent), jedoch ist hier ein deutlicher Rückgang zu verzeichnen (2020: 23 Prozent). Dies ist insofern überraschend, als die weiteren Studienergebnisse zeigen, dass kleine Unternehmen sehr wohl weniger Sanktionsmaßnahmen ergriffen haben und dies auch häufiger als Versäumnis bezeichnen. Unabhängig von der Unternehmensgröße jedoch sollte die abschreckende Wirkung von Sanktionen nicht unbeachtet bleiben, denn mit angemessenen Sanktionsmechanismen lässt sich der Toleranz in Bezug auf Fehlverhalten entgegenwirken.

» Vertrauen ist gut, Kontrolle besser? Für jedes zweite Unternehmen sind fehlende oder mangelhafte Kontrollen ein Risikofaktor für die Begehung wirtschaftskrimineller Handlungen. Ein gesunder Mittelweg kann zielführend sein. «

» Unter Druck entstehen Diamanten, heißt es. Dies gilt jedoch nicht für eine ordentliche Unternehmenskultur. Immer häufiger liegt in ihm ein Risikofaktor hinsichtlich wirtschaftskrimineller Handlungen. «

Drei von vier Unternehmen messen dem Fehlen von Schulungen oder Trainings eine geringe Bedeutung hinsichtlich der Vermeidung von Wirtschaftskriminalität bei. Dazu passt, dass nur drei von fünf Unternehmen angaben, Schulungen durchzuführen. Hier sei allerdings angemerkt: Sinn und Zweck von Schulungen zur Vermeidung von Wirtschaftskriminalität sollten stärker ins Bewusstsein rücken. Schließlich handelt es sich dabei um Maßnahmen, die vergleichsweise einfach umzusetzen sind und insbesondere den Faktoren mangelndes Unrechtsbewusstsein wie auch Unachtsamkeit und Nachlässigkeit gezielt entgegenwirken können, also genau den Aspekten, die jeder zweite Befragte als erhebliche Risikofaktoren einordnet.

Nicht vorhandene Leit- und Vorbilder im Management beziehungsweise Top-Management sowie fehlende oder mangelhafte Leitlinien beziehungsweise Vorgaben hält nur einer von fünf Befragten für besonders problematisch. Insbesondere große Unternehmen, gemessen an ihrem erzielten Umsatz, bemängeln in der diesjährigen Studie das Fehlen von Leit- und Vorbildern auf Managementebene (29 Prozent), was gegenüber 2018 einen Anstieg von 15 Prozentpunkten bedeutet und ein Defizit hinsichtlich des „Tone at the Top" vermuten lässt.

Wer den Risiken trotzen will, braucht eine starke Basis

2. Umgang mit Wirtschaftskriminalität in der deutschen Wirtschaft

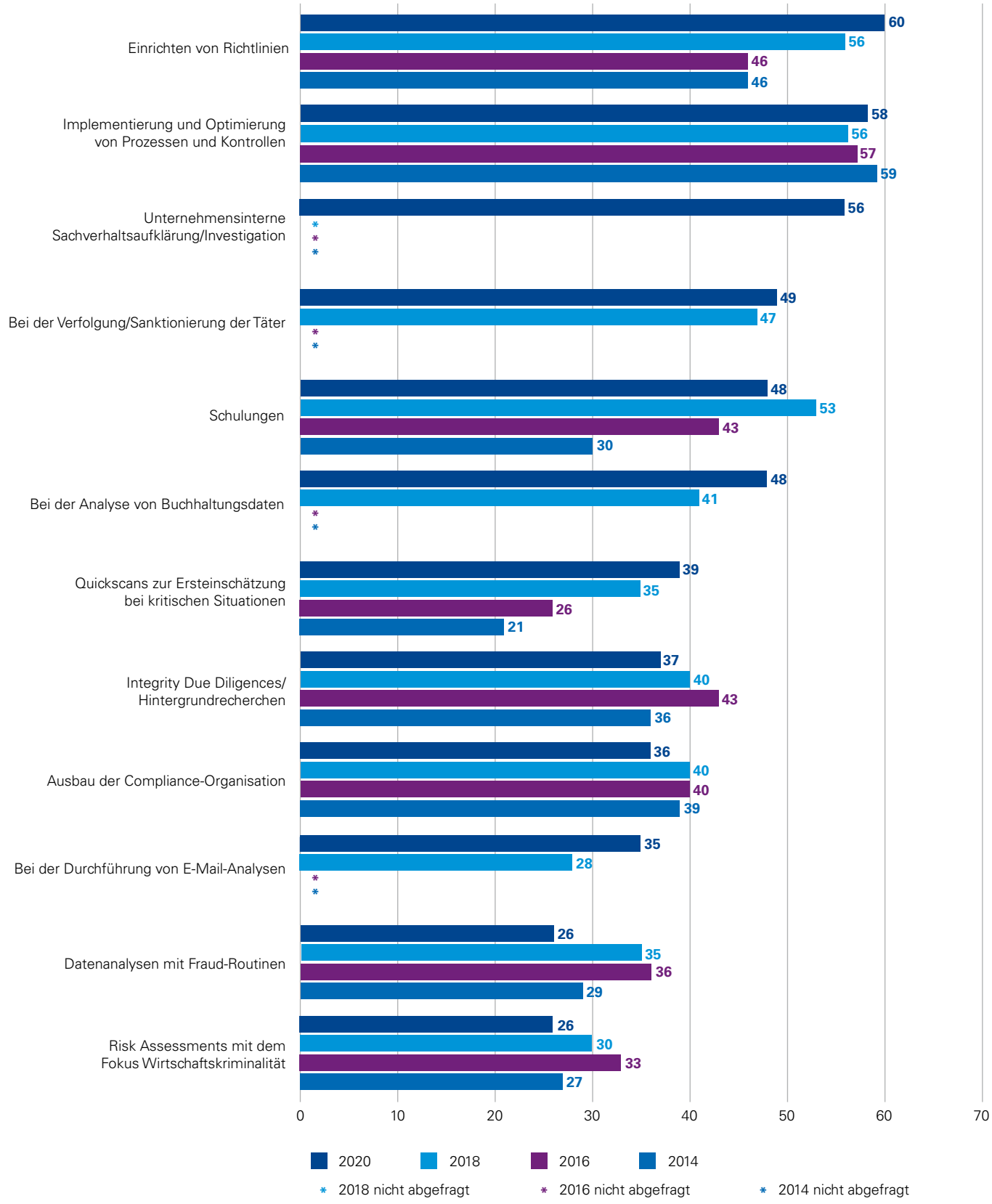
Die Tendenz eines präventiven Ansatzes zur Vermeidung von Wirtschaftskriminalität ist weiterhin erkennbar. Externe Unterstützung im Umgang mit wirtschaftskriminellen Handlungen ist bereits bei der Mehrheit der Unternehmen üblich oder zumindest beabsichtigt.

2.1 Externe Unterstützung beim Umgang mit Wirtschaftskriminalität

Um die mit Wirtschaftskriminalität einhergehenden Herausforderungen bewältigen zu können, reichen interne Mittel allein oftmals nicht aus. Der Trend, auf externe Unterstützung zurückzugreifen, wird von den diesjährigen Befragungsergebnissen bestätigt.

Dies gilt vor allem für das Einrichten von Richtlinien (2020: 60 Prozent, 2018: 56 Prozent), die Implementierung und Optimierung von Prozessen und Kontrollen (2020: 58 Prozent, 2018: 56 Prozent) sowie die unternehmensinterne Sachverhaltsaufklärung beziehungsweise Investigation (2020: 56 Prozent – erstmals als Antwortmöglichkeit aufgeführt). Unterstützung in Form von systemseitigen und prozessbezogenen Maßnahmen macht erneut den Großteil der in Anspruch genommenen externen Dienstleistungen aus.

Abbildung 9: Externe Unterstützung beim Umgang mit wirtschaftskriminellen Handlungen[1]



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

[1] Die Antwortmöglichkeiten „Bei der Verfolgung/Sanktionierung der Täter", „Bei der Analyse von Buchhaltungsdaten" und „Bei der Durchführung von E-Mail-Analysen" wurden erstmals in der Studie aus 2018 aufgeführt, die Antwortmöglichkeit „Unternehmensinterne Sachverhaltsaufklärung/Investigation" erstmals in der diesjährigen Studie.

» Wirtschaftskriminalität ist nicht immer allein mit internen Mitteln zu bewältigen. Unterstützungsleistungen Dritter können einen wertvollen Beitrag im Umgang mit wirtschaftskriminellen Handlungen leisten. «

Eine Zunahme der externen Unterstützung seit 2018 zeigt sich insbesondere auch bei der Analyse von E-Mails (35 gegenüber 28 Prozent) sowie Analyse von Buchhaltungsdaten (48 gegenüber 41 Prozent). Vor allem kleine Unternehmen (nach Umsatz) setzen bei der Analyse von E-Mails vermehrt auf externe Unterstützung (36 Prozent). Dies könnte damit zu erklären sein, dass dies sowohl hoch spezialisierte Technik als auch zeitliche und personelle Ressourcen erfordert, die bei kleinen Unternehmen eventuell nicht im selben Umfang vorhanden sind wie bei größeren.

Große Unternehmen vertrauen vor allem bei der Durchführung von Schulungen (62 Prozent) sowie beim Ausbau der Compliance-Organisation (51 Prozent) auf externe Fachleute. Mittlere Unternehmen (nach Umsatz) hingegen nehmen überdurchschnittlich häufig bei der Einrichtung von Richtlinien (63 Prozent), der unternehmensinternen Sachverhaltsaufklärung (63 Prozent), der Implementierung und Optimierung von Prozessen und Kontrollen (62 Prozent) und der Verfolgung beziehungsweise Sanktionierung von Tätern (57 Prozent) externe Unterstützung in Anspruch.

In Sachen externe Unterstützung bei Schulungen zeigt sich ein erheblicher Unterschied zwischen Unternehmen, die von kriminellen Vorfällen betroffen waren, und solchen, bei denen dies nicht der Fall ist: Erstere bauen zu 61 Prozent (im gleichen Umfang wie 2018) auf externe Unterstützung, bei Letzteren sind es lediglich etwa zwei von fünf (43 Prozent). Vor allem große Unternehmen sehen in Schulungen durch externe Dienstleister ein großes Potenzial (62 Prozent; Durchschnitt: 48 Prozent).

Auch bei der Anwendung von Quickscans zur Ersteinschätzung kritischer Situationen ziehen bereits betroffene Unternehmen deutlich häufiger externe Expertise hinzu (jedes zweite Unternehmen), während nur jedes dritte der anderen Gruppe solche Unterstützung in Anspruch nimmt.

Risk Assessments bilden den Grundstein für die Einrichtung wirksamer Schutzvorkehrungen. Hier kann externes Know-how dabei helfen, das Risikobewusstsein zu schärfen – auch im Sinne eines Benchmarkings.

Bemerkenswert ist, dass das Hinzuziehen externer Unterstützung bei Datenanalysen mit Fraud-Routinen um 9 Prozentpunkte zurückgegangen ist – nur noch etwas mehr als jedes vierte Unternehmen (26 Prozent) nahm hierbei die Hilfe Dritter in Anspruch. Während in diesem Bereich etwa jedes zweite große Unternehmen (nach Umsatz) auf externe Expertise zurückgreift, ist es bei kleinen Unternehmen nur jedes fünfte.

Betrachtet man diese Ergebnisse im Zusammenhang mit der Einschätzung des eigenen Schutzniveaus, zeigt sich, dass Unternehmen, die sich selbst als schlecht geschützt ansehen, gleichwohl relativ selten externe Unterstützung hinzuziehen (34 Prozent). Bei sehr gut oder gut geschützten Unternehmen beläuft sich dieser Wert auf 45 Prozent. Insbesondere gilt dies bei der Verfolgung beziehungsweise Sanktionierung von Tätern: Hier vertrauen Unternehmen mit sehr gutem Schutzniveau in 51 Prozent der Fälle auf die Hilfe von Externen, Unternehmen mit einem schlechten Schutzniveau allerdings in lediglich 37 Prozent der Fälle.

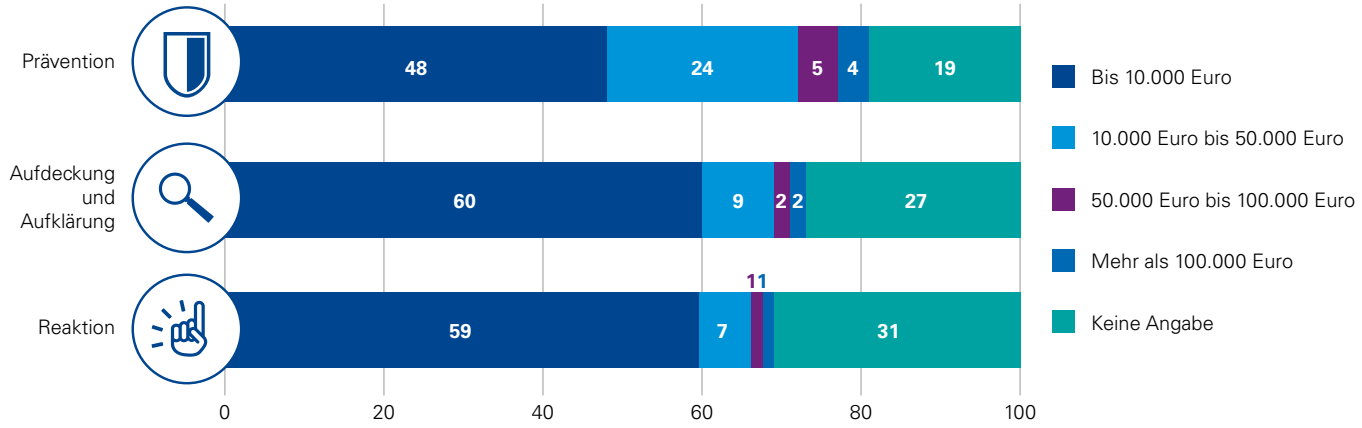
» Dass einer unternehmensinternen Sachverhaltsaufklärung beziehungsweise Investigation eine enorm große Bedeutung zukommt, bestätigen nicht nur die Ergebnisse der Studie. Vor allem unter Berücksichtigung des kommenden Verbandssanktionengesetzes wird hier das zukünftige Vorgehen der Unternehmen spannend zu beobachten sein. «

2.2 Investitionsbereitschaft

48 Prozent der Befragten geben an, in den zurückliegenden zwei Jahren lediglich bis zu 10.000 Euro für externe Unterstützung bei der Umsetzung präventiver Maßnahmen ausgegeben zu haben. Im Rahmen der Aufdeckung und Aufklärung sowie der Reaktion auf wirtschaftskriminelle Sachverhalte wurde eine solche Summe um einiges häufiger in externe Unterstützung investiert (59 und 60 Prozent). Deutlich größere Beträge – 50.000 Euro und mehr – wurden am ehesten für Unterstützung bei der Implementierung ordnungsgemäßer Präventionsmaßnahmen ausgegeben: 9 Prozent der Unternehmen geben dies zu Protokoll.

» Branchenübergreifend wurden vor allem in die Phase der Prävention vergleichsweise große Beträge investiert. Gute Präventionsmaßnahmen stellen für viele Unternehmen den ökonomisch sinnvollsten Weg zum Schutz vor Wirtschaftskriminalität und deren Folgen dar. «

Abbildung 10: Investitionen in den vergangenen zwei Jahren



Quelle: KPMG, Deutschland, 2020; Rundungsdifferenzen möglich

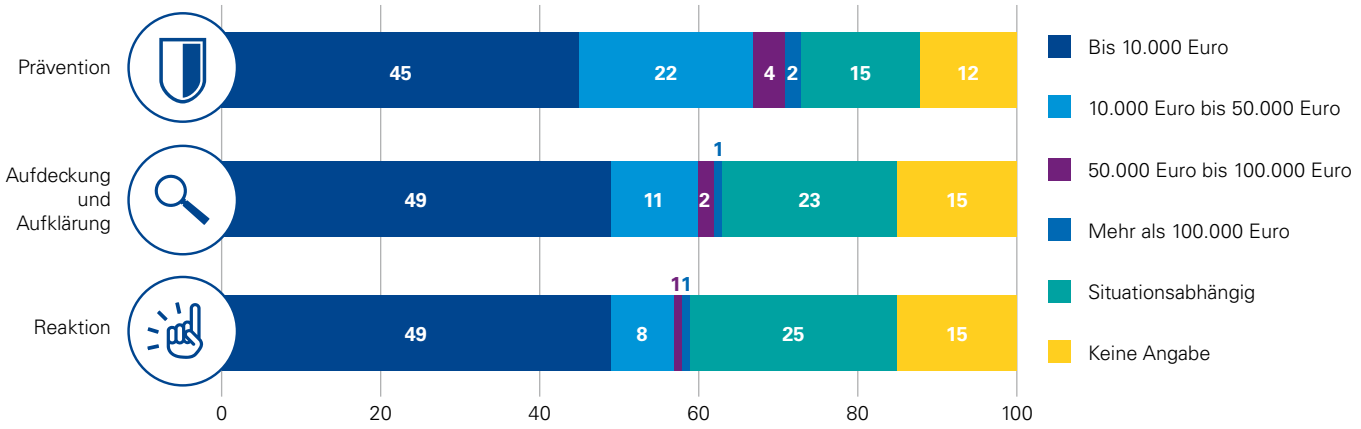
Angaben in Prozent

Ein Blick auf die grafische Darstellung (Abbildung 10) macht jedoch auch deutlich: Ein beträchtlicher Anteil der Befragten hat (erneut) keine Angaben zu den getätigten Investitionen gemacht, insbesondere bei den Aspekten Aufdeckung und Aufklärung sowie Reaktion. Zudem ist der Anteil im Vergleich zur Studie von 2018 um jeweils 4 Prozentpunkte gestiegen – bei Aufdeckung und Aufklärung auf 27 und bei Reaktion auf 31 Prozent. Eine solche Unsicherheit bezüglich der tatsächlich aufgewendeten Beträge birgt das grundlegende Risiko, dass Unternehmen nicht angemessen evaluieren können, welche Maßnahmen sich nicht nur als effektiv, sondern auch als kosteneffizient erwiesen haben oder erweisen. Vor allem unter dem Gesichtspunkt einer ökonomischen Unternehmensführung sind diese Kenntnisse jedoch sinnvoll und notwendig.

Die bereits 2018 festgestellte Zunahme eines präventiven Ansatzes lässt sich durch fast identische Angaben der Befragten erneut bestätigen. Mit einer solchen Herangehensweise lassen sich positive Effekte dahingehend erzielen, dass einerseits die Häufigkeit von Vorfällen reduziert und andererseits die aufgrund von Wirtschaftskriminalität entstehenden Schäden minimiert werden können. Somit bestätigt ein präventiv wirkender Prozess den ökonomischen Grundgedanken der Unternehmen. Die Anforderungen, die mit dem geplanten Verbandssanktionengesetz künftig auf Unternehmen zukommen können, unterstreichen diesen Gedanken. Bei der Abwägung des „Ob" von Investitionen sollten Unternehmen künftig berücksichtigen, dass das Gesetz (nach dem jetzigen Entwurfsstand) präventive Maßnahmen sanktionsmildernd bewertet und unternehmensinterne Ermittlungen mit einer Verminderung des Höchstmaßes der Sanktion um die Hälfte honoriert. Mit diesem Anreiz unterstreicht auch der Gesetzgeber die Wichtigkeit solcher Prozesse in und für Unternehmen.

Trotz dieses zusätzlichen Arguments für eine Stärkung der Präventionsmaßnahmen können oder wollen sich mehr Unternehmen als bisher bezüglich der Höhe der Investitionen in den kommenden zwei Jahren nicht festlegen. So geben 14 Prozent aller Befragten an, nicht zu wissen, wie hoch die geplanten Investitionen ausfallen werden, 21 Prozent wollen diese lediglich situationsabhängig tätigen. Während in der vorherigen Studie lediglich 7 Prozent der Unternehmen angaben, eine Investition in präventive Maßnahmen situationsabhängig zu tätigen, stieg der Anteil in der diesjährigen Studie auf 15 Prozent an. Auch für die übrigen Phasen wird vermehrt angegeben, dass dort nur situationsabhängig investiert werden soll – mit einem Anstieg von 18 auf 23 Prozent (Aufdeckung und Aufklärung) beziehungsweise von 20 auf 25 Prozent (Reaktion). Lassen sich aufgrund der generellen Unvorhersehbarkeit wirtschaftskrimineller Handlungen bei den beiden letztgenannten Phasen die tatsächlich erforderlichen Investitionsvolumina wahrlich schwer im Voraus beziffern, verhält es sich für Investitionen in die Prävention grundsätzlich umgekehrt: Gerade in diesem Bereich könnte ein klar definierter und somit bezifferbarer Plan verfolgt werden, weshalb der Anstieg der situationsabhängigen Investitionsbereitschaft hier überrascht.

Abbildung 11: Geplante Investitionen in den nächsten zwei Jahren



Quelle: KPMG, Deutschland, 2020; Rundungsdifferenzen möglich

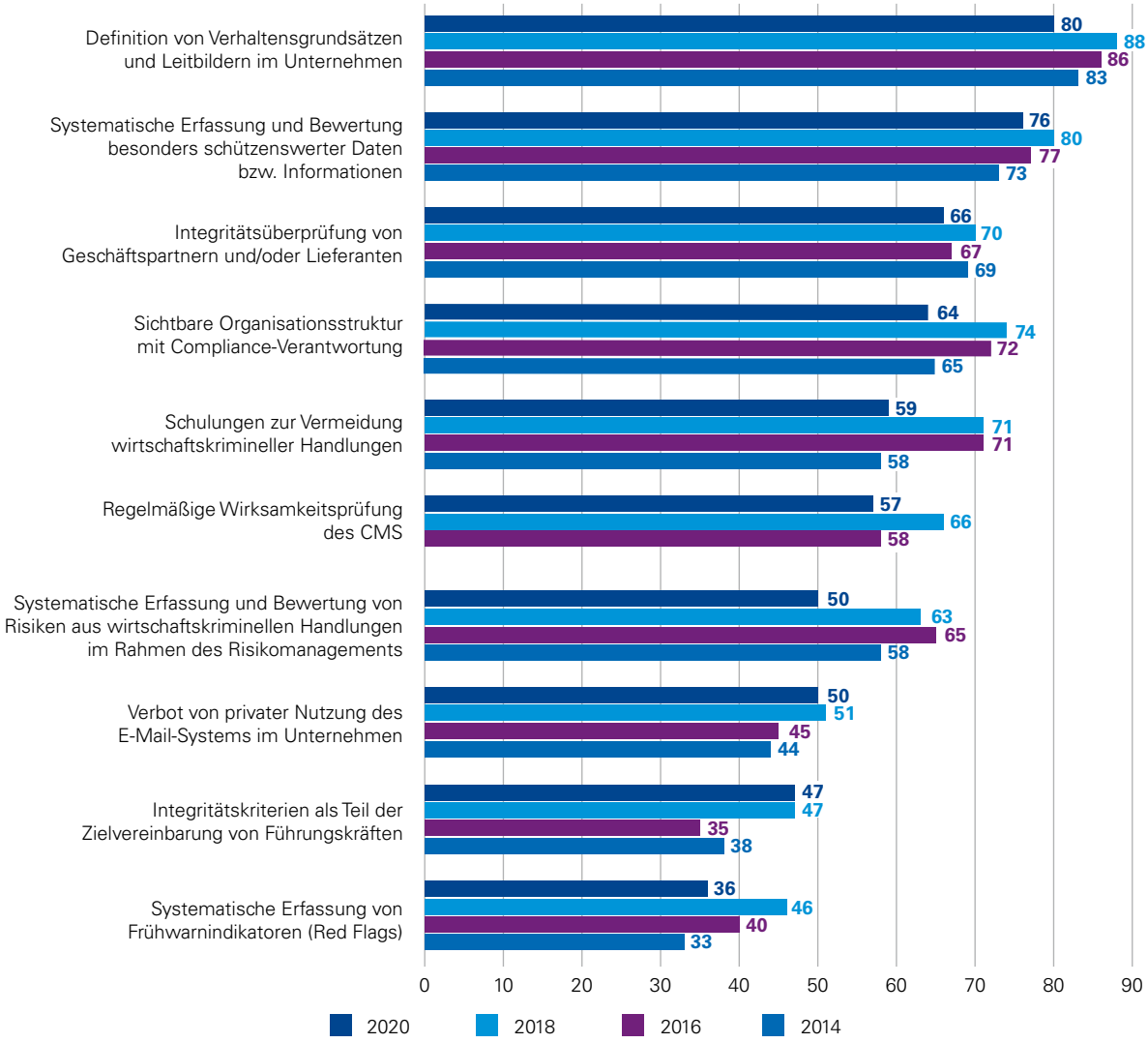
Angaben in Prozent

2.3 Präventionsmaßnahmen

Wie in der vorausgegangenen Studie sind auch in diesem Jahr die Definition von Verhaltensgrundsätzen und Leitbildern im Unternehmen (80 Prozent) sowie die systematische Erfassung und Bewertung besonders schützenswerter Daten beziehungsweise Informationen (76 Prozent) die meistgenannten Präventionsmaßnahmen. Einhergehend damit, dass andere abgefragte Maßnahmen wie die Durchführung von Schulungen und das Bestehen einer sichtbaren Organisationsstruktur in der diesjährigen Studie seltener genannt werden als zuvor, rückt nun die Integritätsüberprüfung von Geschäftspartnern oder auch Lieferanten auf Platz drei der gewählten Präventionsmaßnahmen vor (66 Prozent). Dies unterstreicht die zunehmende Bedeutung und auch Notwendigkeit eines Risikomanagements im Hinblick auf Drittparteien (das sogenannte Third Party Risk Management), denn es gilt zu bedenken: Mangelnde Kenntnis und unzureichende Kontrollen derartiger Akteure können unter anderem zu einer Einschränkung der Leistungsfähigkeit, zu Reputationsschäden und auch zu finanziellen Einbußen führen. Dies gilt insbesondere für global agierende Unternehmen oder solche mit einer hohen Abhängigkeit von komplexen Lieferketten. Vor allem große Unternehmen – gemessen an ihrem Umsatz – sehen hierin eine effektive Präventionsmaßnahme (große Unternehmen: 77 Prozent; kleine Unternehmen: 59 Prozent).

Grundsätzlich ist festzuhalten, dass im Vergleich zu der vorangegangenen Studie die Bandbreite der genutzten Präventionsmaßnahmen seitens der Unternehmen rückläufig ist.

Abbildung 12: Präventive Maßnahmen in den Unternehmen



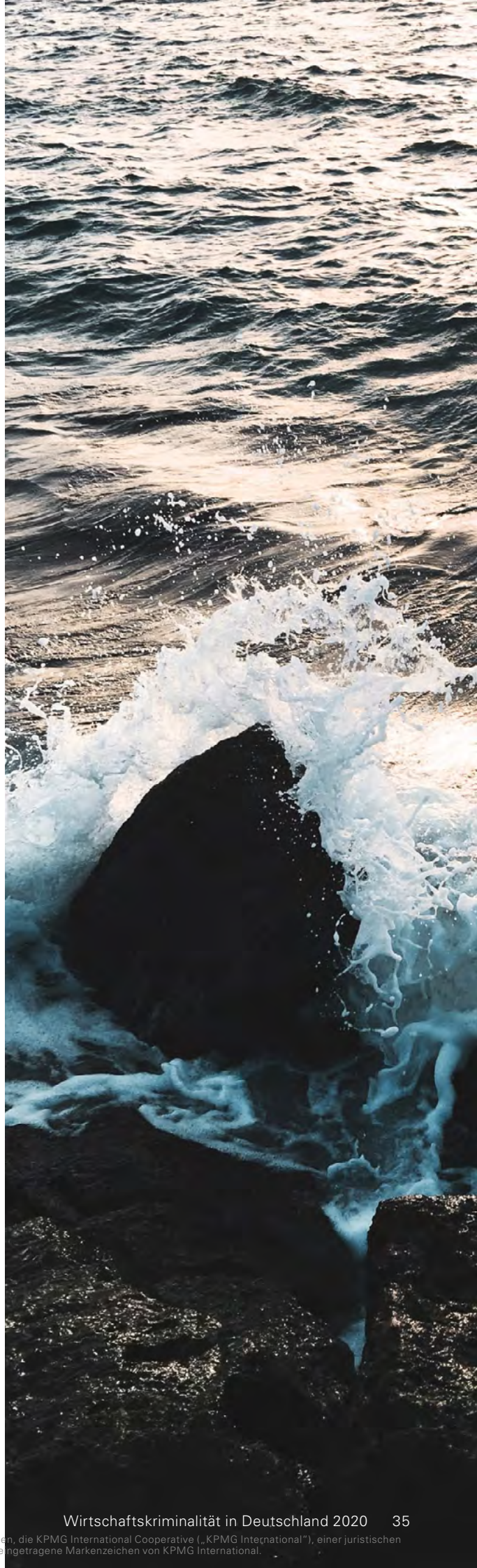
Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Nichtsdestotrotz zeigt sich erneut, dass bereits betroffene Unternehmen eine größere Bandbreite von Präventionsmaßnahmen implementiert haben als diejenigen, die bisher nicht von Wirtschaftskriminalität betroffen waren. Auffällige Unterschiede bestehen insbesondere bei der Durchführung von Schulungen (betroffen: 71 Prozent; nicht betroffen: 53 Prozent) sowie der systematischen Erfassung und Bewertung von Risiken aus wirtschaftskriminellen Handlungen (58 gegenüber 45 Prozent). Diesen Zahlen zufolge scheinen betroffene Unternehmen auf vergangene Vorfälle reagiert und entsprechende Gegenmaßnahmen ergriffen zu haben.

Hinsichtlich der systematischen Erfassung und Bewertung von Risiken, die mit wirtschaftskriminellen Handlungen einhergehen, ist ein Rückgang gegenüber 2018 festzustellen. Gaben seinerzeit noch nahezu zwei Drittel aller Befragten (63 Prozent) an, ein System zur Erfassung und Bewertung implementiert zu haben, sind es nunmehr lediglich 50 Prozent. Vor allem Unternehmen mit weniger als 100 Mitarbeitern nutzen eine solche systemseitige Erfassung vergleichsweise selten (36 Prozent).

Ein ähnlicher Rückgang zeigt sich auch im Hinblick auf die Durchführung von Schulungen zur Vermeidung von wirtschaftskriminellen Handlungen (von 71 auf 59 Prozent). Wie bereits erläutert, adressieren Schulungen die in dieser Studie meistgenannten Risikofaktoren – mangelndes Unrechtsbewusstsein, Unachtsamkeit und Nachlässigkeit – und stellen somit eine essenzielle Maßnahme dar. Dabei divergieren die Zahlen zwischen kleinen und großen Unternehmen erheblich (48 zu 93 Prozent). Das gleiche Bild ergibt sich im Hinblick auf das Bestehen einer sichtbaren Organisationsstruktur mit Compliance-Verantwortung (kleine Unternehmen, gemessen am Umsatz: 53 Prozent; große: 91 Prozent). Und auch für die meisten anderen Präventionsmaßnahmen gilt dieser Befund – wenn auch in abgeschwächtem Maß –, was darauf zurückzuführen sein könnte, dass größere Unternehmen mehr finanzielle oder personelle Ressourcen zur Verfügung haben als kleine.



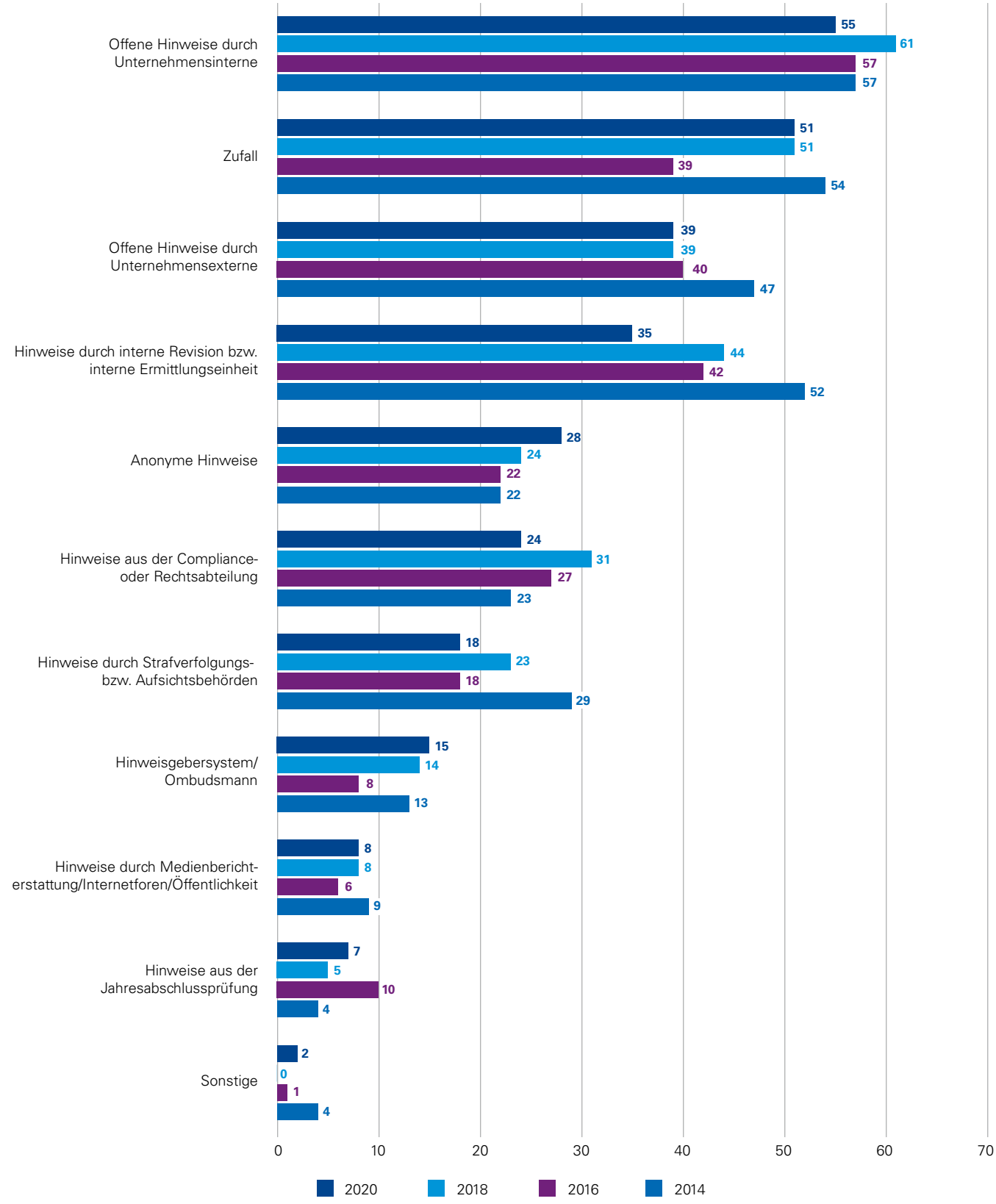
Unternehmen, die ihr Schutzniveau als sehr gut beurteilen, sind bei präventiven Maßnahmen gegenüber schlecht geschützten Unternehmen wesentlich weiter. Eine auffallend große Diskrepanz zeigt sich hinsichtlich der Integritätsprüfung von Geschäftspartnern und Lieferanten. Während Unternehmen mit einem guten Schutz diese Maßnahme zu 68 Prozent umgesetzt haben, geben dies gerade einmal 49 Prozent der schlecht geschützten Unternehmen an. Vor allem angesichts anstehender rechtlicher Neuerungen – hier sei beispielsweise an das in der Diskussion befindliche Gesetz zur Regelung von Lieferketten gedacht – könnte eine Überprüfung der Integrität in naher Zukunft allerdings erheblich an Bedeutung gewinnen.

2.4 Entdeckung der Handlung

Offene Hinweise durch Unternehmensinterne sind nach wie vor die meistgenannte Antwort auf die Frage, wie wirtschaftskriminelle Handlungen entdeckt werden (55 Prozent). In knapp zwei von fünf Fällen stammen die Hinweise aber auch von Externen.

In der diesjährigen Studie zeigt sich erneut, dass die Bedeutung des Zufalls nicht unterschätzt werden darf, denn bei etwas mehr als der Hälfte der Unternehmen sind Vorfälle lediglich durch eine günstige Fügung ans Licht gekommen (51 Prozent, wie schon 2018). Dieser Umstand verdeutlicht, dass Handlungsbedarf besteht, um nicht von zufälligen Erkenntnissen abhängig zu sein, sondern die Entdeckung und Aufklärung wirtschaftskrimineller Sachverhalte systematisch selbst in der Hand zu haben. Bei kleinen Unternehmen (nach Umsatz) kam es in letzter Zeit im Übrigen seltener als bisher zu einer zufälligen Aufdeckung (2020: 45 Prozent, 2018: 50 Prozent).

Abbildung 13: Entdeckung der Handlung



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Sowohl Hinweise aus der internen Revision oder auch internen Ermittlungseinheiten (2020: 35 Prozent, 2018: 44 Prozent) als auch Meldungen durch die Compliance- oder Rechtsabteilung (2020: 24 Prozent, 2018: 31 Prozent) werden im Rahmen der aktuellen Befragung seltener genannt als noch in der vorangegangenen Studie.

Bei etwas mehr als jedem vierten Unternehmen war ein anonymer Hinweis ausschlaggebend für die Entdeckung des betreffenden Vorfalls. Bei großen Unternehmen spielen anonyme Hinweise sogar eine deutlich größere Rolle (44 Prozent). Unter Verweis auf Änderungen rechtlicher Vorgaben wurde bereits 2018 angemerkt, dass Meldungen über Hinweisgebersysteme oder Ombudsmänner in Zukunft an Relevanz gewinnen dürften. Zu nennen ist diesbezüglich die EU-Hinweisgeberrichtlinie, in der die Ausgestaltung interner Meldekanäle detailliert beschrieben ist. Diese sollten so ausgestaltet sein, dass sie von dem Hinweisgeber gegenüber externen beziehungsweise öffentlichen Meldekanälen bevorzugt werden. Gelingt dies, können Unternehmen die weiteren Schritte aktiv steuern. Schon 2018 zeigte sich, dass vor allem große Unternehmen (gemessen am Umsatz) über ein Hinweisgebersystem verfügen. Und wie die Antworten erkennen lassen, werden solche Optionen durchaus genutzt: Zwei von fünf der „Großen" wurden auf diesen Kanälen auf wirtschaftskriminelle Handlungen aufmerksam gemacht (2018: 23 Prozent).

» Mit Blick auf die EU-Hinweisgeberrichtlinie bleibt abzuwarten, inwieweit Hinweise über Hinweisgebersysteme zukünftig eine prominentere Rolle bei der Entdeckung eines wirtschaftskriminellen Vorfalls einnehmen werden. «

Dass sich ein sehr gutes Schutzniveau der Unternehmen förderlich auf die Entdeckung von Wirtschaftskriminalität auswirkt, bestätigt sich in der diesjährigen Studie. So können mehr als zwei Drittel aller Verdachtsfälle bei Unternehmen mit einem sehr guten Schutz dank Hinweisen von Unternehmensinternen aufgedeckt werden (70 Prozent) und auch die Abhängigkeit von zufälligen Entdeckungen verliert an Gewicht (35 Prozent). Die Qualität des Schutzes hängt – dafür sprechen diese Erkenntnisse – folglich von der Einrichtung eines ordnungsgemäßen internen Meldesystems ab.

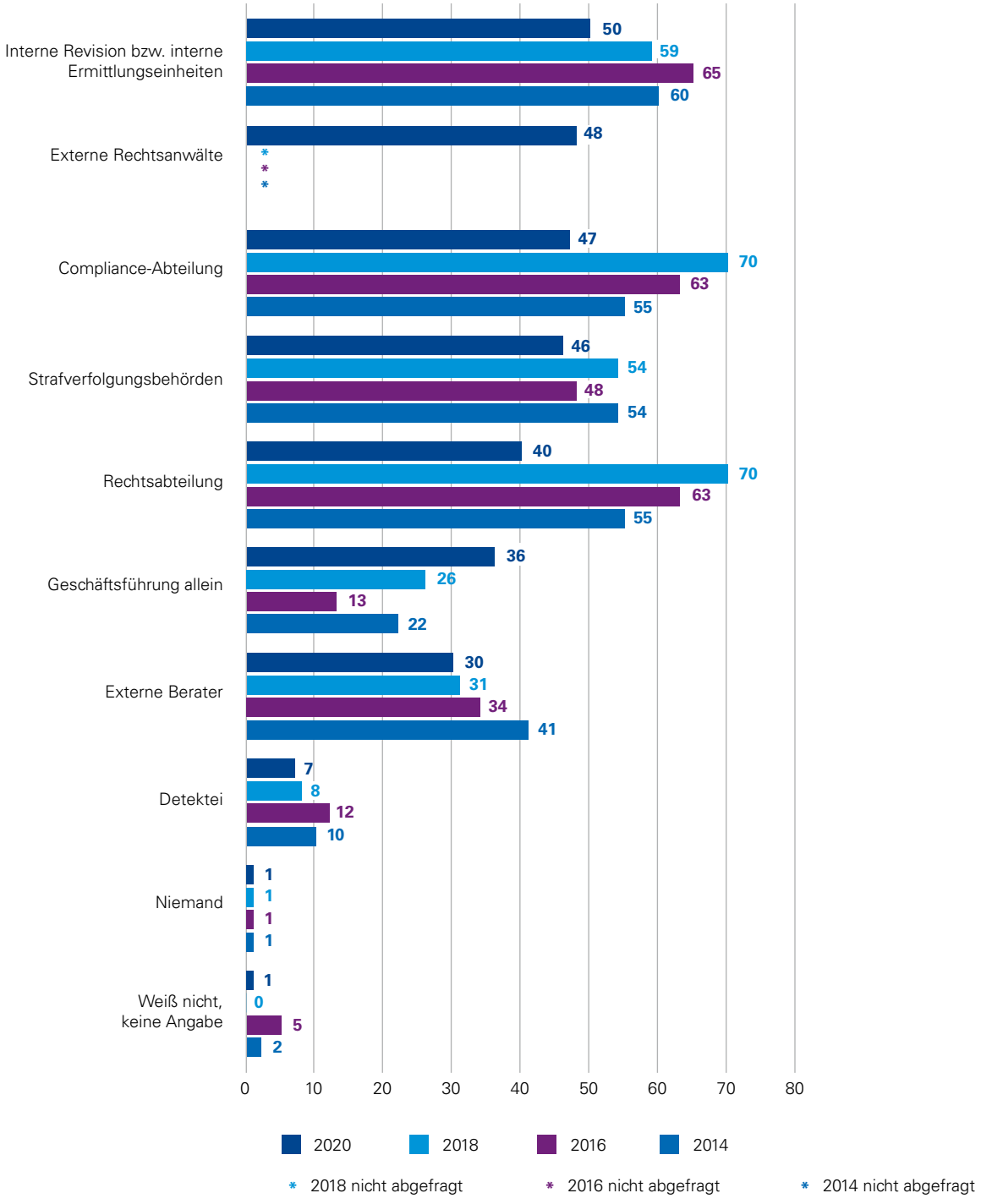
In jedem vierten Fall werden Unternehmen, die ihr Schutzniveau als schlecht einstufen, aufgrund von Hinweisen durch Strafverfolgungs- oder Aufsichtsbehörden auf wirtschaftskriminelle Handlungen innerhalb ihres Unternehmens aufmerksam.

2.5 Operative Aufklärung

Die operative Aufklärung wirtschaftskrimineller Sachverhalte wurde den vorangegangenen Studien zufolge zumeist internen Stellen überlassen, wohingegen externe Unterstützung von vergleichsweise geringer Bedeutung war. Laut der diesjährigen Befragung sind interne wie externe Stellen zu nahezu gleichen Teilen an der operativen Aufklärung beteiligt. Eine auffallend große Vakanz ergab sich lediglich hinsichtlich der Hinzuziehung von Detekteien (7 Prozent).

Unternehmen, die sich als sehr gut geschützt betrachten, nahmen vermehrt externe Unterstützung bei der operativen Aufklärung in Anspruch. So waren externe Rechtsanwälte in mehr als der Hälfte (55 Prozent; schlechtes Schutzniveau: 35 Prozent), andere externe Berater in etwa einem Drittel der Fälle an der Aufklärung beteiligt (30 Prozent; schlechtes Schutzniveau: 18 Prozent). Die Hinzuziehung von Detekteien oder die Aufklärung durch die Strafverfolgungsbehörden war seltener das Mittel der Wahl als noch in der Studie des Jahres 2018.

Abbildung 14: Operative Aufklärung[2]



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

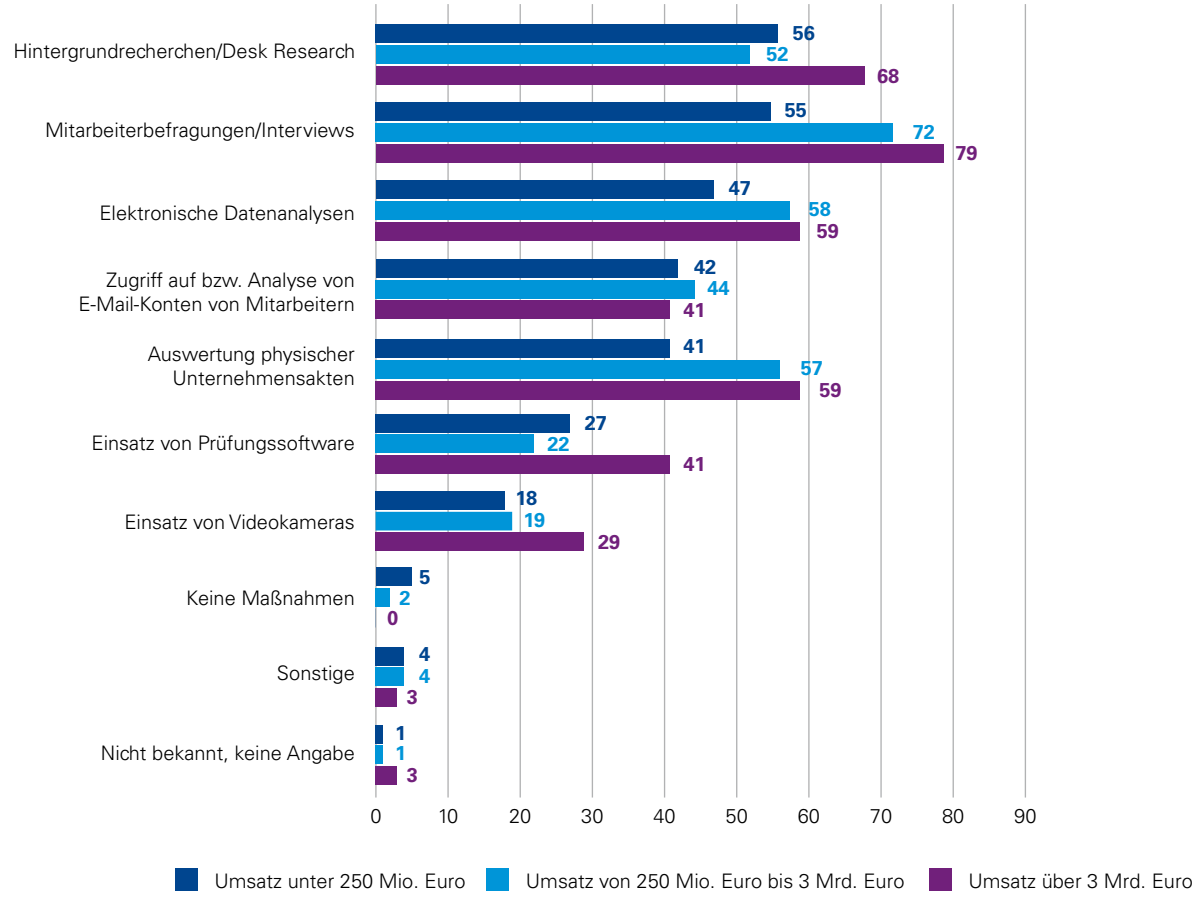
[2] In der diesjährigen Befragung wurde die bisher bestehende Antwortkategorie „Compliance, Legal" unterteilt in „Compliance-Abteilung" und „Rechtsabteilung". Die 2014er, 2016er und 2018er Angaben zu „Compliance, Legal" wurden in der diesjährigen Studie für beide neuen Kategorien verwendet. Es könnte hier hinsichtlich der Vergleichbarkeit zu Verzerrungen kommen. Zudem wurde in der diesjährigen Befragung erstmals die Antwortmöglichkeit „Externe Rechtsanwälte" aufgeführt, weshalb hier für die zurückliegenden Jahre kein Wert ermittelt worden ist.

Große Unternehmen (nach Umsatz) verfügen häufig über spezialisierte Abteilungen für unternehmensinterne Ermittlungen, was die Studienergebnisse belegen. So nennen diese Unternehmen die interne Revision (65 Prozent), die Rechtsabteilung (62 Prozent) sowie die Compliance-Abteilung (56 Prozent) wesentlich häufiger als Bestandteil der operativen Aufklärung, als dies bei kleinen Unternehmen der Fall ist (38, 25 und 28 Prozent). Diesen fehlt es möglicherweise an finanziellen oder personellen Ressourcen, um solche spezialisierten Abteilungen zu führen.

2.6 Aufklärungsmaßnahmen

Im Vergleich zu der Studie aus dem Jahr 2018 ergeben sich hinsichtlich der ergriffenen Maßnahmen zur Aufklärung entsprechender Sachverhalte lediglich geringfügige Abweichungen. Am häufigsten greifen die Unternehmen wie gehabt zu Mitarbeiterbefragungen (65 Prozent), Hintergrundrecherchen (56 Prozent), elektronischen Datenanalysen (53 Prozent) und Auswertungen physischer Unternehmensakten (50 Prozent).

Abbildung 15: Aufklärungsmaßnahmen



Quelle: KPMG, Deutschland, 2020

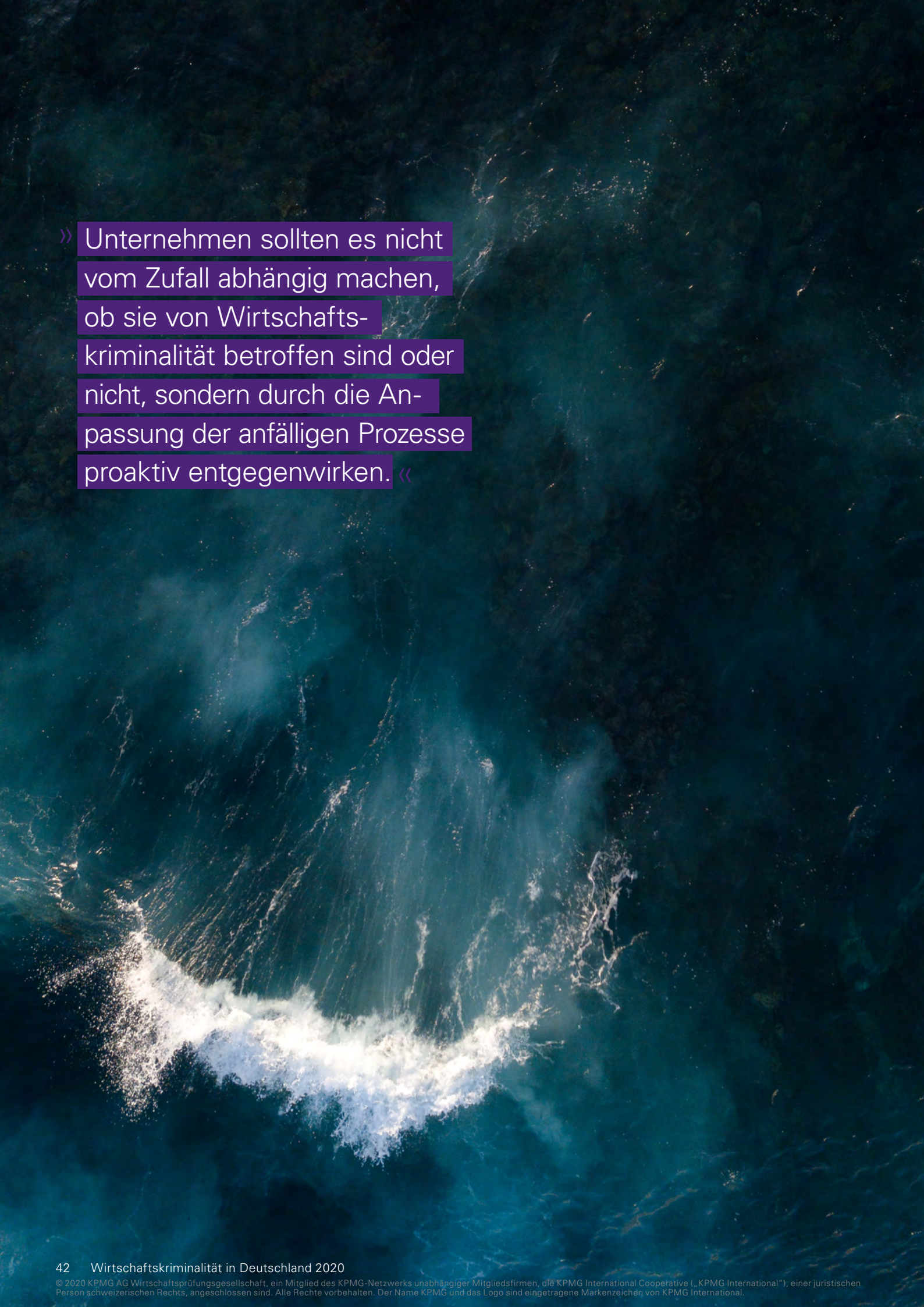
Angaben in Prozent

Der Trend, dass im Zuge der Digitalisierung immer häufiger auch auf digitale Aufklärungsmethoden vertraut wird, setzt sich in der diesjährigen Studie fort. So werden seltener physische Unternehmensakten untersucht, als es noch 2018 der Fall war (50 zu 59 Prozent). Im Gegenzug rücken bei der Aufklärung immer häufiger Analysen von E-Mail-Konten der Mitarbeiter in den Blick.

So gaben die befragten Unternehmen größenunabhängig an, vermehrt auf die Aufklärung mittels der Analyse von E-Mail-Konten der Mitarbeiter zurückzugreifen (2020: 43 Prozent; 2018: 35 Prozent). Bemerkenswerterweise zeigen sich bei den meisten anderen Maßnahmen allerdings nach wie vor Unterschiede zwischen den Größenklassen. Dies gilt insbesondere für Interviews und Mitarbeiterbefragungen: Während sie in kleinen Unternehmen in 55 Prozent der Fälle durchgeführt wurden, waren es bei mittleren Unternehmen 72 Prozent, bei großen Unternehmen sogar 79 Prozent.

Betrachtet man die Nutzung der Aufklärungsmaßnahmen im Verhältnis zum Schutzniveau des jeweiligen Unternehmens, fällt Folgendes auf: Diejenigen Unternehmen, die sich als sehr gut geschützt sehen, greifen zu vielfältigeren Maßnahmen als diejenigen, die sich selbst einen schlechten Schutz bescheinigen. So zum Beispiel bei Interviews (80 gegenüber 63 Prozent) und elektronischen Datenanalysen (65 gegenüber 60 Prozent), doch dies gilt ebenfalls für den Einsatz von Prüfungssoftware und Videokameras.

» Die richtige Wahl der Aufklärungsmaßnahmen ist wesentlicher Bestandteil eines ganzheitlichen Schutzniveaus. Ein sich ergänzendes Gerüst von Maßnahmen dient dazu, Vorfälle effektiv und umfassend aufklären zu können. «



» Unternehmen sollten es nicht vom Zufall abhängig machen, ob sie von Wirtschafts-kriminalität betroffen sind oder nicht, sondern durch die An-passung der anfälligen Prozesse proaktiv entgegenwirken. «

2.7 Maßnahmen nach der Aufklärung

Fast alle abgefragten Maßnahmen, mit denen sich auf wirtschaftskriminelle Handlungen reagieren ließe, werden in der diesjährigen Befragung seltener genannt als noch 2018. Ihre Gewichtung ähnelt allerdings sehr derjenigen von vor zwei Jahren. So sind die Veränderung der bestehenden Präventionsmaßnahmen (69 Prozent) sowie das Stellen einer Strafanzeige (58 Prozent) nach wie vor die am häufigsten genannten Folgemaßnahmen.

Auffällig ist, dass drei von vier Unternehmen, die ihr internes Schutzniveau als sehr gut bezeichnen, einen wirtschaftskriminellen Vorfall als Anlass sehen, die Sicherungsvorkehrungen zu überarbeiten und die internen Prozesse zu schärfen. Dies spricht für ein ausgeprägtes Risikobewusstsein innerhalb der Unternehmens- und Compliance-Kultur, das eine stetige Optimierung der eigenen Maßnahmen fördert. Schließlich steigert es die Wahrscheinlichkeit, dass weitere Vorfälle verhindert oder aber etwaige Schäden minimiert werden, wenn vorhandene Maßnahmen überdacht und gegebenenfalls angepasst werden.

Wie bereits in der 2018er Studie zu erkennen war, gehen große Unternehmen (nach Umsatz) nach der Aufklärung eines Vorfalls wesentlich strikter vor und ergreifen mehr Maßnahmen als kleine. Dies gilt insbesondere für personalbezogene Sanktionen, etwa Kündigungen (65 gegenüber 38 Prozent), Abmahnungen (56 gegenüber 34 Prozent) oder sonstige personelle Veränderungen (47 gegenüber 22 Prozent).

Des Weiteren lassen große Unternehmen eine wesentlich größere Bereitschaft erkennen, auch den Gang vor Gericht zu bestreiten, da sie deutlich öfter Strafanzeigen stellen (groß: 71 Prozent; klein: 52 Prozent) und Schadensersatzforderungen verfolgen (groß: 50 Prozent; klein: 36 Prozent).

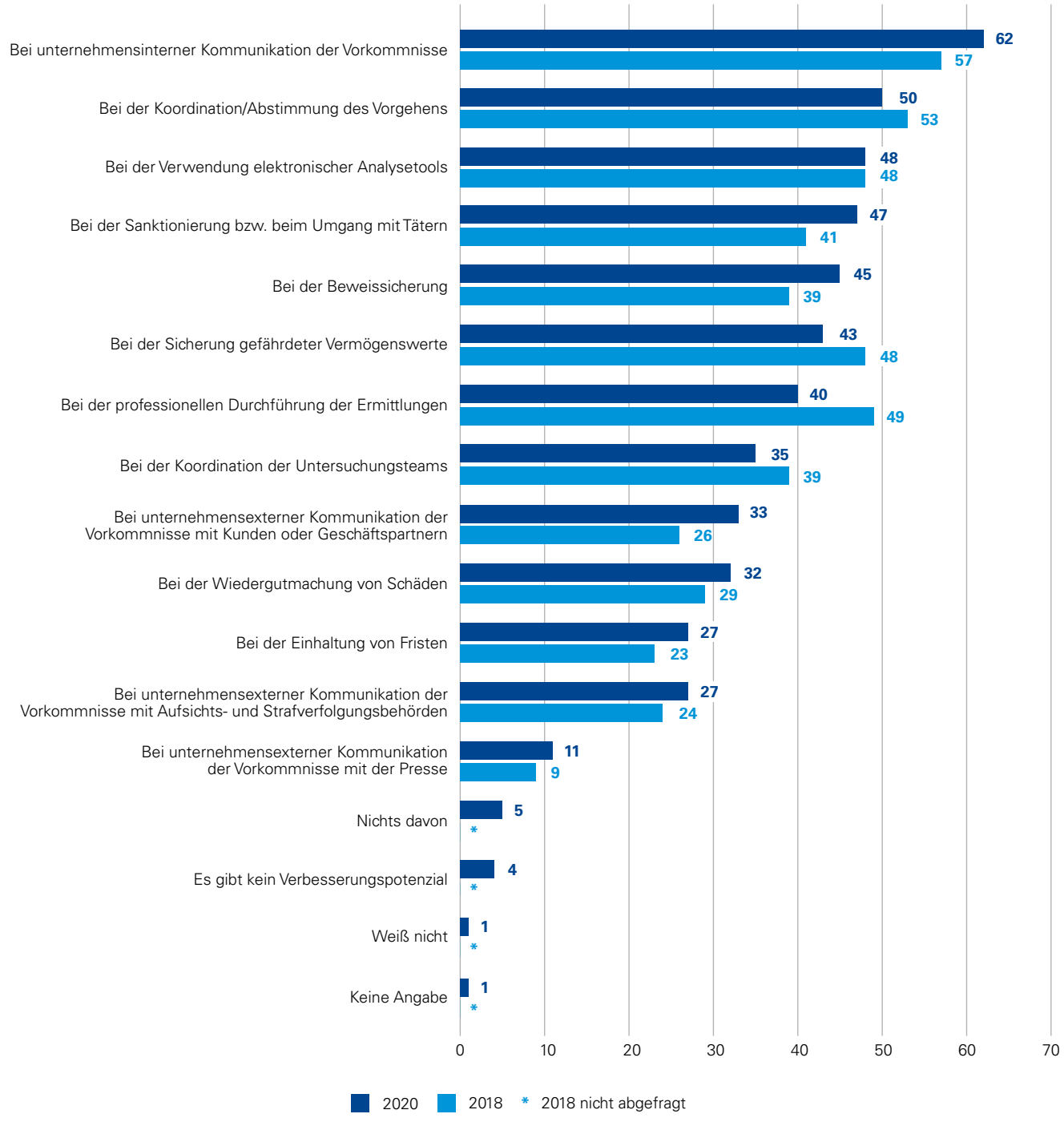
In 6 Prozent aller Fälle haben die Befragten keine weiteren Maßnahmen getroffen.

Abbildung 16: Maßnahmen nach der Aufklärung

Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Abbildung 17: Verbesserungspotenzial beim Umgang mit wirtschaftskriminellen Handlungen



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

2.8 Verbesserungspotenzial beim Umgang mit Wirtschaftskriminalität

Bereits 2018 gaben 91 Prozent der Befragten an, Verbesserungspotenzial beim Umgang mit wirtschaftskriminellen Handlungen zu sehen. Dieser Wert wurde in der diesjährigen Umfrage sogar noch übertroffen: 94 Prozent aller betroffenen Unternehmen bescheinigen sich Verbesserungspotenzial.

Am häufigsten wird Verbesserungspotenzial im Rahmen der unternehmensinternen Kommunikation über Vorkommnisse (62 Prozent) sowie bei der Koordination beziehungsweise Abstimmung des Vorgehens (50 Prozent) genannt. Die interne Krisenkommunikation sowie -koordination bereitet Unternehmen somit nach wie vor Schwierigkeiten. Dies könnte darin begründet sein, dass es den Befragten an klar definierten Krisenreaktionsplänen mangelt, die Verantwortlichkeiten vorgeben und die internen Kommunikationsketten definieren.

Wie schon in der 2018er Ausgabe dieser Studie erkennen 48 Prozent der Befragten Versäumnisse bei der Verwendung elektronischer Analysetools. Dies könnte unter anderem darauf hindeuten, dass die Anwendung derartiger Instrumente allgemein noch nicht zur Routine geworden ist.

» Nahezu jedes Unternehmen sieht Verbesserungsmöglichkeiten beim Umgang mit Wirtschaftskriminalität. Nur wer die festgestellten Schwächen angeht, kann sich langfristig effektiv gegen Wirtschaftskriminalität wappnen. «

Zu den weiteren meistgenannten Versäumnissen zählen die Beweissicherung sowie die Sanktionierung von und der Umgang mit Tätern (45 beziehungsweise 47 Prozent). Letzteres wird eher von kleinen Unternehmen genannt (52 Prozent), was sich mit der bereits dargestellten geringeren Sanktionstätigkeit dieser Unternehmen deckt, die Sanktionsmaßnahmen vielfach nicht mit derselben Stringenz ergreifen wie große Unternehmen.

Sah 2018 noch nahezu jedes zweite Unternehmen Verbesserungspotenzial bei der professionellen Durchführung der Ermittlungen, gilt dies dieses Jahr nur für zwei von fünf (2020: 40 Prozent, 2018: 49 Prozent). Hier scheint somit ein Professionalisierungsprozess zu greifen. Dies kann sich beispielsweise in der Einrichtung spezialisierter Ermittlungseinheiten oder in der bei der aktuellen Erhebung tatsächlich festgestellten vermehrten Hinzuziehung externer Dienstleister äußern.

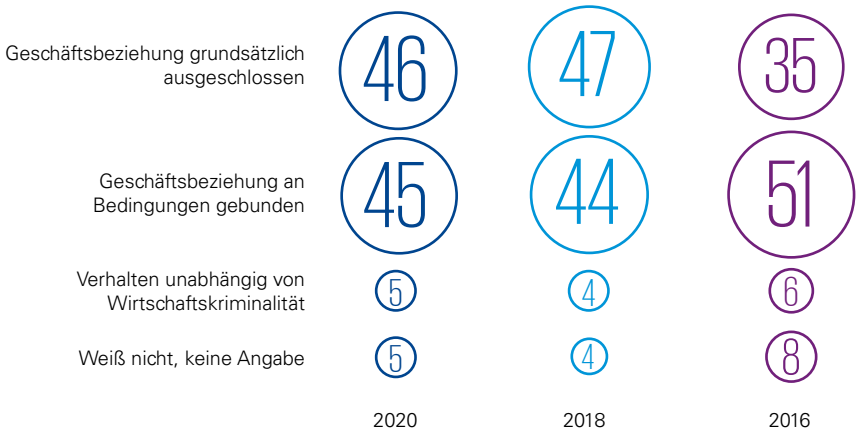
Kleine Unternehmen (nach Umsatz) erkennen hinsichtlich der meisten abgefragten Faktoren mehr Versäumnisse als große Unternehmen. Besonders deutlich sind diese Unterschiede mit Blick auf die unternehmensinterne (klein: 66 Prozent; groß: 47 Prozent) sowie -externe Kommunikation der Vorkommnisse an Kunden und Geschäftspartner (klein: 40 Prozent; groß: 24 Prozent). Des Weiteren bereiten kleinen Unternehmen insbesondere die Sicherung gefährdeter Vermögenswerte (klein: 45 Prozent; groß: 35 Prozent) wie auch die professionelle Durchführung der Ermittlungen größere Schwierigkeiten (klein: 39 Prozent; groß: 29 Prozent).

Zur eigenen Einschätzung des unternehmensinternen Schutzes vor wirtschaftskriminellen Handlungen lässt sich festhalten: Unternehmen mit sehr gutem Schutzniveau sehen weniger Optimierungspotenzial als solche mit schlechtem Schutzniveau. Insgesamt 10 Prozent der Erstgenannten geben im Übrigen an, überhaupt keine Verbesserungsmöglichkeiten zu erkennen.

2.9 Verhalten gegenüber Unternehmen, von denen Wirtschaftskriminalität ausging

Bereits zum dritten Mal wurden Unternehmen im Rahmen der vorliegenden Ausgabe der Studie befragt, wie sie sich gegenüber Unternehmen verhalten, von denen wirtschaftskriminelle Handlungen ausgegangen sind. Hier präsentiert sich ein nahezu identisches Bild im Vergleich zu den Ergebnissen aus der vorangegangenen Studie. So nehmen erneut 91 Prozent der Unternehmen eine Verhaltensänderung innerhalb der Geschäftsbeziehung mit Unternehmen wahr, die im Zusammenhang mit Wirtschaftskriminalität stehen. Dabei wird zu etwa gleichen Teilen die Geschäftsbeziehung entweder an die Erfüllung von Bedingungen gebunden (46 Prozent) oder gar grundsätzlich ausgeschlossen (45 Prozent). 2020 zeigt sich in dieser Hinsicht ein nahezu ausgeglichenes Verhältnis bei den unterschiedlichen Unternehmensgrößen. Große Unternehmen haben ihre Vorgehensweise insofern etwas geändert (2020: 46 Prozent Geschäftsbeziehung ausgeschlossen; 2018: 56 Prozent).

Abbildung 18: Verhalten gegenüber Unternehmen, von denen Wirtschaftskriminalität ausging



Quelle: KPMG, Deutschland, 2020

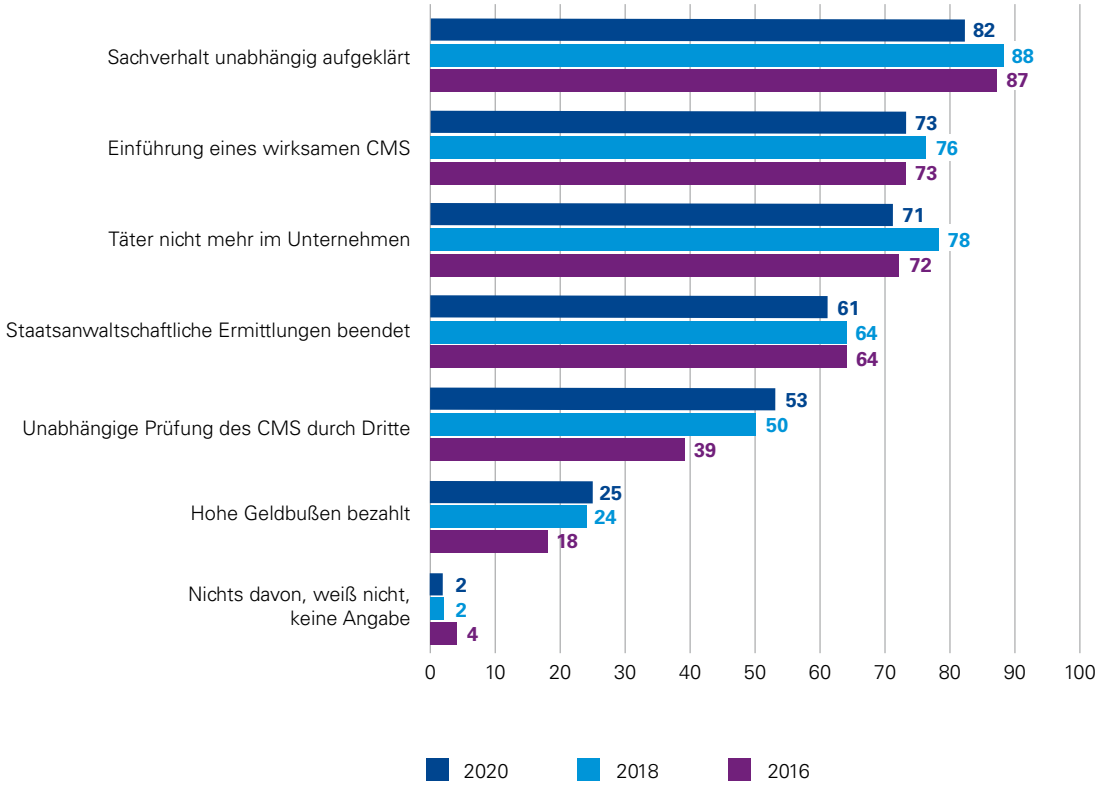
Angaben in Prozent

» Auch ein potenzieller Reputationsschaden darf im Rahmen der Frage nach einer Weiterführung von Geschäftsbeziehungen mit Unternehmen, die ›auffällig geworden‹ sind, nicht außer Acht gelassen werden. «

Vor allem Unternehmen mit einem sehr guten Schutzniveau schließen geschäftliche Beziehungen mit Personen, die wirtschaftskriminelle Taten verüben, grundsätzlich aus. Hierbei zeigt sich eine beachtliche Differenz – 12 Prozentpunkte – im Vergleich zu den Unternehmen mit schlechtem Schutzniveau (50 Prozent zu 38 Prozent). Zwar knüpfen letztgenannte Unternehmen in jedem zweiten Fall die Fortführung der Geschäftsbeziehung an gewisse Bedingungen (50 Prozent), jedoch nehmen sie in 10 Prozent der Fälle überhaupt keine Verhaltensänderung vor.

Ein weiterer Aspekt verdient Erwähnung: Den Befragungsergebnissen zufolge schließen Unternehmen, die selbst bereits von Wirtschaftskriminalität betroffen waren, Geschäftsbeziehungen mit Unternehmen, die sich wegen Wirtschaftskriminalität verantworten müssen, seltener grundsätzlich aus als noch nicht betroffene Studienteilnehmer (38 zu 47 Prozent). Dies könnte darauf zurückzuführen sein, dass sie infolge des betreffenden Vorfalls und etwaiger dabei erlittener Reputationsschäden bei der Wahl neuer Geschäftspartner vor besonderen Herausforderungen stehen und deswegen darauf angewiesen sind, diese unter der Einhaltung von Bedingungen an sich zu binden (betroffen: 53 Prozent; nicht betroffen: 43 Prozent).

Abbildung 19: Bedingungen für eine Fortsetzung der Geschäftsbeziehung



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Hinsichtlich der zu erfüllenden Bedingungen steht nach wie vor die unabhängige Aufklärung des Sachverhalts an erster Stelle. Mit 82 Prozent aller Unternehmen erachtet die Mehrheit dies als wesentlichste Voraussetzung zur Fortsetzung der Geschäftsbeziehung. Zudem sehen etwa drei von vier die Einführung eines wirksamen CMS sowie den Ausschluss des Täters aus dem Unternehmen als probate Mittel für weitere Geschäftsbeziehungen (73 beziehungsweise 71 Prozent).

Ein wirksam implementiertes CMS gewinnt vor allem für große Unternehmen stetig an Bedeutung, in der diesjährigen Studie ist es für diese Unternehmensgruppe sogar gleichbedeutend mit der eigentlichen Aufklärung des Sachverhalts. Für jeweils 84 Prozent der großen Unternehmen (nach Umsatzgröße) haben diese beiden Optionen oberste Priorität. Eine gegenläufige Einschätzung äußern kleine Unternehmen: Nur 68 Prozent von ihnen erkennen ein wirksames CMS als geeignete Maßnahme zur Fortführung der Geschäftsbeziehung an. Zum Vergleich: 2018 waren es hier noch 73 Prozent. Die Forderung großer Unternehmen nach einem wirksamen CMS ist allerdings nicht direkt mit der Forderung verbunden, dieses durch unabhängige Dritte überprüfen zu lassen (nur 46 Prozent legen darauf Wert). Diese Bedingung wiederum spielt bei kleinen und mittleren Unternehmen eine größere Rolle (klein: 52 Prozent; mittel: 56 Prozent). Insbesondere nicht betroffene Unternehmen verlangen diese Maßnahme (57 Prozent; betroffen: 44 Prozent). Ihnen ist offensichtlich an zusätzlicher Absicherung gelegen, bevor sie mit Unternehmen zusammenarbeiten, die bekanntermaßen mit wirtschaftskriminellen Handlungen im Zusammenhang standen oder stehen.

Darüber hinaus verlangen etwa drei von fünf Befragten, dass die staatsanwaltschaftlichen Ermittlungen beendet sind.

Unwissenheit ist ein Spiel mit dem Feuer

3. Sanktionen und Embargos

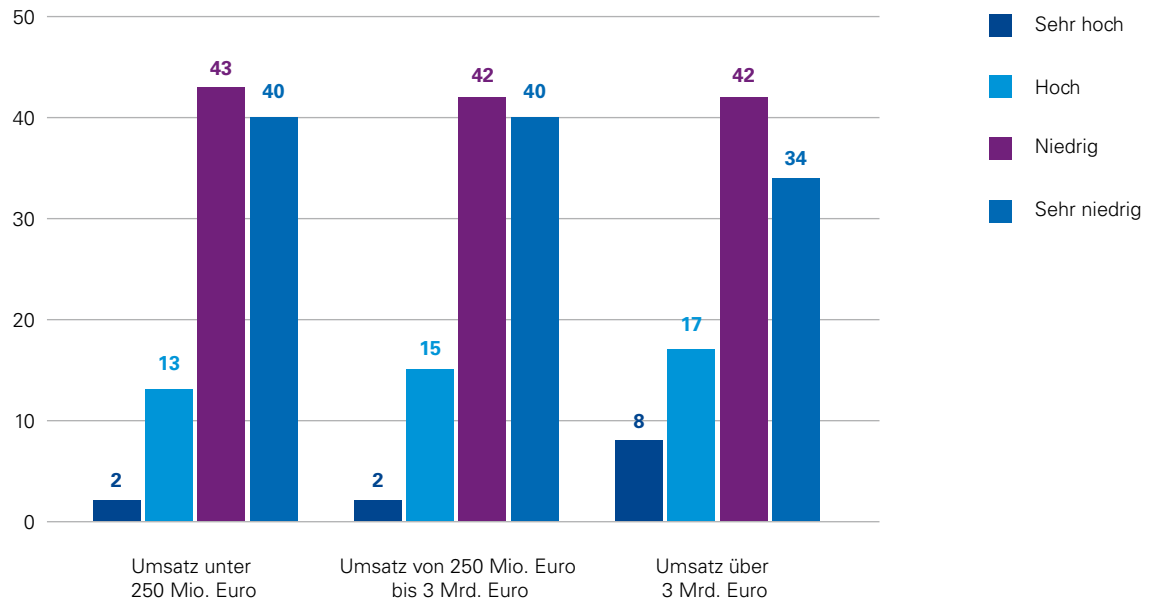
Über die Hälfte der deutschen Unternehmen ist mit dem Thema Sanktionen und Embargos nicht vertraut, obwohl bei Verstößen gravierende Bußgelder erwartet werden.

3.1 Informationsstand und Risikowahrnehmung zu Sanktionen und Embargos

Mehr als jedes zweite befragte Unternehmen (52 Prozent) bekennt, nicht mit dem Thema Sanktions- und Embargo-Compliance vertraut zu sein. Vor allem kleine Unternehmen (nach Umsatz) haben hier Nachholbedarf. Von ihnen geben lediglich 42 Prozent an, informiert zu sein. Mittlere und große Unternehmen (56 und 65 Prozent) hingegen verfügen über bessere Kenntnisse auf diesem Feld.

82 Prozent schätzen das Risiko, mit Sanktions- und Embargovorschriften in Konflikt zu geraten, als niedrig oder sehr niedrig ein, was im Vergleich zu der Risikowahrnehmung im Hinblick auf die weiteren abgefragten Delikte (siehe Abschnitt 1.2) den geringsten Wert darstellt. Jedoch zeigt sich, dass mit zunehmender Unternehmensgröße auch ein erhöhtes Risikobewusstsein einhergeht. Nur knapp jedes sechste der kleinen und mittleren, aber jedes vierte der großen Unternehmen sieht ein hohes oder sehr hohes Risiko, gegen Sanktions- und Embargovorschriften zu verstoßen. Unter Umständen ist dies deshalb der Fall, da große Unternehmen häufig international oder gar global agieren und Geschäftsbeziehungen zu Unternehmen aus Drittländern unterhalten, was mit einem erhöhten Bewusstsein für Sanktions- und Embargovorschriften einhergeht.

Abbildung 20: Risikowahrnehmung im Hinblick auf Sanktions- und Embargoverstöße



Quelle: KPMG, Deutschland, 2020

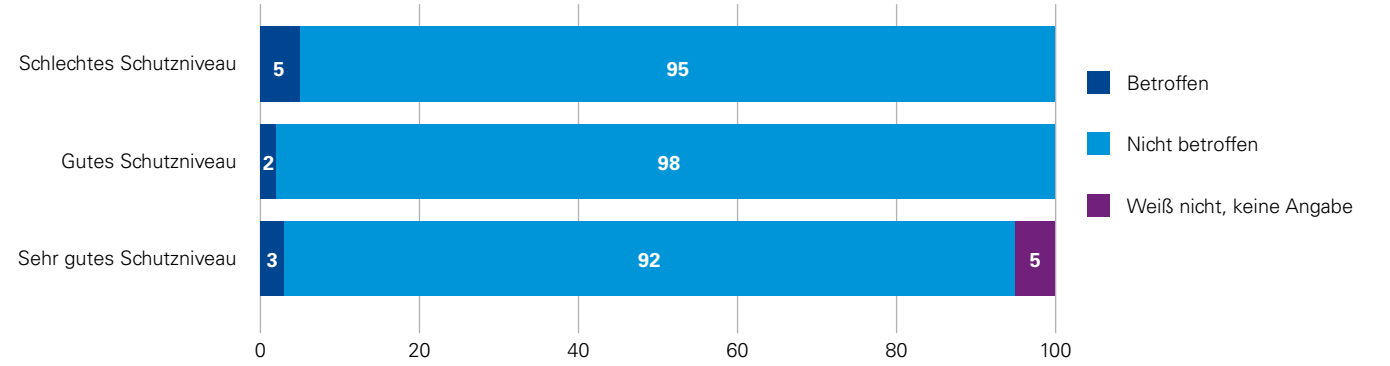
Angaben in Prozent

3.2 Verstöße und entsprechende erwartete Auswirkungen[3]

Lediglich 3 Prozent der befragten Unternehmen geben an, in den vergangenen zwei Jahren gegen Sanktions- und Embargovorschriften verstoßen zu haben. Von den weiteren abgefragten Delikten erhält nur der Aspekt, von einer Manipulation jahresabschlussrelevanter Informationen betroffen gewesen zu sein, mit 2 Prozent noch weniger Nennungen (siehe Abschnitt 1.2).

[3] Die folgenden Fragen richteten sich ausschließlich an die Unternehmen, die angaben, mit Sanktions- und Embargo-Compliance vertraut zu sein.

Abbildung 21: Betroffenheit von Wirtschaftskriminalität in Abhängigkeit vom unternehmensinternen Schutzniveau



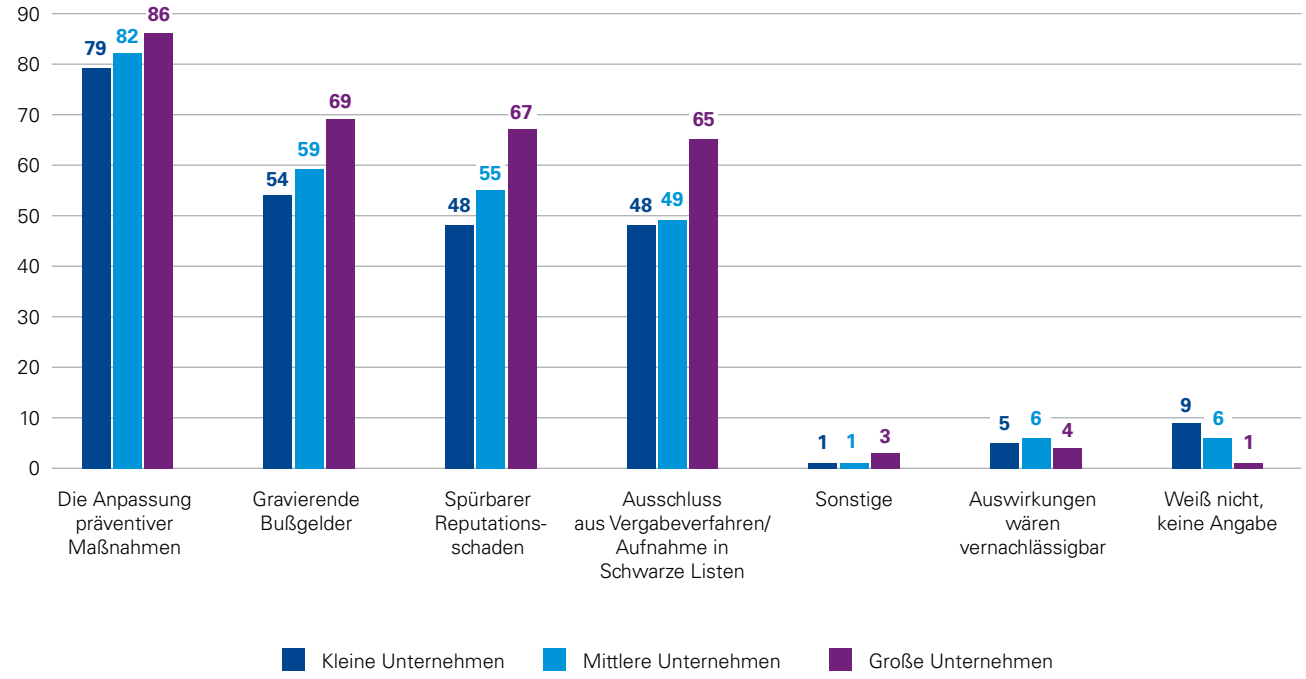
Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Für den Fall eines entdeckten Sanktions- oder Embargoverstoßes beabsichtigt eine deutliche Mehrheit der Studienteilnehmer (83 Prozent), präventive Maßnahmen anzupassen. Dies ist auch im Hinblick auf die im Rahmen dieser Studie grundsätzlich abgefragten Deliktsarten der am meisten genannte Schritt nach der Aufklärung eines wirtschaftskriminellen Vorfalls (60 Prozent – siehe Abschnitt 2.7). Abgesehen von der Anpassung der präventiven Maßnahmen erwarten etwa drei von fünf Befragten gravierende Bußgelder (61 Prozent) und auch spürbare Reputationsschäden (58 Prozent). Grundsätzlich zeigt sich, dass große Unternehmen häufiger als kleine oder mittelgroße (gemessen am Umsatz) davon ausgehen, unter den verschiedenen abgefragten Auswirkungen zu leiden. Dies könnte auf den besseren Kenntnisstand der großen Unternehmen zurückzuführen sein, der sie potenzielle Folgen und deren Eintrittswahrscheinlichkeit realistischer einschätzen lässt.

Bei dem Ausschluss aus Vergabeverfahren und der Aufnahme in „Schwarze Listen" zeigt sich ebenfalls ein deutlicher Unterschied im Hinblick auf die Unternehmensgrößen (gemessen an der Mitarbeiterzahl). Während weniger als jedes zweite kleine oder mittlere Unternehmen (48 beziehungsweise 49 Prozent) eine solche Folge erwartet, sehen immerhin 65 Prozent der großen dies als eine drohende Konsequenz. In dieser Hinsicht fällt zudem auf, dass Befragte, die ihr Schutzniveau als schlecht bewerten, diese Konsequenz seltener für sich annehmen als die übrigen (schlechtes Schutzniveau: 46 Prozent; Durchschnitt übrige Befragte: 56 Prozent).

Abbildung 22: Auswirkungen im Falle eines entdeckten Sanktions- und Embargoverstoßes nach Mitarbeiterzahl



Quelle: KPMG, Deutschland, 2020

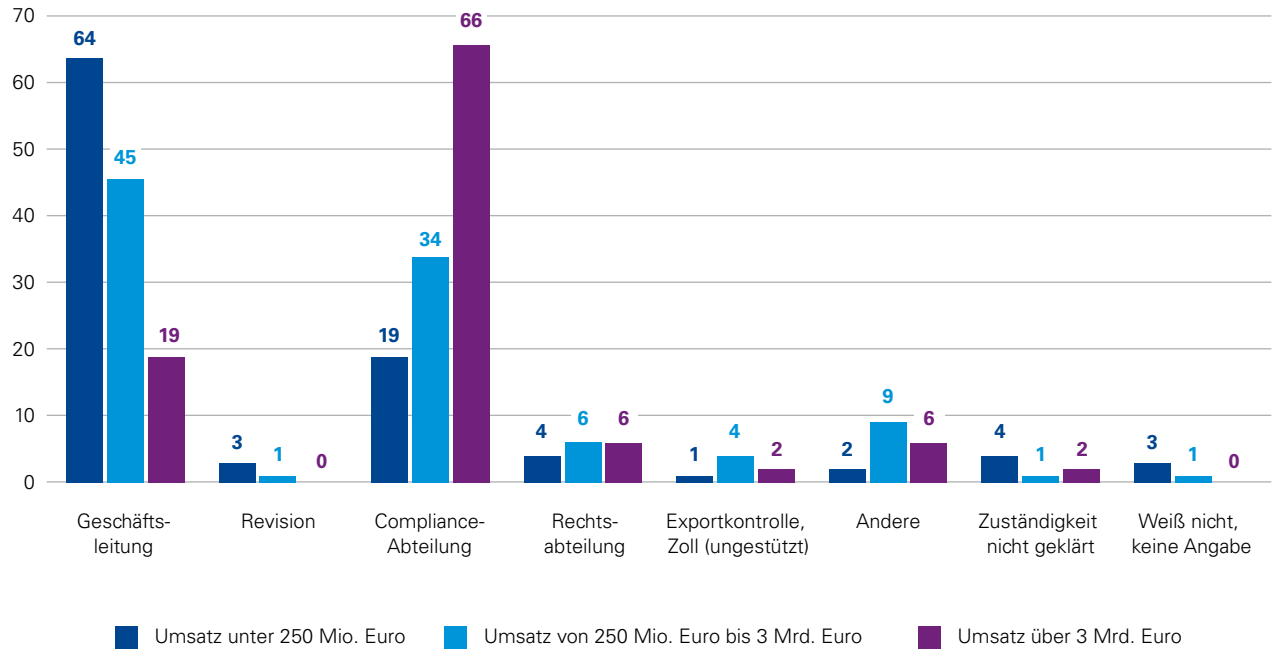
Angaben in Prozent

3.3 Zuständigkeit für die Einhaltung von Sanktions- und Embargovorschriften

Ein großer Teil der Befragten benennt die Geschäftsleitung (52 Prozent) sowie die Compliance-Abteilung (30 Prozent) als die Einheiten, die für die Einhaltung von Sanktionen und Embargovorschriften zu sorgen haben. Wie schon hinsichtlich der operativen Aufklärung festgestellt, liegt auch auf diesem Feld die Verantwortung in großen Unternehmen eher bei der spezialisierten Compliance-Abteilung, wohingegen man sich in kleinen auf die Geschäftsleitung verlässt. So verweisen die Vertreter großer Unternehmen zu lediglich 19 Prozent auf die Geschäftsleitung, aber zu 66 Prozent auf die Compliance-Abteilung. Bei kleinen Unternehmen ist dies umgekehrt (Geschäftsleitung: 64 Prozent; Compliance-Abteilung: 19 Prozent).

Unabhängig von der Unternehmensgröße verorten wenige Befragte die Zuständigkeit bei der Rechtsabteilung oder der Revision (5 beziehungsweise 2 Prozent). 3 Prozent der Studienteilnehmer wollen oder können sich auf keine der abgefragten Optionen festlegen.

Abbildung 23: Zuständigkeiten für die Einhaltung von Sanktionen und Embargovorschriften



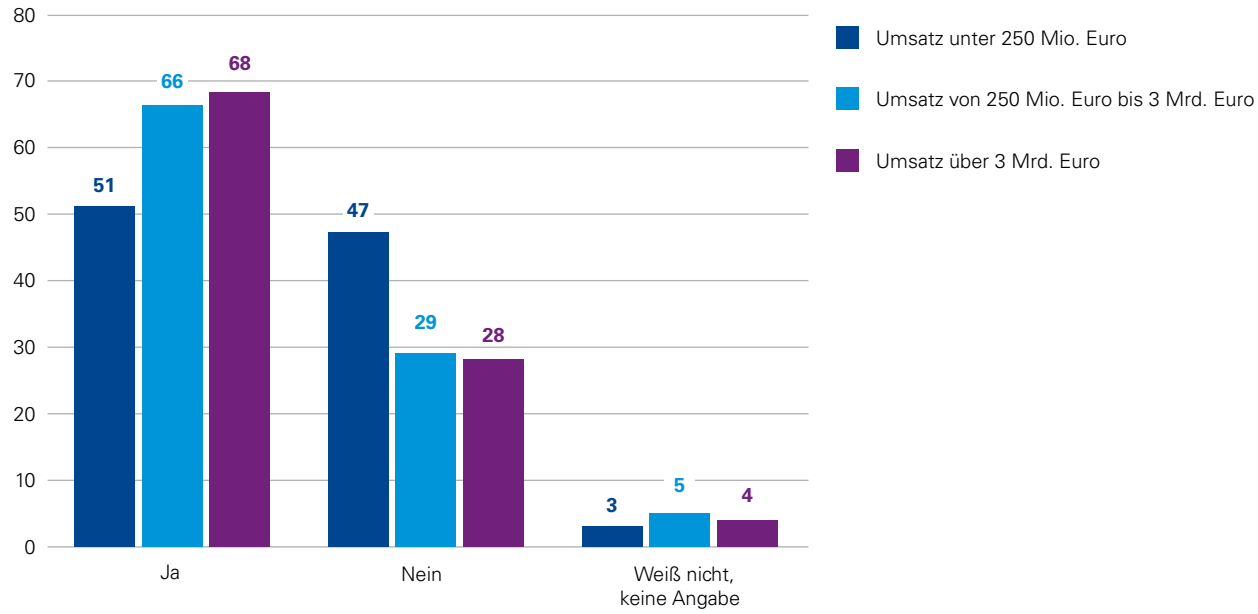
Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

3.4 Managementsysteme und Präventionsmaßnahmen zu Sanktionen und Embargos

Drei von fünf befragten Unternehmen (58 Prozent) haben den Angaben zufolge ein Managementsystem eingerichtet, das explizit Fragen zu Sanktionen und Embargos abdeckt. Insbesondere mittlere und große Unternehmen (nach Umsatz) haben ein solches System implementiert (66 beziehungsweise 68 Prozent).

Abbildung 24: Einrichtung eines Managementsystems im Bereich Sanktionen und Embargos



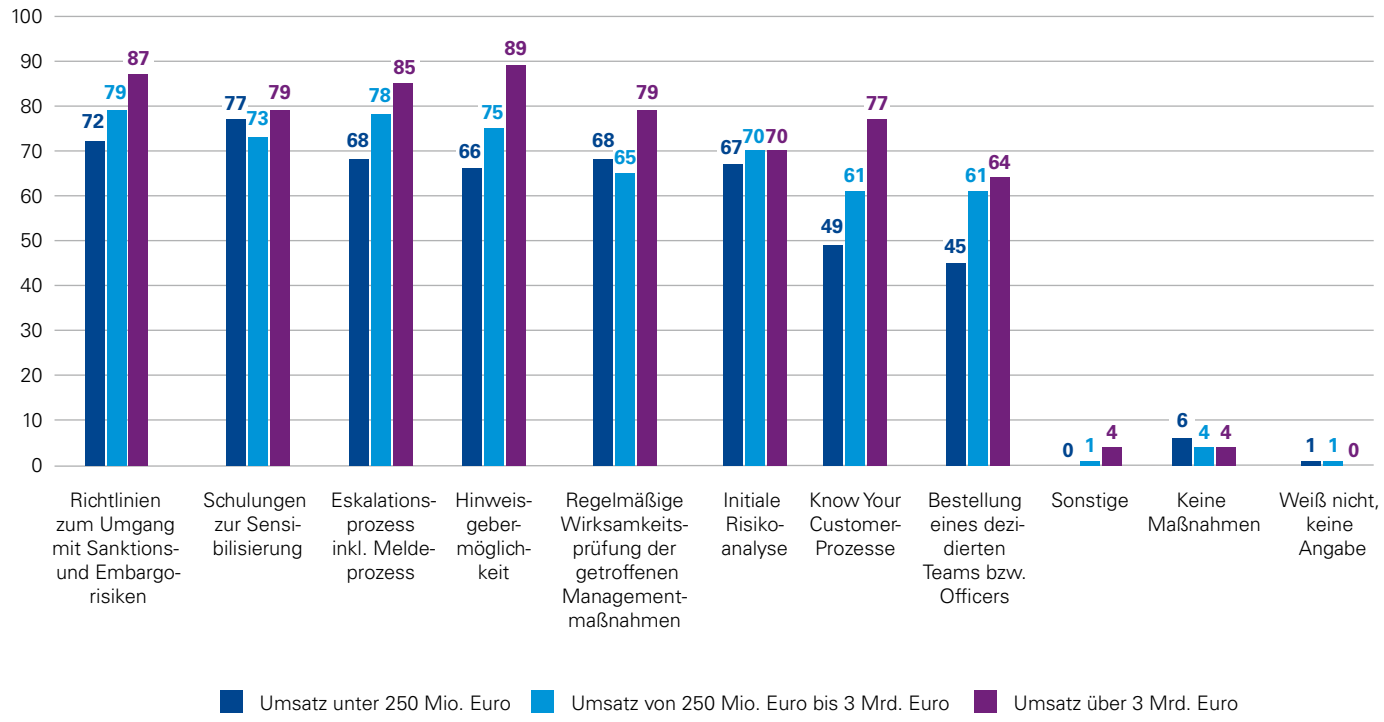
Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Mit Blick auf die Gesamtheit der Unternehmen, die mit dem Thema Sanktionen und Embargos vertraut sind, lässt sich feststellen, dass die Befragten einen durchaus diversifizierten Präventionsansatz verfolgen. So verweisen mehr als drei Viertel (76 Prozent) sowohl auf Richtlinien zum Umgang mit diesem Thema als auch auf Schulungen zur Sensibilisierung. Nahezu gleich viele Unternehmen verfügen darüber hinaus über einen Eskalations- und Meldeprozess (74 Prozent) sowie eine Hinweisgebermöglichkeit (72 Prozent). Ferner lassen gut zwei von drei Unternehmen wissen, sie würden die Wirksamkeit der getroffenen Maßnahmen regelmäßig überprüfen und eine initiale Risikoanalyse durchführen (jeweils 68 Prozent).

Wie schon angedeutet zeigen sich im Zuge dieser Fragestellung zum Teil enorme Diskrepanzen zwischen den Unternehmen, und zwar sowohl nach Größe als auch dahingehend, wie sie ihr jeweiliges Schutzniveau bewerten. So führen Befragte mit einem sehr guten Schutzniveau wesentlich häufiger Maßnahmen wie Schulungen und initiale Risikoanalysen (85 beziehungsweise 77 Prozent) durch als solche, die ihr Schutzniveau als schlecht einstufen (64 beziehungsweise 59 Prozent). Zudem versichern sie sich in größerer Regelmäßigkeit der Wirksamkeit der getroffenen Maßnahmen (sehr gutes Schutzniveau: 75 Prozent; schlechtes Schutzniveau: 50 Prozent).

Abbildung 25: Präventionsmaßnahmen im Bereich Sanktionen und Embargos



Quelle: KPMG, Deutschland, 2020

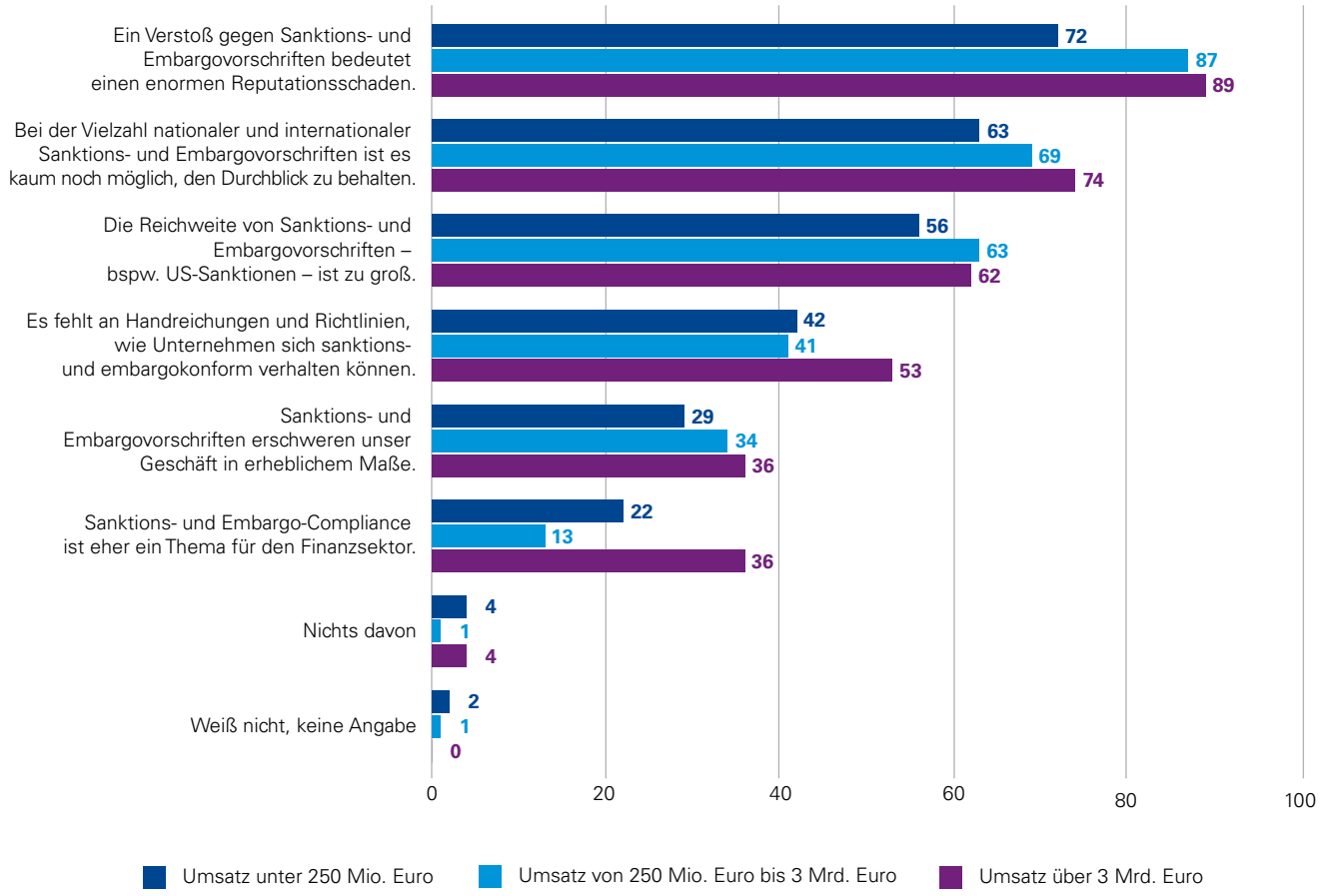
Angaben in Prozent

Bei der Betrachtung nach Größenklassen (nach Umsatz) wiederum machen insbesondere Eskalations- und Meldeprozesse (groß: 85 Prozent; klein: 68 Prozent), Hinweisgebermöglichkeiten (groß: 89 Prozent; klein: 66 Prozent) sowie Know Your Customer-Prozesse (groß: 77 Prozent; klein: 49 Prozent) den Unterschied aus. Des Weiteren haben umsatzstarke Unternehmen häufiger einen Beauftragten oder ein Team für die Einhaltung von Sanktions- und Embargovorschriften bestellt (groß: 64 Prozent; klein: 45 Prozent).

3.5 Aussagen zum Thema Sanktionen und Embargos

Abschließend wurden die Studienteilnehmer unter Verweis auf einige Aussagen zum Thema Sanktions- und Embargo-Compliance befragt, ob sie diesen zustimmen.

Abbildung 26: Zustimmende Aussagen zum Thema Sanktionen und Embargos



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Vier von fünf Befragten äußern die Ansicht, ein Verstoß gegen Sanktions- und Embargovorschriften sei mit einem enormen Reputationsschaden verbunden. Dieses Risiko erkennen insbesondere mittlere und große Unternehmen – gemessen an ihrem Umsatz – (87 und 89 Prozent), wohingegen kleine dieser Aussage seltener zustimmen (72 Prozent) – möglicherweise, weil sie für den Fall von Verstößen unter Umständen mit einer geringeren medialen Aufmerksamkeit rechnen.

Darüber hinaus geben mehr als zwei von drei Umfrageteilnehmern an, angesichts der Fülle nationaler und internationaler Sanktions- und Embargovorschriften sei es kaum noch möglich, den Überblick zu wahren. Im Einklang damit geben drei von fünf an, die Reichweite von Sanktions- und Embargovorschriften sei zu groß. Gleichzeitig fehlt es auch 43 Prozent der Befragten an Richtlinien oder Handreichungen, anhand derer sich regelkonformes Verhalten sicherstellen ließe. Insbesondere große Unternehmen beklagen einen Mangel an Übersichtlichkeit (74 Prozent) und an Handreichungen (53 Prozent).

Knapp zwei von drei der umsatzstarken Unternehmen geben an, Sanktions- und Embargo-Compliance sei eher ein Thema für den Finanzsektor (36 Prozent). Dieser Trugschluss ist dahingehend überraschend, als ein Verstoß gegen Sanktions- und Embargovorschriften auch für Unternehmen außerhalb der Finanzbranche eine große Rolle spielen kann.

Ungeachtet der geäußerten Bedenken ist weniger als ein Drittel der Befragten der Ansicht, dass Sanktions- und Embargovorschriften ihr Geschäft in erheblichem Maße erschweren.

4. Einsatz digitaler Compliance-Werkzeuge

Der Einsatz digitaler Compliance-Werkzeuge nimmt zu. Dies führt bei dem Großteil der Unternehmen zu einer Effizienzsteigerung der gesamten Compliance-Einheit und wirkt auch präventiv.

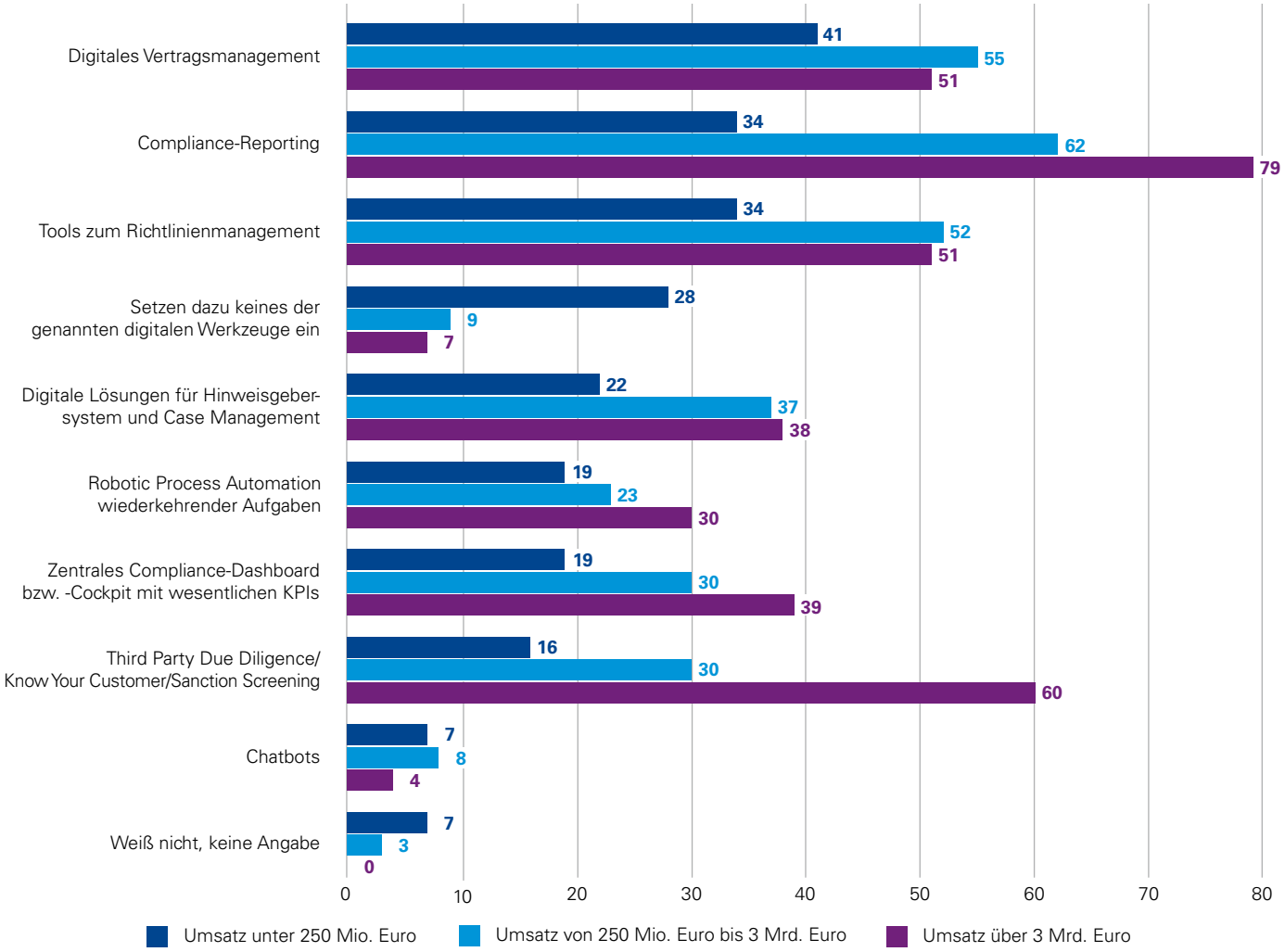
4.1 Hintergründe und tatsächlicher Einsatz digitaler Werkzeuge im Compliance-Umfeld

Sowohl im persönlichen Alltag als auch im unternehmerischen Kontext – aktuell beispielsweise im Rahmen der Umstrukturierungen interner Prozesse oder bei der Schaffung von Home-Offices in Zeiten des Coronavirus: Das Thema Digitalisierung ist allgegenwärtig. Allerdings birgt es neben dem enormen Potenzial der Effizienzsteigerung auch teils erhebliche Risiken im Hinblick auf wirtschaftskriminelle Handlungen. Um dem daraus resultierenden Spannungsfeld gerecht zu werden, kann es für Unternehmen förderlich sein, digitale Compliance-Werkzeuge effizient in der Prozesslandschaft zu implementieren. Diese können wirtschaftskriminellen Handlungen entgegenwirken, aber auch für Synergieeffekte sorgen. Vor diesem Hintergrund wurden die Teilnehmer der diesjährigen Studie zum operativen Einsatz digitaler Compliance-Maßnahmen befragt.

Nahezu jedes zweite Unternehmen hat das Compliance-Reporting sowie das Vertragsmanagement digitalisiert (je 47 Prozent). Insbesondere Ersteres ist gerade in großen Unternehmen mittlerweile nahezu Standard (79 Prozent). Darüber hinaus haben bereits mehr als zwei von fünf Unternehmen (41 Prozent) das eigene Richtlinienmanagement digitalisiert.

Etwa ein Viertel (28 Prozent) der Befragten gibt zu Protokoll, digitale Lösungen für Hinweisgebersysteme und das Fallmanagement einzusetzen, wobei dies in großen Organisationen häufiger so ist als in kleinen (38 gegenüber 22 Prozent).

Abbildung 27: Einsatz digitaler Werkzeuge zur Prävention, Aufdeckung und Aufklärung von Wirtschaftskriminalität



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

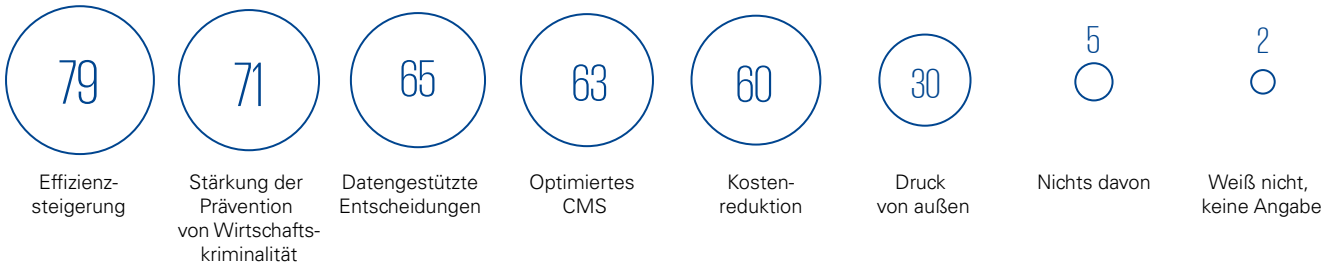
Während es sich bei den vier meistgenannten digitalen Angeboten um Management- oder Reporting-Werkzeuge handelt, werden Tools, die sich auf die Analyse und Verbesserung unternehmensinterner Prozesse beziehen, bislang seltener eingesetzt. Dies könnte darin begründet sein, dass der Implementierungsaufwand und somit auch der Ressourcenbedarf im Bereich der Prozesse deutlich höher und komplexer ist, zum Beispiel im Hinblick auf die zu berücksichtigende Vielzahl von Systemen und Schnittstellen.

Dennoch nutzt derzeit lediglich knapp jedes vierte der befragten Unternehmen ein zentrales Compliance-Dashboard oder -Cockpit mit wesentlichen Kennzahlen sowie eine digitale Third Party Due Diligence, Know Your Customer-Prüfungen und Sanction Screenings (jeweils 24 Prozent).

Für nahezu alle abgefragten digitalen Werkzeuge hat die Umfrage ergeben, dass kleine Unternehmen weniger (teils sogar viel weniger) davon Gebrauch machen als mittlere oder große (72 zu 93 Prozent).

Gefragt nach den Gründen für die Digitalisierung im Compliance-Umfeld, nennen die Studienteilnehmer in erster Linie eine erhoffte Effizienzsteigerung (79 Prozent). Dies gilt insbesondere für Unternehmen, die den eigenen Schutz als gut oder sehr gut bewerten. Rund vier von fünf Vertretern dieser Gruppe sehen dies als den wichtigsten Treiber für die Digitalisierung im Compliance-Umfeld an, wohingegen lediglich knapp zwei Drittel der schlecht vorbereiteten Unternehmen dieser Ansicht sind.

Abbildung 28: Gründe für die Digitalisierung im Compliance-Umfeld



Quelle: KPMG, Deutschland, 2020

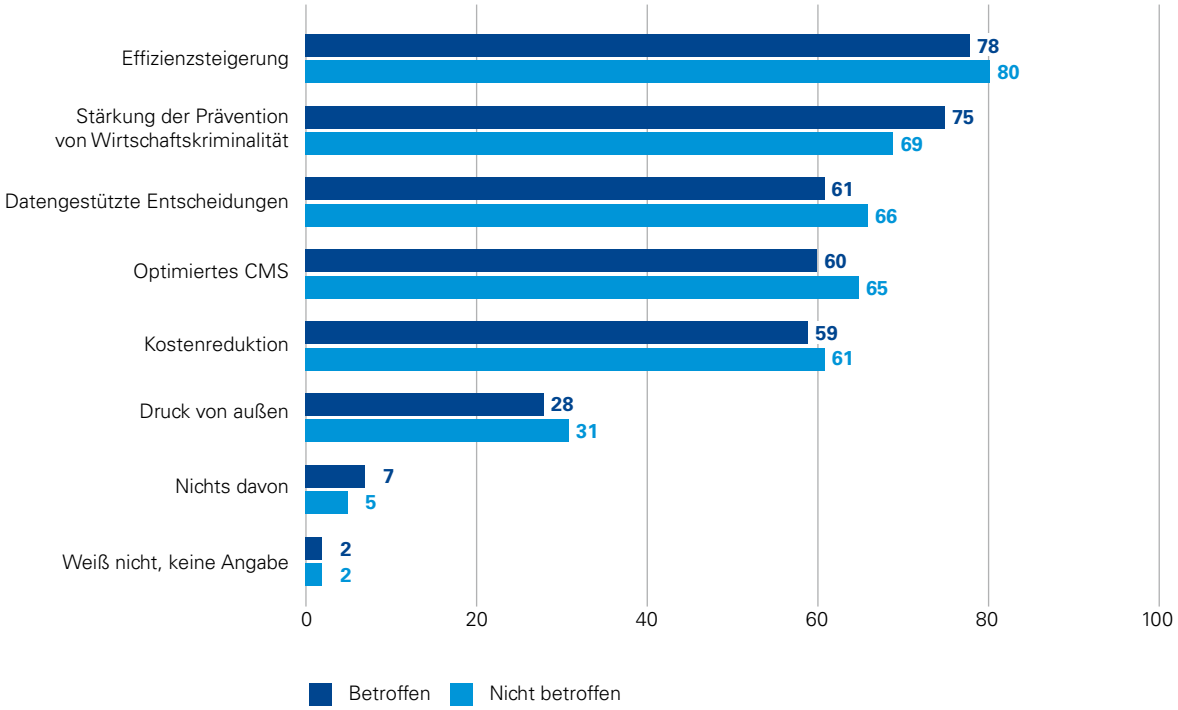
Angaben in Prozent

» Die Möglichkeiten, die sich aus der Digitalisierung des Compliance-Umfelds ergeben, sollten unbedingt ergriffen werden – ein Mangel an Ressourcen sollte diesem wichtigen Schritt nicht im Weg stehen. «

71 Prozent der Umfrageteilnehmer verweisen bei der Digitalisierung des Compliance-Umfelds auch auf eine Stärkung des Schutzes vor wirtschaftskriminellen Handlungen. Allerdings zeigt sich hier kein sonderlich großer Unterschied zwischen nach eigener Aussage sehr gut oder aber schlecht gewappneten Unternehmen (sehr gut: 70 Prozent; schlecht: 64 Prozent).

Dass Entscheidungen durch die Verwendung digitaler Werkzeuge datengestützt getroffen werden können, ist für nahezu zwei von drei Befragten ausschlaggebend für die Digitalisierung des Compliance-Umfelds (65 Prozent). Doch auch die von der Digitalisierung begünstigte Optimierung des CMS sowie Kostensenkungen sind für viele Befragte wichtige Faktoren (63 beziehungsweise 60 Prozent).

Abbildung 29: Gründe für die Digitalisierung der Compliance-Tools in Abhängigkeit von der Betroffenheit



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

4.2 Herausforderungen sowie Vor- und Nachteile der Digitalisierung im Compliance-Umfeld

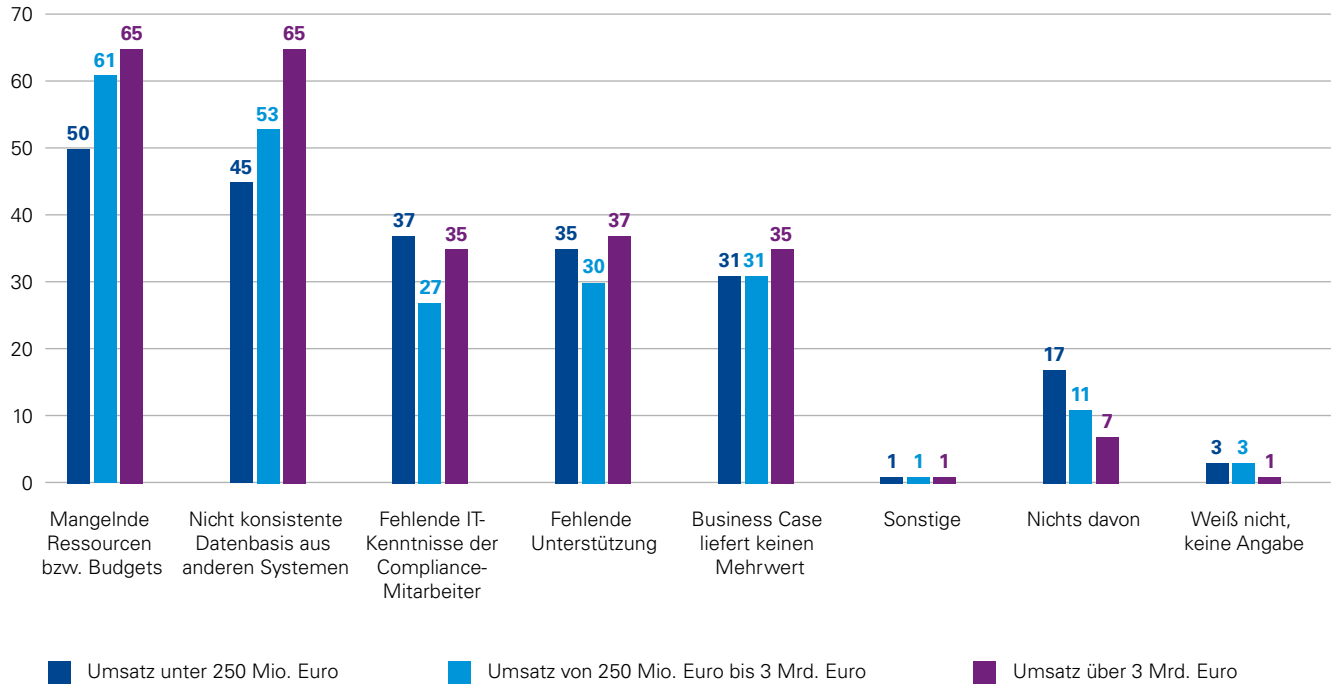
Mehr als jedes zweite befragte Unternehmen sieht in mangelnden Ressourcen oder Budgets (55 Prozent) die größte Hürde bei der Digitalisierung des Compliance-Umfelds. Diese Einschätzung wird von großen Unternehmen (nach Umsatz) sogar deutlicher als von kleinen geäußert (65 gegenüber 50 Prozent). Dies unterstreicht, dass der Digitalisierungsprozess auch bei Unternehmen dieser Größenordnung noch nicht abgeschlossen ist.

Vor allem bei umsatzstarken Unternehmen (65 Prozent) stellt zudem die mangelnde Konsistenz der Daten aus unterschiedlichen Systemen eine mächtige Hürde in der Digitalisierung des Compliance-Umfelds dar. Dies dürfte allerdings kaum überraschen, denn große Unternehmen verfügen häufiger als kleine über eine sehr komplexe IT-Landschaft, deren Harmonisierung anspruchsvoll ist und vollumfängliche Analysen zu einer Herausforderung macht. Hierfür bedarf es der ausführlichen Planung und umfangreicher Ressourcen. Von der Gesamtheit aller Befragten bezeichnet die Hälfte eine nicht konsistente Datenbasis als große Hürde.

Fehlende IT-Kenntnisse der Mitarbeiter sowie ein Mangel an Unterstützung bereiten etwa jedem Dritten Sorgen.

Bemerkenswert ist, dass knapp ein Drittel der Unternehmen keinen Mehrwert im Business Case zur Digitalisierung sieht, wobei dies insbesondere für diejenigen gilt, die ihren Schutz vor Wirtschaftskriminalität als schlecht einschätzen (41 Prozent).

Abbildung 30: Hürden bei der Digitalisierung im Compliance-Umfeld

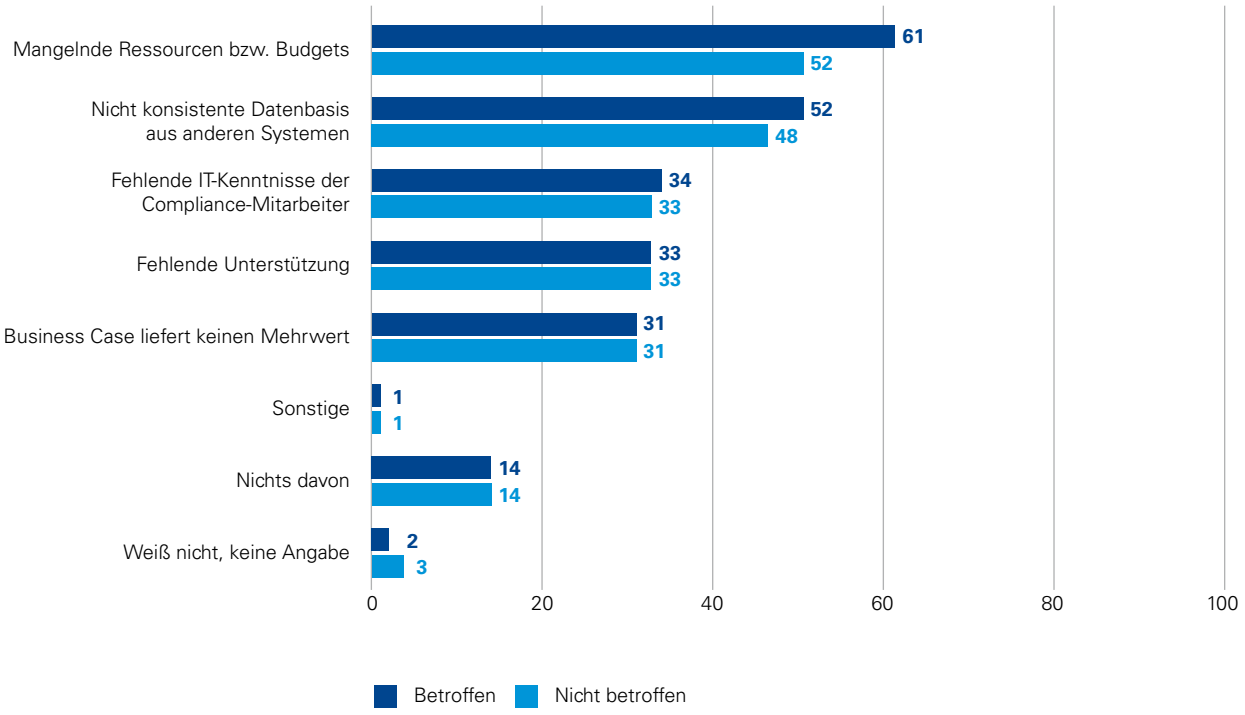


Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Aus der Perspektive derer, die bereits von Wirtschaftskriminalität betroffen waren, ist der Mangel an Ressourcen überdurchschnittlich häufig (61 Prozent) die größte Hürde für die Digitalisierung. Dieser Faktor scheint demnach der tatsächliche Knackpunkt im Hinblick darauf zu sein, wie effektiv und effizient die Digitalisierung im Compliance-Umfeld voranschreitet.

Abbildung 31: Hürden bei der Digitalisierung in Abhängigkeit von der Betroffenheit durch wirtschaftskriminelle Handlungen



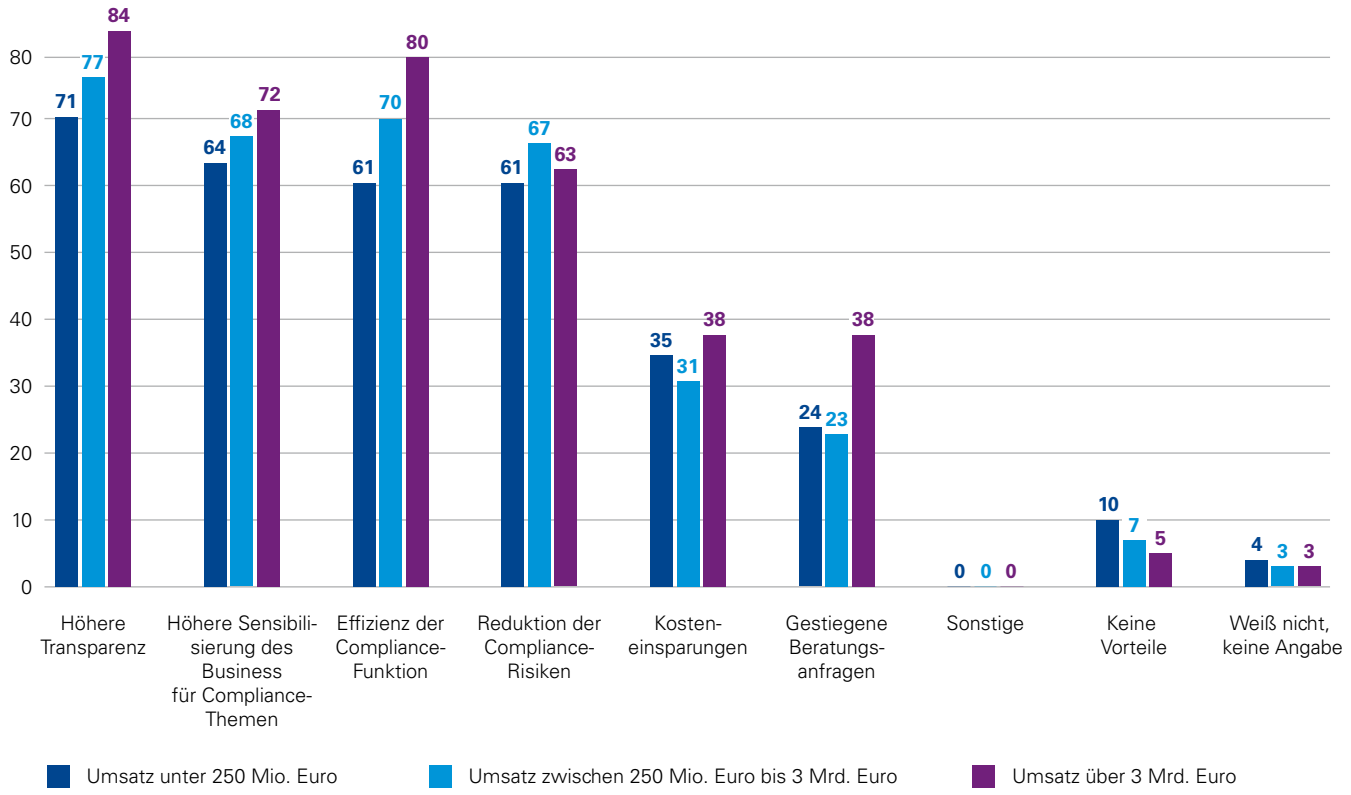
Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Ein Großteil der Umfrageteilnehmer sieht in der Einführung digitaler Compliance-Lösungen viele Vorteile. Insbesondere verweisen sie auf eine höhere Transparenz (75 Prozent), eine verbesserte Sensibilisierung des Business für Compliance-Themen (66 Prozent), eine effizientere Compliance-Funktion (66 Prozent) sowie die Reduktion der Compliance-Risiken (63 Prozent). Es fällt auf, dass diese Vorteile in der Wahrnehmung großer Unternehmen stärker ausgeprägt sind als bei den mittleren und den kleinen, insbesondere Transparenz und Effizienz (84 beziehungsweise 80 Prozent).

Diese Antworten beziehungsweise ihre Gewichtungen dürften als Hinweis darauf dienen, dass die Digitalisierung des Compliance-Umfelds förderlich sein kann für eine bessere Compliance-Kultur sowie das entsprechende Verständnis der Mitarbeiter.

Abbildung 32: Vorteile durch die Digitalisierung des Compliance-Umfelds

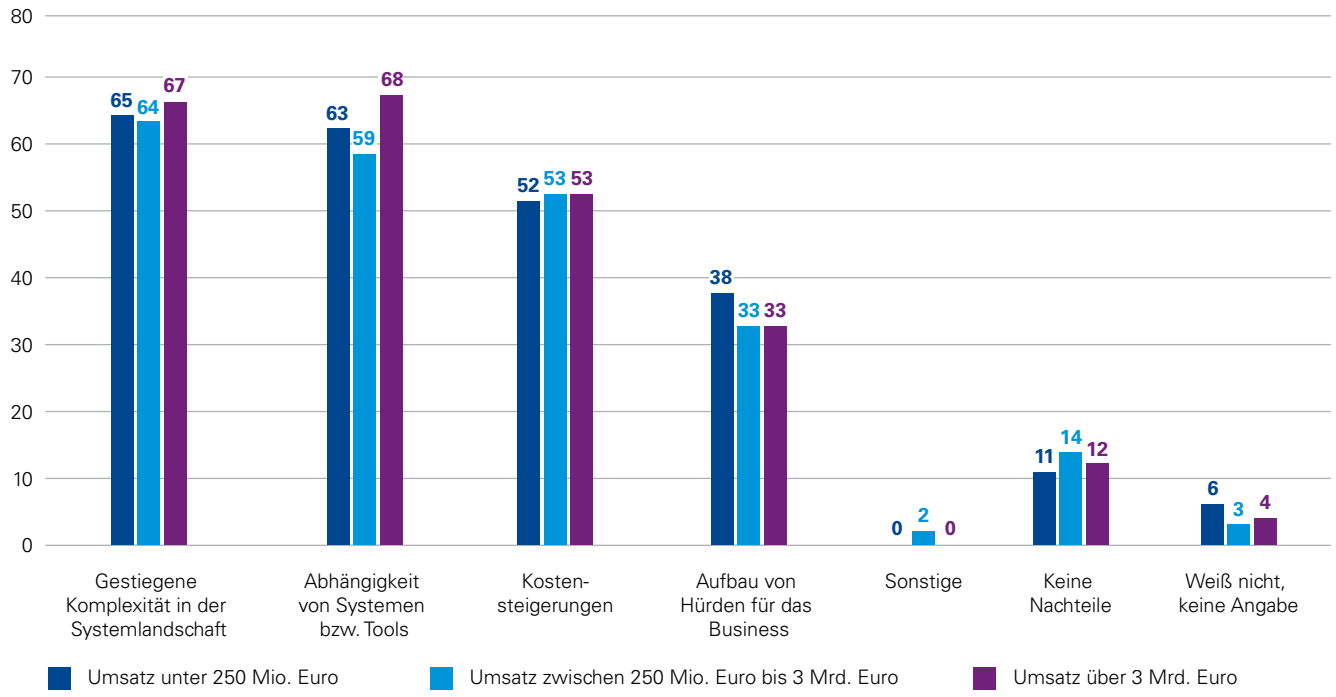


Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Kosteneinsparungen verzeichnete mehr als jedes dritte Unternehmen (34 Prozent), nachdem es digitale Elemente im Compliance-Bereich implementiert hatte. Dass Unternehmen trotz der Investitionen, die eine Digitalisierung grundsätzlich mit sich bringt, Kostenvorteile ins Feld führen, macht deutlich, welches Potenzial in der Umsetzung digitaler Lösungen steckt. 35 Prozent der kleinen und 31 Prozent der mittelgroßen Unternehmen geben an, dies beobachten zu können, große Unternehmen sogar in 38 Prozent der Fälle.

Abbildung 33: Nachteile durch die Digitalisierung des Compliance-Umfelds



Quelle: KPMG, Deutschland, 2020

Angaben in Prozent

Dennoch bringt eine digitale Lösung der Compliance-Funktion aus Sicht der Befragten nicht ausschließlich Vorteile mit sich. So geben 65 Prozent der Befragten an, eine gestiegene Komplexität beobachtet zu haben, und 62 Prozent bemängeln die Abhängigkeit von Systemen oder Tools. Für etwa jedes dritte Unternehmen (35 Prozent) bringt die Digitalisierung der Compliance-Landschaft auch Hürden für das operative Geschäft mit sich.

Bei gut der Hälfte der Unternehmen (53 Prozent) scheinen sich die mit der Digitalisierung einhergehenden Investitionen nicht auszuzahlen; sie verweisen bezüglich der Implementierung und des Betriebs digitaler Compliance-Werkzeuge auf Kostensteigerungen. Hier wird zu beobachten sein, ob diese Kosten sich im Lauf der Zeit wieder ausgleichen.

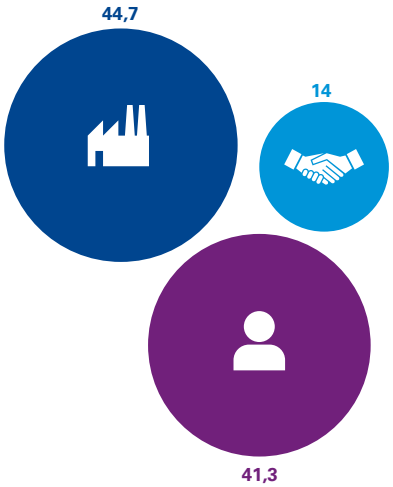
Abschließend sei auf einen übergreifenden Aspekt verwiesen: Von den genannten Vorteilen wollen den Antworten zufolge auch Unternehmen profitieren, die bislang keine digitalen Compliance-Werkzeuge implementiert haben, doch sehen sie sich dabei mit Herausforderungen konfrontiert. Immerhin einem Drittel (33 Prozent) der Studienteilnehmer fehlt es dabei an entsprechendem Know-how. Für sie empfiehlt sich unter Umständen ein Blick über den Tellerrand: Eine Möglichkeit, die nötige Unterstützung zu erhalten, besteht häufig darin, Unternehmen um Hilfe zu bitten, die bereits auf digitale Lösungen im Compliance-Bereich vertrauen. Vor diesem Hintergrund ist es nicht überraschend, dass 38 Prozent der großen Unternehmen angeben, einen Anstieg an Beratungsanfragen verzeichnet zu haben. Der Nutzen eines wahrnehmbaren Schutzes vor Wirtschaftskriminalität mitsamt entsprechenden Compliance-Elementen liegt somit nicht nur in der Prävention gegen einschlägige Delikte, sondern bisweilen zudem in einer positiven Außenwirkung des eigenen Unternehmens.

Erhellendes über unsere Daten

5. Über die Studie

Für die vorliegende Studie wurden Vertreter von 1.000 repräsentativ nach Branche, Mitarbeiterzahl und Umsatz ausgewählten Unternehmen in Deutschland zu ihren Erfahrungen im Bereich Wirtschaftskriminalität befragt.

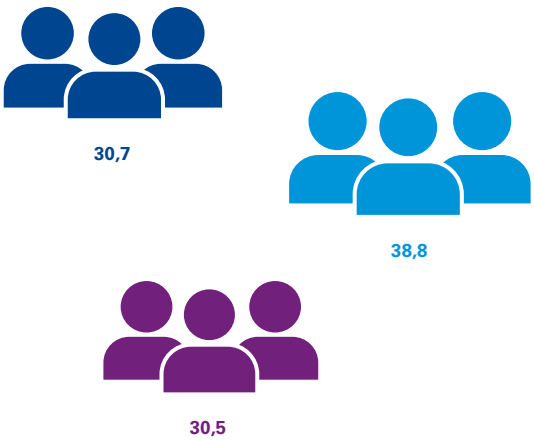
Abbildung 34: Unternehmen nach Branche



- Verarbeitendes Gewerbe (Automobilindustrie, Chemie und Pharma, Energie und Rohstoffe, industrielle Produktion, Technologie)
- Handel (Handel und Konsumgüter)
- Andere Dienstleister (Gesundheitswirtschaft, Medien und Telekommunikation, Öffentlicher Sektor, Banken und Versicherungen)

Quelle: KPMG, Deutschland, 2020 *Angaben in Prozent*

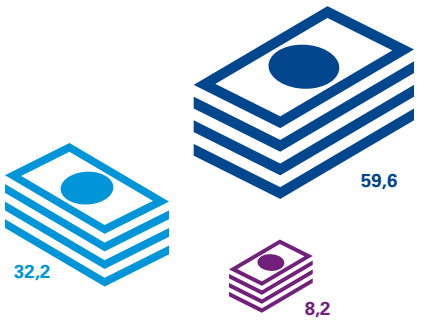
Abbildung 35: Befragte nach Mitarbeiterzahl



- Bis 100 Mitarbeiter
- 101 bis 500 Mitarbeiter
- Über 500 Mitarbeiter

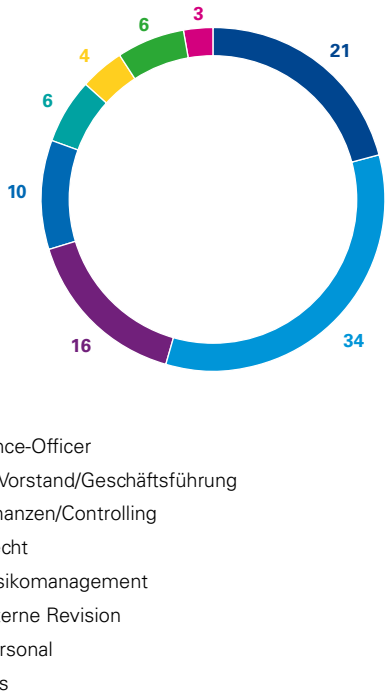
Quelle: KPMG, Deutschland, 2020 *Angaben in Prozent*

Abbildung 36: Unternehmen nach Umsatz



Quelle: KPMG, Deutschland, 2020 *Angaben in Prozent*

Abbildung 37: Funktion des Ansprechpartners



Quelle: KPMG, Deutschland, 2020 *Angaben in Prozent*

Wie bei den vorherigen Ausgaben dieser Studie wurde das Sozialforschungsinstitut Kantar in Bielefeld mit den telefonischen Interviews durch speziell geschulte Mitarbeiter beauftragt. Die Erfahrung hat gezeigt, dass die Teilnehmer der Studie aufgrund der Komplexität des Themas eine persönliche Befragung wünschen. Die Interviews wurden im Zeitraum von September 2019 bis Januar 2020 durchgeführt. Die konkreten Gesprächspartner und ihre jeweiligen Antworten sind KPMG nicht bekannt.

Der standardisierte Fragebogen orientiert sich an der Struktur der Vorgängerstudie mit Anpassungen bezüglich der diesjährigen Studienschwerpunkte. Außerdem soll der Aufbau der vorliegenden Studie wie schon die Vorgängerversionen mit der ebenfalls von KPMG veröffentlichten Studie „Computerkriminalität in der deutschen Wirtschaft" vergleichbar sein.

Der Fragebogen wurde vom Bereich Forensic der KPMG AG Wirtschaftsprüfungsgesellschaft konzipiert.

» Nicht nur, da sich das Phänomen ständig wandelt, sondern vor allem auch aufgrund neuer regulatorischer Anforderungen – Wirtschaftskriminalität ist und bleibt ein relevantes Thema für deutsche Unternehmen. «

Umfassend unterstützt

6. Über Forensic von KPMG

Der Bereich Forensic von KPMG erbringt Leistungen rund um die Prävention, Aufdeckung und Aufklärung von Wirtschaftskriminalität und Compliance-Verstößen. Das Leistungsspektrum umfasst die folgenden Services:

Forensic Investigations
Unabhängige unternehmensinterne Ermittlungen bei Verdacht wirtschaftskrimineller Handlungen auf Basis erprobter Methoden.

Third Party Risk Management
Beratung bei Identifizierung, Bewertung und Management der verschiedenen Risiken, die mit Third Parties verbunden sind, sowie Unterstützung bei der Einhaltung und Verwaltung von Programmanforderungen an das Risikomanagement.

Datenschutz
Beratung bei der Einrichtung von Datenschutzmanagement-Systemen und Unterstützung bei der Reaktion auf Datenschutzvorfälle.

Anti-Financial Crime (Finanzsektor)
Etablierung von Anti-Financial Crime-Maßnahmen zur Prävention von Geldwäsche, Terrorismusfinanzierung oder Sanktionsverstößen.

Geldwäscheprävention (Nichtfinanzsektor)
Prävention, Aufdeckung und Aufklärung von Geldwäschevorfällen und Unterstützung bei der Einrichtung des geldwäschespezifischen Risikomanagements.

Fraud Risk Management
Unterstützung bei der Konzeption und Implementierung eines ganzheitlichen Fraud Risk Managements.

Corporate Intelligence
Recherche, Analyse und Aufbereitung von Hintergrundinformationen zu Unternehmen, Geschäftspersonen und Vermögenswerten.

Evidence & Disclosure Management
Unterstützung bei allen Electronic Discovery-Aktivitäten von Datenlokalisierung bis zu Sicherung, Dokumentenklassifizierung und Analyse.

Forensic Data Analytics
Unterstützung bei der zielgerichteten Analyse strukturierter Datenbestände zur frühzeitigen Identifikation von Wirtschaftskriminalität.

Cyber Response & Investigation
Unterstützung bei der Eindämmung und Lösung von Cyber-Vorfällen.

KPMG AG
Wirtschaftsprüfungsgesellschaft

Barbara Scheben
Partner, Head of Forensic Deutschland
T +49 69 9587-3737
bscheben@kpmg.com

Alexander Geschonneck
Partner, KPMG Global Forensic Steering Group
T +49 30 2068-1520
ageschonneck@kpmg.com

An dieser Studie haben mitgewirkt:
Jacqueline Becker und Yannik Lindt

www.kpmg.de

www.kpmg.de/socialmedia