HSLU Hochschule Luzern

Wirtschaft
Institut für Finanzdienstleistungen
Zug IFZ

ACFE
Association of Certified Fraud Examiners
Switzerland Chapter

Entwicklung der Wirtschafts-kriminalität in der Schweiz

Studie 2025
Fokusthema: Künstliche Intelligenz

FH Zentralschweiz

Autoren

Susanne Grau
Dozentin und Projektleiterin
Institut für Finanzdienstleistungen Zug IFZ
Hochschule Luzern – Wirtschaft

Prof. Dr. Marco Passardi
Dozent
Institut für Finanzdienstleistungen Zug IFZ
Hochschule Luzern – Wirtschaft

Dr. Jonas Miesner
Wissenschaftlicher Mitarbeiter
Institut für Finanzdienstleistungen Zug IFZ
Hochschule Luzern – Wirtschaft

Mitarbeit	Nathalie Frei
Layout & Design	Manuel Gesslein

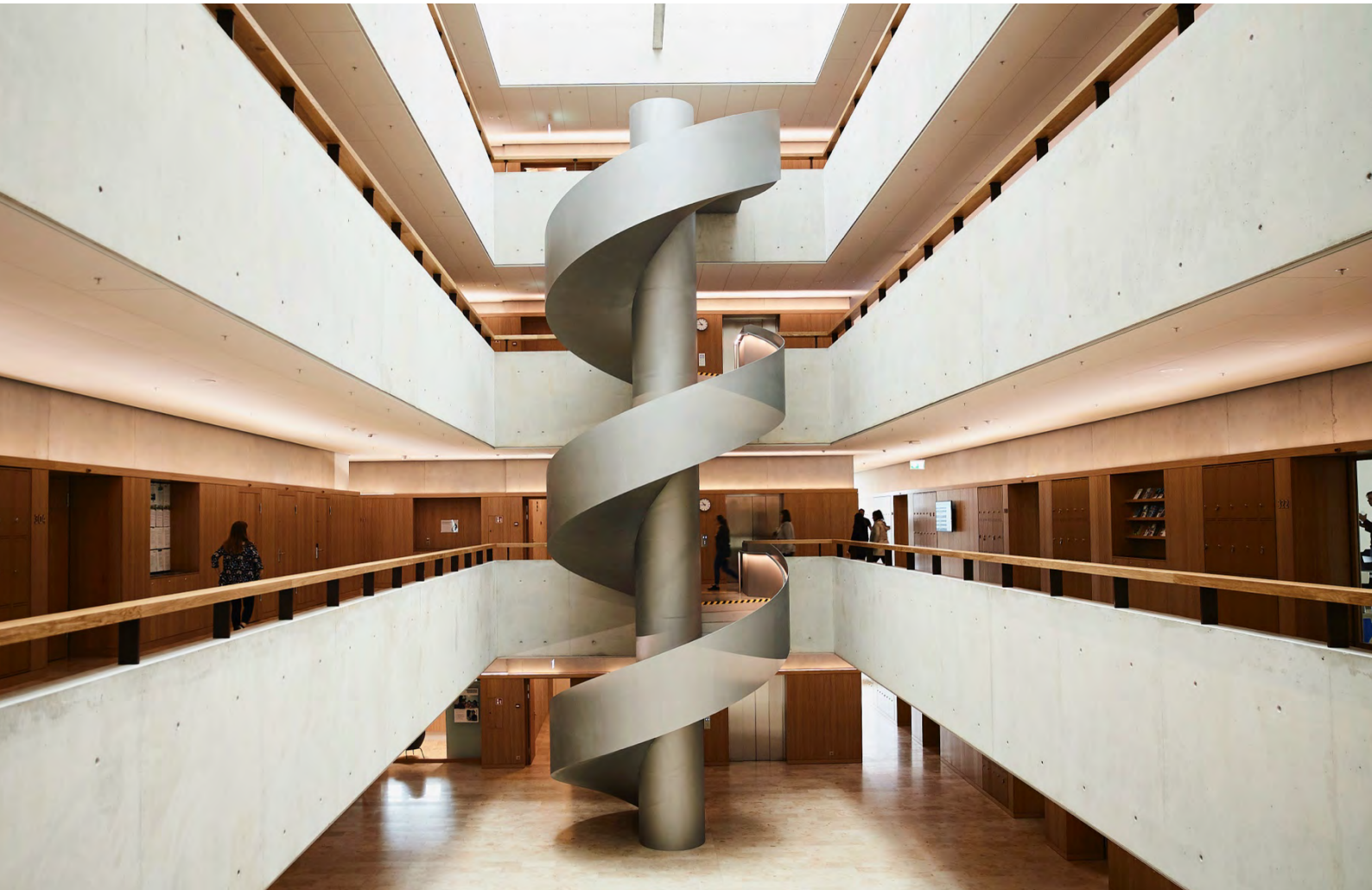
Alle Rechte vorbehalten. Vervielfältigungen jeglicher Art sind ohne Zustimmung des Herausgebers nicht gestattet. Die Inhalte dieser Veröffentlichung dienen ausschliesslich der allgemeinen Information. Sie basieren auf den Einschätzungen der Umfrageteilnehmenden sowie auf der Auswertung weiterer herangezogener Studien. Die Informationen wurden mit grösstmöglicher Sorgfalt recherchiert und zusammengestellt. Dennoch besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und / oder Aktualität, insbesondere haben sie weder rechtsverbindlichen Charakter noch stellen sie eine Rechtsberatung dar.

Institut für Finanzdienstleistungen Zug IFZ
Hochschule Luzern – Wirtschaft

Das Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern – Wirtschaft zählt zu den führenden Schweizer Hochschulinstituten im Finanzbereich. Es verbindet Forschung, Beratung und Weiterbildung mit hoher Praxisnähe – auch in Themen, die für die Sicherheit und Integrität von Unternehmen von zentraler Bedeutung sind, wie Wirtschaftskriminalität, Compliance, Cybercrime und forensische Prüfung.

Aufbauend auf grundlegenden, praxisnahen Bachelor- und konsekutiven Masterstudiengängen bietet das IFZ ein umfassendes Weiterbildungsportfolio im Bereich der Wirtschaftskriminalistik. Hervorzuheben ist der Master of Advanced Studies (MAS) Economic Crime Investigation, welcher sich aus den Certificate of Advanced Studies (CAS) «Economic Crime Investigation Essentials», «Advanced» und «Expert» zusammensetzt. Der MAS Economic Crime Investigation richtet sich gezielt an Fach- und Führungskräfte aus Wirtschaft, Verwaltung, Finanzdienstleistung, Rechtsberatung oder Strafverfolgung, die wirksame Strategien zur Prävention, Aufdeckung und Bekämpfung von Betrug, Geldwäscherei, Korruption, Bilanzdelikten sowie Cyber- und Vermögensdelikten entwickeln wollen. Die modular aufgebaute, seit mehr als 20 Jahren auf dem Markt erfolgreich angebotene, Weiterbildung vermittelt vertiefte Kenntnisse zu rechtlichen Rahmenbedingungen, forensischen Methoden, Standards der Fallaufklärung sowie zur Umsetzung von Schutz- und Compliance-Massnahmen im Unternehmensumfeld. Absolvierende sind darauf vorbereitet, wirtschaftskriminelle Risiken professionell zu erkennen und nachhaltige Lösungen im betrieblichen und regulatorischen Kontext zu schaffen.

Weitere Informationen zu den modularen MAS- und CAS-Studiengängen sowie Spezialisierungen finden Sie direkt beim IFZ.



Vorwort: Unternehmen im Spannungsfeld

Liebe Leserinnen und Leser

Wirtschaftskriminalität stellt Unternehmen in der Schweiz fortwährend und zunehmend vor grosse Herausforderungen. Das Spektrum doloser Handlungen – ob Betrug, Veruntreuung, Korruption oder Verstösse gegen aufsichtsrechtliche Bestimmungen – kann nicht nur zu erheblichen finanziellen Schäden führen, sondern auch das Vertrauen von Investoren, Kunden und der Öffentlichkeit erschüttern. Unternehmen sind sich der Risiken und des Drucks bewusst, weshalb die Prävention, Aufdeckung und Reaktion in Aufsichtsgremien stetig mehr Raum einnimmt.

Aktuell sehen sich Unternehmen einem dynamischen Spannungsfeld ausgesetzt; volatile Märkte, der von USA angezettelte Zollkrieg und strengere regulatorischer Anforderungen stellen Schweizer Unternehmen vor die Herausforderungen, innerhalb dieser verschärften Rahmenbedingungen ihre nachhaltigen Wachstumsstrategien zu verfolgen. Gleichzeitig üben steigende finanzielle und nichtfinanzielle (z. B. ESG) Erwartungen von Investoren und anderen Stakeholdern zusätzlichen Druck aus. Dieses Spannungsgefüge kann als Nährboden für wirtschaftskriminelle Risiken fungieren, wenn interne Kontrollmechanismen und Corporate Governance Prozesse hinter derartigen dynamischen Entwicklungen zurückbleiben – insbesondere in Zeiten künstlicher Intelligenz (KI). Umso wichtiger ist ein holistisches Unternehmensverständnis im Umgang mit Wirtschaftskriminalität, ihrer Risikoeinschätzung und Prävention sowie der kontinuierlichen Verbesserung der Corporate Governance.

Vor diesem Hintergrund haben wir uns entschieden, im Jahr 2025 erstmalig die Studie zur **Entwicklung der Wirtschaftskriminalität in der Schweiz** zu lancieren. Diese Studie positioniert sich im Zentrum dieses Spannungsfeldes – zwischen wachsenden heteronomen Anforderungen und internen Kontrollsystemen der Unternehmen. Unser Ziel ist es, mit dieser Studie fundierte Erkenntnisse über die aktuellen Risiken bezüglich wirtschaftskrimineller Handlungen, das Ausmass der Betroffenheit Schweizer Unternehmen sowie die Wirksamkeit bestehender Präventionsmassnahmen zu gewinnen. Einerseits soll die Untersuchung dazu eine empirische Grundlage für die Risikoeinschätzung bereitstellen. Andererseits sollen die Ergebnisse den Schweizer Unternehmen zur Weiterentwicklung ihrer Schutzmassnahmen gegenüber sich wandelnden Bedrohungsszenarien dienen. Nicht nur die Implementierung, sondern auch die regelmässige Überprüfung der bestehenden Kontrollmechanismen – angepasst an rechtliche, wirtschaftliche und technologische Entwicklungen – sind zur Sicherung nachhaltiger Praktiken sowie wirtschaftlichen Erfolges unerlässlich. Sie bilden das Fundament für Vertrauen von Investoren, Kunden und Geschäftspartnern.

Wir wünschen Ihnen eine spannende Lektüre und hoffen, dass Sie aus dieser Studie gewinnbringende Erkenntnisse für Ihre tägliche Arbeit gewinnen werden.

Ihre Susanne Grau
Leitung Wirtschaftskriminalistik am
Institut für Finanzdienstleistungen Zug IFZ
der Hochschule Luzern – Wirtschaft

Ihr Michael Dietrich
Präsident ACFE Switzerland Chapter
Association of Certified Fraud Examiners

Executive Summary

Wirtschaftskriminalität stellt in der Schweiz eine erhebliche Herausforderung für Unternehmen dar. Sie manifestiert sich nicht nur in klassischen Delikten wie Betrug, Veruntreuung und Korruption, sondern zunehmend auch in Cyberkriminalität. Diese Delikte verursachen erhebliche wirtschaftliche Schäden und untergraben das Vertrauen von Investoren, Kunden und der Öffentlichkeit in die Integrität der betroffenen Unternehmen. Vor diesem Hintergrund besteht ein zentrales Ziel der Studie darin, aktuelle Risiken und Trends in Bezug auf Wirtschaftskriminalität innerhalb der Schweiz darzulegen. Ausserdem sollen Aussagen über die Arten von wirtschaftskriminellen Handlungen sowie geeigneter Präventionsmassnahmen hergeleitet werden.

Vor diesem Hintergrund wird das Risiko der Betroffenheit als eher hoch eingeschätzt, wobei nur ein Viertel der befragten Schweizer Unternehmen über Vorfälle von Wirtschaftskriminalität im eigenen Unternehmen in den letzten zwei Jahren berichten; die Tätergruppen sind dabei zunehmend auch externe Personen, die sich digitaler Werkzeuge bedienen.

Ein weiterer Schwerpunkt der Studie liegt auf der Rolle von Präventionsmassnahmen und der Corporate Governance. Viele Unternehmen weisen weiterhin Schwächen in der systematischen Erfassung wirtschaftskrimineller Risiken auf, was deren Bekämpfung erschweren kann. Dennoch wird die Notwendigkeit, verschiedene Kontroll- und Präventionsmassnahmen – insbesondere mit Bezug zu informationstechnischen Systemen – umzusetzen, von fast allen Unternehmen erkannt. Umgesetzte Massnahmen folgen etablierten Best Practices; internationale Studien heben vergleichbare Ergebnisse hervor.

Besonders in Zeiten fortschreitender technologischer Entwicklungen, wie der Nutzung von Künstlicher Intelligenz (KI) – dem Fokusthema dieser Studie 2025 – sehen Unternehmen neue Herausforderungen und Chancen für die Prävention von Wirtschaftskriminalität. Ein einheitliches Bild zeichnet sich noch nicht ab – es gibt Vorreiter und Unternehmen mit Nachholbedarf. Cyberkriminalität wird zwar oft als eine zukünftige Herausforderung betrachtet, jedoch wird das Risiko von KI-generierten Betrugsversuchen, wie etwa Deep Fakes, häufig unterschätzt. Auf Grundlage dieses Fokusthemas – Künstliche Intelligenz – wird ein Framework (SAFER) vorgestellt, das Unternehmen im Umgang mit KI-generierten Betrugsversuchen unterstützt.

Damit Schweizer Unternehmen auch in Zukunft sowohl erfolgsorientiert als auch nachhaltig (insb. SDG 16) agieren können, sollten sie ihre Schutzmechanismen an die sich schnell ändernden technologischen und wirtschaftlichen Rahmenbedingungen anpassen. Insbesondere im Bereich der Cyberkriminalität sollten Präventionsbemühungen verstärkt werden. Dies umfasst sowohl die Implementierung wirksamerer Kontrollsysteme als auch die Förderung einer offenen und werteorientierten Unternehmenskultur, die persönliche Anreize setzt, Verantwortung zu übernehmen und zur Sicherheit der Unternehmen beizutragen.

FRAUD

Inhaltsverzeichnis

2 Autoren

3 Vorwort: Unternehmen im Spannungsfeld

5 Executive Summary

7 Inhaltsverzeichnis

8 1 Stand der Forschung und Zielsetzung

8 1.1 Begriffliches – Wirtschaftskriminalität und Künstliche Intelligenz

9 1.2 Aktuelles und Zielsetzung

11 2 Studiendesign

11 2.1 Teilnehmende Unternehmen

15 3 Generelle Entwicklung und eigene Betroffenheit

15 3.1 Risikoentwicklung

21 3.2 Eigene Betroffenheit

25 4 Risikoprävention und Corporate Governance

32 5 Fokusthema 2025 – Künstliche Intelligenz

32 5.1 KI im Fokus der Unternehmen

37 5.2 Handlungsempfehlungen zu KI-generierten Betrugsversuchen

40 6 Fazit und Ausblick zur Studie

41 Literaturverzeichnis

43 Abbildungsverzeichnis

44 Studienpartner

1 Stand der Forschung und Zielsetzung

1.1 Begriffliches – Wirtschaftskriminalität und Künstliche Intelligenz

Der Begriff *Wirtschaftskriminalität* wird allgemein für Straftaten verwendet, die einen wirtschaftlichen Bezug aufweisen oder im Rahmen von unternehmerischen bzw. beruflichen Tätigkeiten begangen werden (Brunner et al. 2024b). Eine klare Begriffsbestimmung ist insofern anspruchsvoll, als der Ausdruck kein fest umrissener juristischer Terminus ist. Auch das geltende Schweizer Recht kennt keine Legaldefinition des Begriffs Wirtschaftskriminalität; sie findet typischerweise in einem wirtschaftlichen Umfeld statt, im Rahmen einer an sich legitimen Tätigkeit – beispielsweise innerhalb eines Unternehmens oder einer Behörde – und grenzt sich dadurch von der organisierten Kriminalität im Milieu der Unterwelt ab (siehe Bundesamt für Polizei fedpol 2023). Meist handelt es sich um nicht-gewaltsame, vermögensbezogene Delikte, die auf finanzielle oder anderweitige, unrechtmässige Vorteile abzielen (Brunner et al. 2024b). Typische Erscheinungsformen sind insbesondere Betrugs- und Korruptionsdelikte, Geldwäscherei, Bilanzfälschungen (etwa durch falsche Finanzberichterstattung), Insiderhandel, Steuerhinterziehung sowie weitere Verstösse, die Unternehmen, Investoren oder staatliche Institutionen schädigen. Derartige strafbare Handlungen können in das Kernstrafrecht (Art. 137 – 172ter StGB) und in das Nebenstrafrecht (weitere Gesetzte) differenziert werden (Brunner et al. 2024b).

Internationale Definitionsbemühungen sind insbesondere auf Edwin H. Sutherland zurückzuführen, der in den 1930er Jahren das bis dahin vorherrschende Verständnis, dass Kriminalität primär ein Phänomen der Unterschicht sei, hinterfragte. In diesem Zusammenhang definierte er «White Collar Crime» als eine rechtswidrige Handlung, die von einer verantwortlichen Person mit einem hohen sozialen Status im Rahmen ihrer beruflichen Tätigkeit begangen wird (Sutherland 1949). Seine Darlegungen haben auch weiterhin im Kern Bestand – dies zeigt beispielsweise die KPMG Studie - Global profiles of the fraudster (2025). Damit tragen sie in der Kriminalistik zum unmittelbaren Verständnis bezüglich des Profils der Täter sowie mittelbar zum Modus Operandi bei. Beide Sichtweisen – die rechtliche Einordnung einzelner Tatbestände und die gesamtgesellschaftliche Betrachtung des Täterverhaltens – tragen zu einem holistischen Verständnis von Wirtschaftskriminalität bei.

Künstliche Intelligenz

Vor dem Hintergrund des diesjährigen Schwerpunktthemas wird ein weiterer Fokus auf das Verständnis von *Künstlicher Intelligenz* (KI) gelegt. KI ist ein Sammelbegriff für Technologien und Methoden, die es Computern ermöglichen, menschliche Intelligenzleistungen (wie Lernen, Problemlösen, Wahrnehmung und Sprachverstehen) nachzuahmen. Wesentliche Merkmale solcher Systeme sind die Fähigkeit, aus Erfahrungen, d. h. Daten, zu lernen und mit Unsicherheit umzugehen, um autonom Entscheidungen zu treffen. Man unterscheidet hierbei zwischen schwacher KI, die auf eng begrenzte Aufgaben spezialisiert ist (z. B. Sprachassistenten), und starker KI, einer hypothetischen künstlichen allgemeinen Intelligenz auf menschlichem Niveau, die bislang noch nicht erreicht ist. (Stryker und Kavlakoglu 2024)

Die historische Entwicklung der Künstlichen Intelligenz ist durch zahlreiche Meilensteine geprägt, die gemeinsam dem heutigen Verständnis den Weg ebneten (nicht abschliessend): Die Ursprünge der Künstlichen Intelligenz reichen bis ins 18. Jahrhundert zurück: 1711 entwickelte Gottfried Leibniz den Calculus Ratiocinator, der als formale Grundlage für Denkmaschinen gilt. 1936 formulierte Alan Turing mit der Turingmaschine ein mathematisches Modell für theoretische Informatik. Die eigentliche Geburtsstunde der modernen KI fand 1956 auf der Dartmouth Conference statt, bei der John McCarthy den Begriff Artificial Intelligence prägte.

In den folgenden Jahrzehnten entstanden bedeutende Systeme wie der Chatbot ELIZA (1966, Joseph Weizenbaum) und das erste Expertensystem MYCIN (1972, Ted

Shortliffe). Ein grosser Meilenstein bildete 1997 der Sieg des Schachcomputers Deep Blue (IBM) über den Weltmeister Garry Kasparov. Die Entwicklung setzte sich mit Watson (IBM) fort, der 2011 in der Quizshow Jeopardy! gegen menschliche Kontrahenten gewann. Seit 2022 ist eine zunehmende Verbreitung der Large Language Modells (LLMs) zu beobachten, wie ChatGPT. Durch diese neuen generativen KI-Ansätze ist es möglich, Deep-Learning-Modelle im Vorfeld mit umfangreichen Datenmengen zu trainieren (Stryker und Kavlakoglu 2024; Grzybowski et al. 2024). Vor diesem Hintergrund sehen sich Unternehmen mit der neuen Herausforderung konfrontiert, geeignete Massnahmen zu treffen, KI-assistierter Wirtschaftskriminalität vorzubeugen.

1.2 Aktuelles und Zielsetzung

In der Schweiz nimmt Wirtschaftskriminalität eine zunehmend bedeutsame Stellung bei den Unternehmen ein. Einerseits haben mehrere spektakuläre Fälle und Skandale in der jüngeren Vergangenheit das öffentliche Bewusstsein für Wirtschaftsdelikte geschärft – wie z. B. der Wirecard-Skandal von 2020, der als beispielloser Fall von Bilanzmanipulation in die Wirtschaftsgeschichte einging (Karami 2022). Andererseits zeigen statistische Entwicklungen eine deutliche Zunahme der Vorfälle von dolosen Handlungen. So ist beispielsweise die Zahl der gemeldeten Betrugsfälle (Art. 146 StGB) nach der Polizeilichen Kriminalstatistik (PKS 2025) von 9‘304 im Jahr 2013 auf 24‘195 Fälle im Jahr 2022 angestiegen (+160 %), wobei die aufgeklärten Betrugsfälle einen deutlich geringeren Anstieg aufzeigen (siehe auch Brunner et al. 2024a).

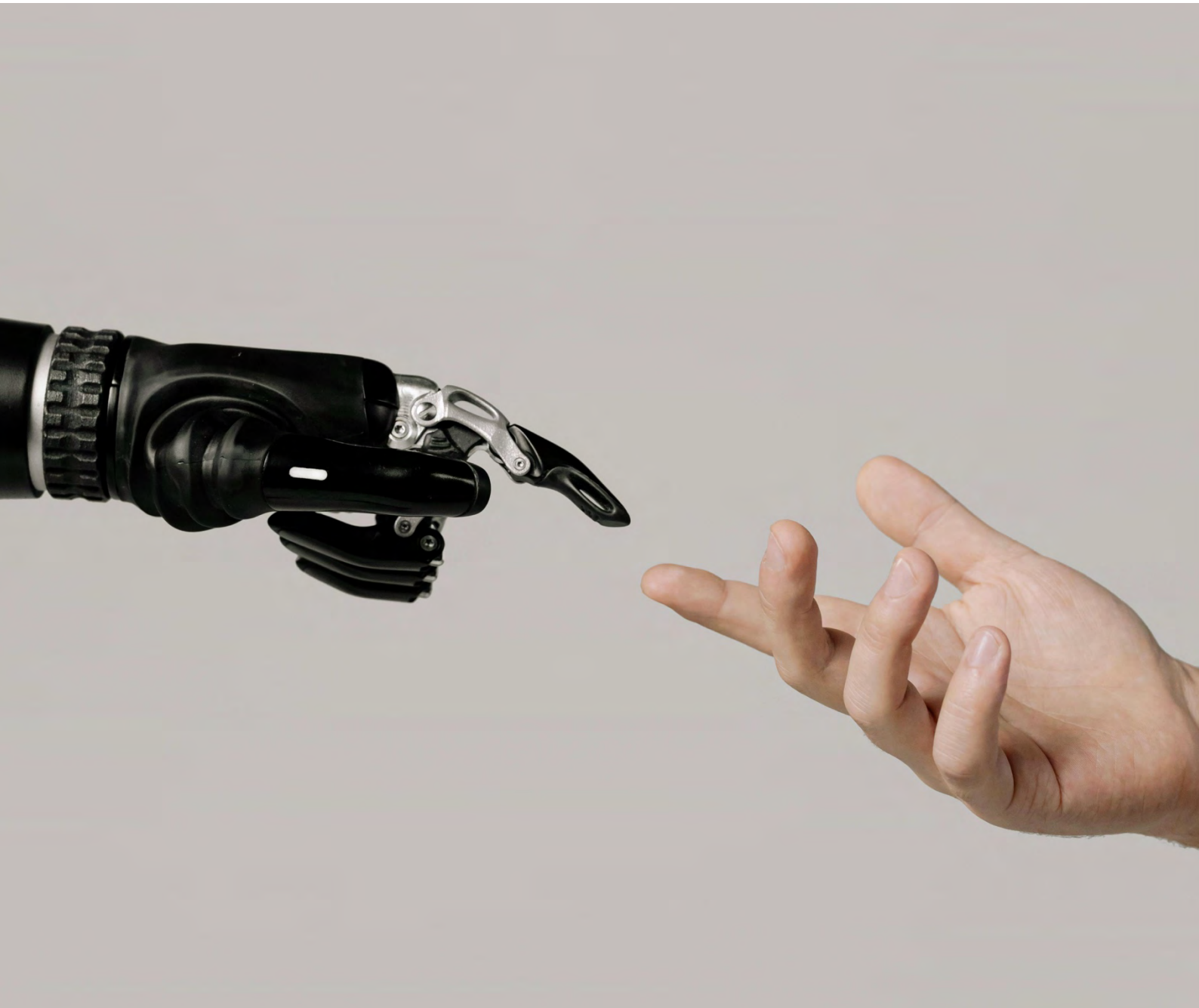
Auf internationaler Ebene ist fast jedes zweite Unternehmen (46 %) zwischen 2020 und 2022 betroffen gewesen; dies geht aus einer internationalen Studie von PwC hervor (n= 1‘296 Unternehmen aus 53 Ländern), wobei dieser Anteil rückblickend stagniert (PwC 2022). Eine deutliche Dynamik zeigt sich demgegenüber in der Entwicklung und Verlagerung der Deliktarten. Eine Studie von Ernst & Young aus dem Jahr 2014 zeigt, dass nahezu die Hälfte der befragten Unternehmen (48 % von insgesamt 2‘700 Unternehmen aus 59 Ländern) das Risiko von Cyberkriminalität als gering einschätzte (EY 2014). Während klassische Betrugs- und Veruntreuungsdelikte weiterhin existieren, nimmt die Cyberkriminalität zunehmend mehr Raum bei den Unternehmen ein (siehe KPMG 2020; PwC 2022). Auch in der Schweiz sind Unternehmen vor cyberkriminellen Akteuren nicht gefeit. Die fortschreitende Digitalisierung und die Vernetzung globaler Geschäftsprozesse haben die Angriffsflächen erheblich vergrössert, wodurch Cyberkriminalität zu einer der gravierendsten Bedrohungen für die Unternehmenssicherheit avanciert ist.

Bei den Tätern handelt es sich – insbesondere in Europa – um zunehmend externe Personen (PwC 2022), was auf eine Verlagerung hin zu organisierter Kriminalität schliessen lässt, die vor Ländergrenzen keinen Halt macht. Strafverfolgungsbehörden sehen sich hierbei – im internationalen Raum – mit vielfältigen Herausforderungen konfrontiert: In einer globalisierten, digital vernetzten Wirtschaft können Straftäter ihre illegal erzielten Gewinne mühelos in andere Länder transferieren und dort durch komplexe Firmengeflechte oder anonyme Offshore-Konten verschleiern (Eurojust 2024). Moderne Technologien erlauben es zudem, Delikte aus der Ferne in denjenigen Jurisdiktionen zu begehen, die die schwächsten Kontrollen und Strafverfolgungsmechanismen aufweisen. Dies führt dazu, dass Strafverfolgungsbehörden vor grossen Problemen stehen, da sich die Beweiserhebung und Täterermittlung über Ländergrenzen hinweg äusserst komplex und zeitaufwändig gestalten kann.

Gesamthaft betrachtet sind die ökonomischen Schäden, die durch das Spektrum doloser Handlungen entstehen, erheblich. Laut dem *2024 Report to the Nations* der Association of Certified Fraud Examiners (ACFE), einer Studie, in der über 20‘000 Fälle von *occupational fraud* analysiert wurden, verlieren Organisationen weltweit jährlich etwa 5 % ihres Umsatzes durch verschiedene Arten von Betrug. Hochgerechnet auf die Summe aller Bruttoinlandsprodukte weltweit im Jahr 2022 entspricht dies einem Verlust von über 5 Billionen USD (ACFE 2024b).

Doch wie nehmen Unternehmen in der Schweiz die Verbreitung und Ausprägung wirtschaftskrimineller Handlungen tatsächlich wahr? Gibt es Unterschiede zu internationalen Entwicklungen, oder spiegeln sich globale Trends auch in der Schweizer Unternehmenslandschaft wider? An diese zentralen Fragen möchten wir, das **Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern – Wirtschaft**, gemeinsam mit dem Switzerland Chapter der **Association of Certified Fraud Examiners (ACFE),** mit unserer **Studie zur Entwicklung der Wirtschaftskriminalität in der Schweiz** anknüpfen. Unser Ziel ist es, mit den Erkenntnissen der Studie Unternehmen zu unterstützen, aktuelle wirtschaftskriminelle Risiken besser einzuschätzen und gezielt zu adressieren.

Zur vertiefenden Analyse der Ergebnisse werden ergänzend ausgewählte Erkenntnisse der ACFE berücksichtigt. Darüber hinaus tragen weitere einschlägige Studien mit geografischem Bezug zur Schweiz sowie internationale Vergleichsstudien zu einer vertiefenden Betrachtung von Wirtschaftskriminalität in der Schweiz bei. Ein Teil der Untersuchung widmet sich wiederkehrenden, grundlegenden Themen, um langfristige Entwicklungen und Trends im Bereich der Wirtschaftskriminalität zu analysieren. Ergänzend dazu setzt die Studie mit einem wechselnden Fokusthema gezielte Akzente auf besonders aktuelle und drängende Herausforderungen – im Fokus dieser ersten Studie steht Künstliche Intelligenz.



2 Studiendesign

2.1 Teilnehmende Unternehmen

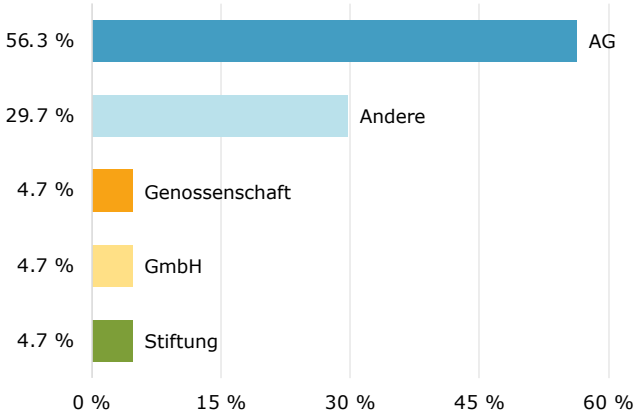
Um ein umfassendes Bild der Entwicklung der Wirtschaftskriminalität in der Schweiz zu erhalten, richtete sich die Umfrage gezielt an Entscheidungsträger in den Bereichen Legal und Compliance sowie Risk. Ausserdem zur Umfrage eingeladen wurden Geschäftsführer, Mitglieder des Verwaltungsrats, Inhaber sowie Entscheidungsträger mit direkter Verantwortung im Bereich Wirtschaftskriminalität. Durch die gezielte Ansprache dieser Schlüsselpersonen in Unternehmen wird sichergestellt, dass die erhobenen Daten auf fundierten Erfahrungen basieren und ein Aufzeigen aktueller Trends und Herausforderungen im Bereich der Wirtschaftskriminalität aus der Praxis ermöglichen.

Aus ca. 350 Zugriffen auf die Umfrage liessen sich 64 vollständige Datensätze ableiten; ausgeschlossen wurden Eingaben, die die Umfrage nicht vollständig beantworteten. Dies entspricht einer Ausschöpfungsrate von 18 %, wobei sich die Ausfälle unsystematisch gestalteten. Die Mehrheit der Teilnehmenden beantwortete die Umfrage auf Deutsch (89 %), gefolgt von Französisch (8 %) und Englisch (3 %).

Zur Rechtsform

Mehr als die Hälfte der befragten Personen sind in Unternehmen tätig, die als Aktiengesellschaft (AG) organisiert sind (56.3 %). Den zweithöchsten Anteil bildet mit 29.7 % die Kategorie „andere“ Organisationsformen. Diese umfasst – nachträglich zusammengefasst – privatrechtliche Unternehmensformen (z. B. Einzelunternehmen, Kollektiv- oder Kommanditgesellschaften), öffentlich-rechtliche Institutionen (wie Gemeinden, kantonale oder eidgenössische Verwaltungen und Gerichte) sowie spezifische Rechtsformen wie Anstalten oder Anwaltspraxen. Jeweils 4.7 % der Teilnehmenden stammen aus Genossenschaften, GmbHs sowie Stiftungen. Die vorliegende Verteilung lässt erkennen, dass insbesondere kapitalmarktorientierte oder Organisationen mit juristischem Bezug an der Erhebung teilgenommen haben bei denen Fragen der Corporate Governance, der internen Kontrollen sowie der aufsichtsrechtlichen Pflichten besondere Bedeutung entfalten und teilweise regulatorisch vorgeschrieben sind.

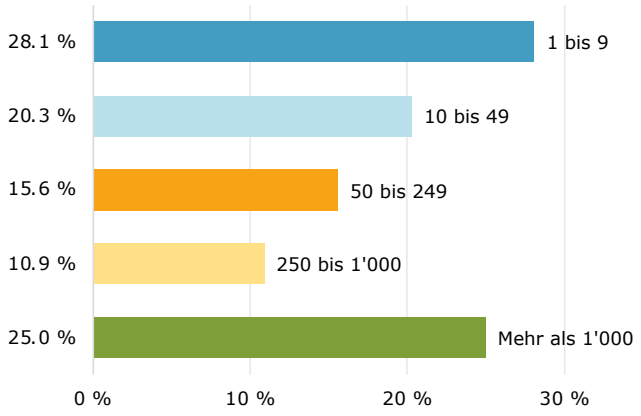
Abb. 1: Rechtsform der Unternehmen



Anzahl der Mitarbeitenden

Anknüpfend an die dargestellte Verteilung der Rechtsformen lässt sich auch in Bezug auf die Unternehmensgrösse eine heterogene Zusammensetzung der Stichprobe feststellen. Unternehmen mit 1 bis 9 Mitarbeitenden (28.1 %) und Unternehmen mit über 1‘000 Mitarbeitenden (25.0 %) machen zusammen 53.1 % der Stichprobe aus. Diese beiden Gruppen markieren somit die beiden Pole der Unternehmensgrössen in der Erhebung. Für die Kategorie der kleinen und mittleren Unternehmen (KMU) – also Unternehmen mit weniger als 250 Mitarbeitenden – ergibt sich ein Anteil von insgesamt 64.0 % an der Stichprobe. Diese setzt sich aus Unternehmen mit 1 bis 9 Mitarbeitenden (28.1 %), 10 bis 49 Mitarbeitenden (20.3 %) sowie 50 bis 249 Mitarbeitenden (15.6 %) zusammen.

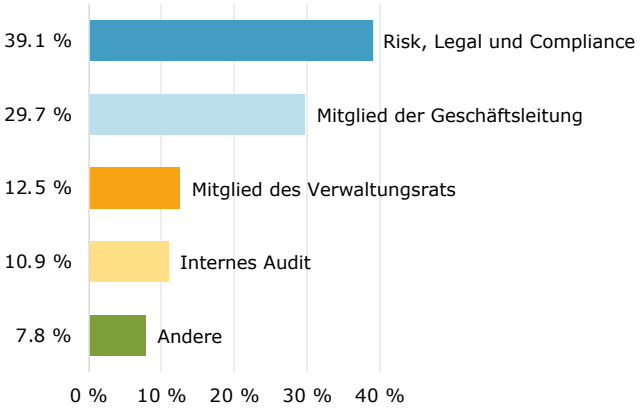
Abb. 2: Anzahl der beschäftigten Mitarbeiter im Unternehmen



Position der Teilnehmenden im Unternehmen

Auch hinsichtlich der Funktion der teilnehmenden Personen ergibt sich ein vielschichtiges Bild, welches mit den Fokusgruppen gemäss der Zielsetzung übereinstimmt. Der grösste Anteil entfällt auch mit 39.1 % auf Fachpersonen aus dem Bereich Risk, Legal und Compliance. 29.7 % der Befragten sind Mitglieder der Geschäftsleitung, gefolgt von Mitgliedern des Verwaltungsrats mit 12.5 % sowie dem Internen Audit mit 10.9 %. Weitere 7.8 % gaben an, andere Funktionen im Unternehmen zu bekleiden (u.a. aus dem Bereich Finanzen, Verwaltung & öffentliche Ämter).

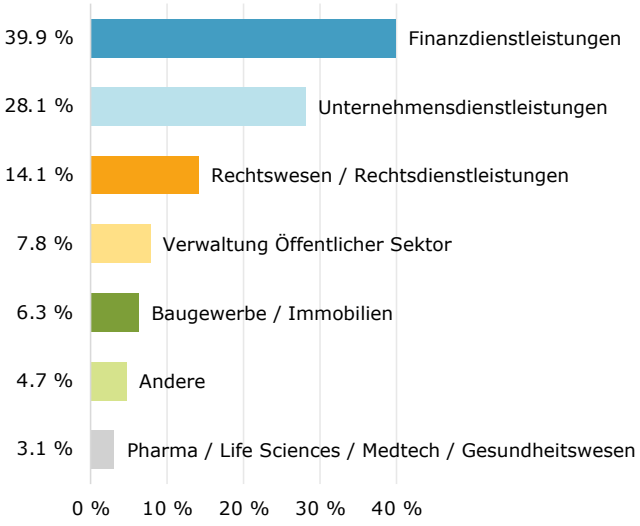
Abb. 3: Position der Teilnehmenden im Unternehmen



Branchen der Unternehmen

An erster Stelle steht der Bereich Finanzdienstleistungen, aus dem 35.9 % der teilnehmenden Unternehmen stammen, gefolgt von Unternehmensdienstleistungen mit 28.1 %. Auf dem dritten Rang folgen Rechtswesen bzw. Rechtsdienstleistungen mit 14.1 %. Geringer vertreten sind der öffentliche Sektor bzw. die Verwaltung (7.8 %), das Baugewerbe / Immobilien (6.3 %), die Kategorie „Andere“ – u.a. spezialisierte Verwaltung, Industrie – (4.7 %) sowie Pharma, Life Sciences, Medtech und Gesundheitswesen mit 3.1 %.

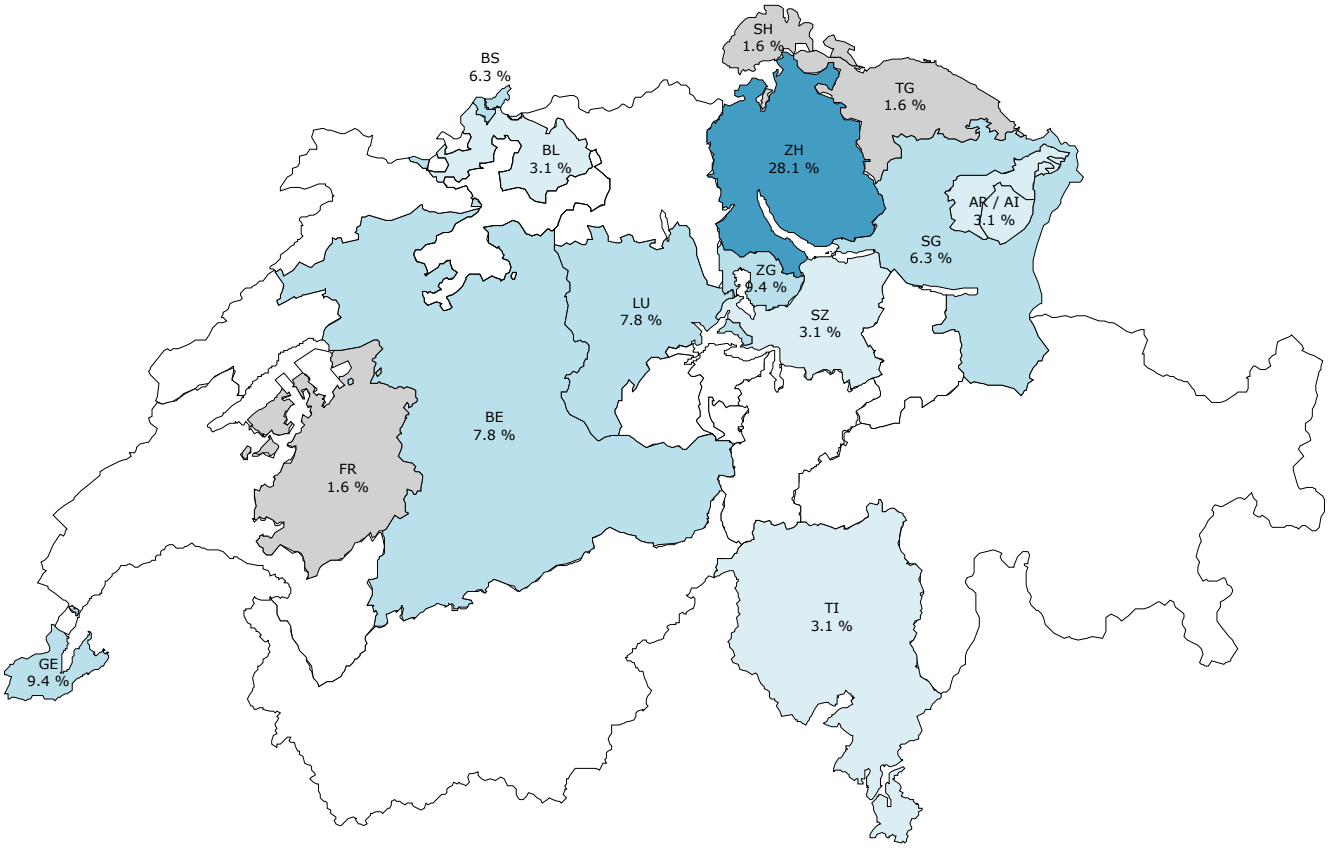
Abb. 4: Branchenstruktur der befragten Unternehmen



Räumliche Verteilung der Unternehmen in der Schweiz

Über ein Viertel (28.1 %) der befragten Unternehmen sind im Kanton Zürich verortet und nehmen den mit Abstand grössten Anteil ein, gefolgt von Genf und Zug mit je 9.4 %. Auf den folgenden Positionen liegen Luzern und Bern mit jeweils 7.8 %, sowie Basel-Stadt und St. Gallen mit je 6.3 %. Die Herkunft der teilnehmenden Unternehmen ist demnach schwerpunktmässig in der Zentralschweiz, der Region Zürich sowie der Nordwestschweiz zu verorten; ebendiese Grossregionen, die durch ihre Dienstleistungsorientierung bekannt sind.

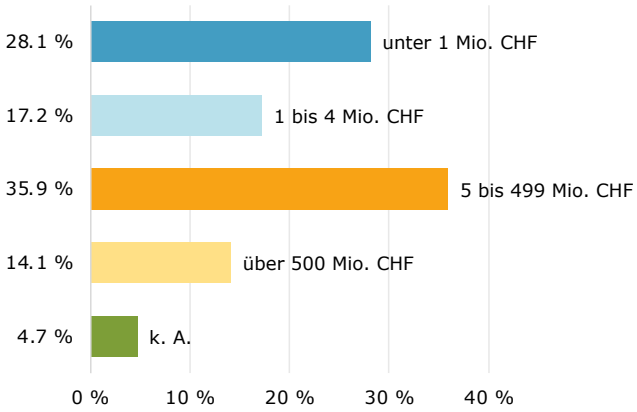
Abb. 5: Räumliche Verteilung der Unternehmen in der Schweiz



Erwirtschafteter Umsatz der Unternehmen

Bezüglich des Umsatzes zeigt sich eine deutliche Streuung innerhalb der Stichprobe, mit einer Konzentration im mittleren bis oberen Segment. 35.9 % der teilnehmenden Unternehmen erwirtschafteten im letzten abgeschlossenen Geschäftsjahr einen Umsatz zwischen CHF 5 Mio. und CHF 499.9 Mio., während 28.1 % einen Umsatz von unter CHF 1 Mio. angaben. Weitere 17.2 % ordnen sich im Bereich zwischen CHF 1 Mio. und CHF 4,9 Mio. ein. Einen Jahresumsatz von über CHF 500 Mio. meldeten 14.1 %.

Abb. 6: Erwirtschafteter Umsatz im letzten abgeschlossenen Geschäftsjahr



3 Generelle Entwicklung und eigene Betroffenheit

Aufbauend auf den strukturellen Merkmalen der teilnehmenden Unternehmen widmet sich das folgende Kapitel 3 der Einschätzung zur generellen Entwicklung wirtschaftskrimineller Handlungen sowie der konkreten Betroffenheit im eigenen Unternehmenskontext. Damit rücken die subjektive Risikoentwicklung (Abschnitt 3.1) ebenso wie die eigenen Erfahrungswerte im Umgang mit dolosen Handlungen (Abschnitt 3.2) in den Vordergrund. Ergänzend herangezogen werden Erkenntnisse aus bestehender Fachliteratur, die die empirischen Ergebnisse für die Schweiz in einen grösseren Zusammenhang einordnen.

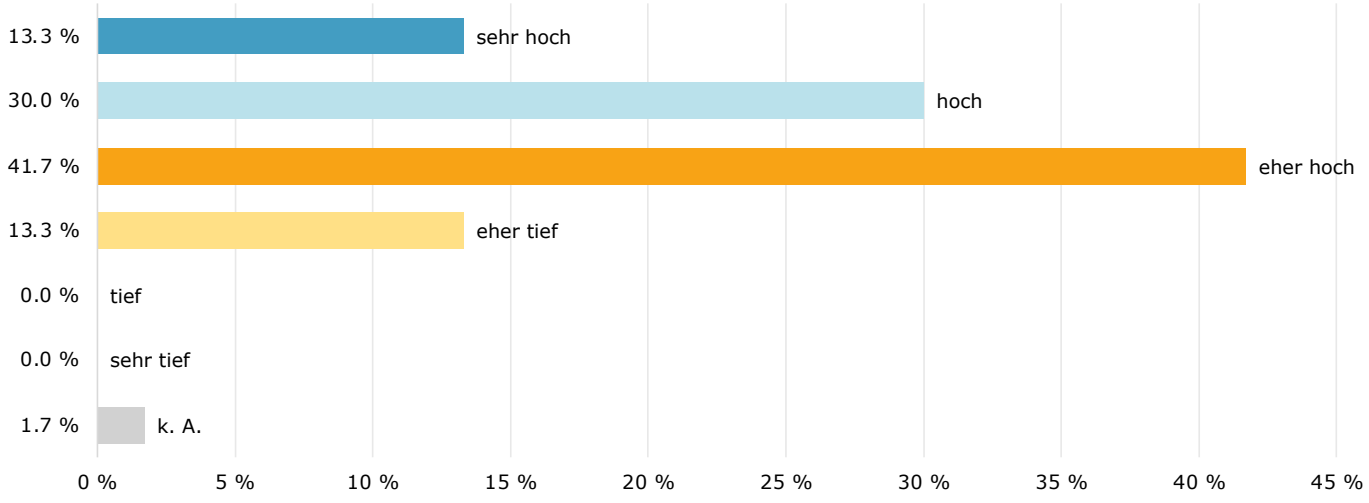
3.1 Risikoentwicklung

85 % der Unternehmen schätzen das Risiko wirtschaftskrimineller Handlungen im Allgemeinen als hoch ein.

Die befragten Unternehmen in der Schweiz zeigen ein ausgeprägtes Risikobewusstsein hinsichtlich wirtschaftskrimineller Bedrohungen im gesamtwirtschaftlichen Umfeld. Wie Abbildung 7 verdeutlicht, stufen 41.7 % das Risiko als eher hoch, 30 % als hoch und 13.3 % sogar als sehr hoch ein. Zusammengenommen bewerten damit 85 % der Teilnehmenden das Risiko für Schweizer Unternehmen, von Wirtschaftskriminalität betroffen zu sein, als hoch. Nur 13.3 % schätzen es als eher tief ein; eine Einschätzung des allgemeinen Risikos als tief oder sehr tief erfolgte durch kein Unternehmen.

Diese Wahrnehmung deckt sich weitgehend mit den Ergebnissen der KPMG-Studie „Im Spannungsfeld – Wirtschaftskriminalität in Deutschland“ (2020), in der 78 % der befragten deutschen Unternehmen angaben, dass Wirtschaftskriminalität ein relevantes oder sehr relevantes Risiko darstellen würde. Besonders auffällig ist in beiden Studien, dass lediglich ein geringer Teil der Befragten das Risiko als gering oder vernachlässigbar einstuft. Wirtschaftskriminalität wird folglich als substanzielle und konstante Bedrohung wahrgenommen.

Abb. 7: Selbstwahrnehmung des Risikos hinsichtlich wirtschaftskrimineller Handlungen

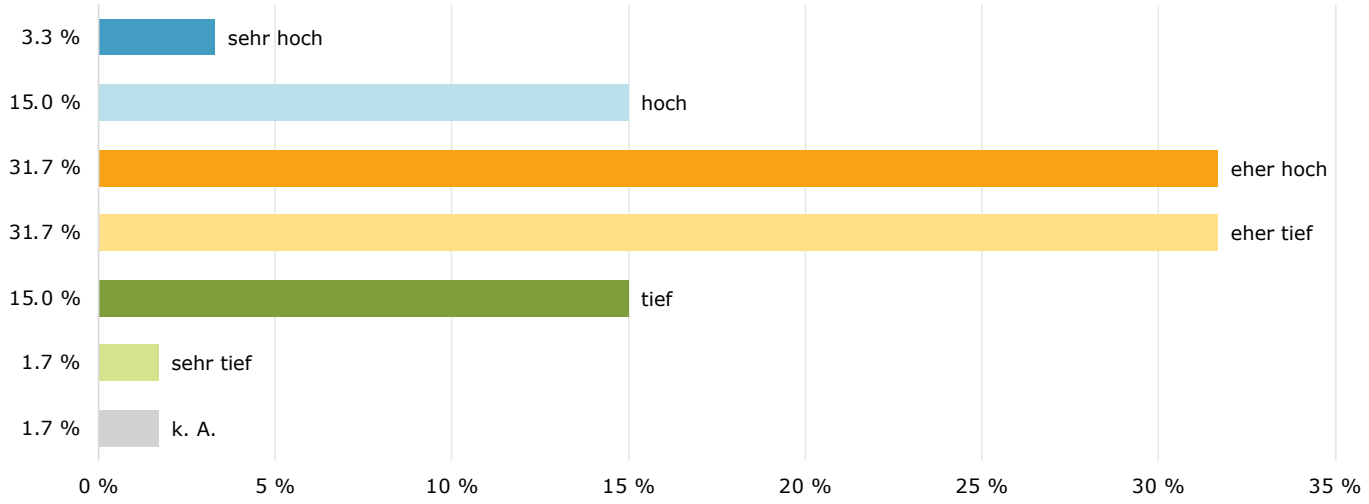


Die Wahrnehmung des Risikos innerhalb der eigenen Organisation fällt im Vergleich zur Gesamteinschätzung des allgemeinen Risikos zurückhaltend aus.

Während fast 80 % der Befragten das Risiko für Schweizer Unternehmen zumindest als «eher hoch» einschätzen (vgl. Abbildung 7), fällt die Beurteilung des eigenen wirtschaftskriminellen Gefährdungspotenzials differenzierter und verhaltener aus. Jeweils 31.7 % der Befragten sehen ihr Unternehmen als eher hoch bzw. eher tief gefährdet. 15.0 % schätzen das Risiko als hoch, weitere 3.3 % als sehr hoch ein. Gleichzeitig beurteilen 16.7 % das eigene Risiko als tief oder sehr tief.

Diese annähernd ausgeglichene Verteilung spiegelt ein ambivalentes Risikobewusstsein wider. Einerseits erkennt ein substanzieller Teil der Unternehmen die reale Gefahr von wirtschaftskriminellen Handlungen betroffen sein zu können, andererseits bleibt ein ähnlich grosser Anteil bei einer eher optimistischen Einschätzung bezüglich der eigenen Organisation. Der Vergleich zur allgemeinen Risikoeinschätzung legt einen Wahrnehmungsunterschied zwischen Fremd- und Eigenrisiko offen. Diese kognitive Diskrepanz ist in der psychologischen Risikoforschung bekannt – häufig gehen Organisationen davon aus, dass andere stärker gefährdet sind als sie selbst (*optimism bias*). Auch andere Studien zeigen diese Tendenz auf (z. B. KPMG 2020).

Abb. 8: Selbstwahrnehmung des Risikos hinsichtlich wirtschaftskrimineller Handlungen

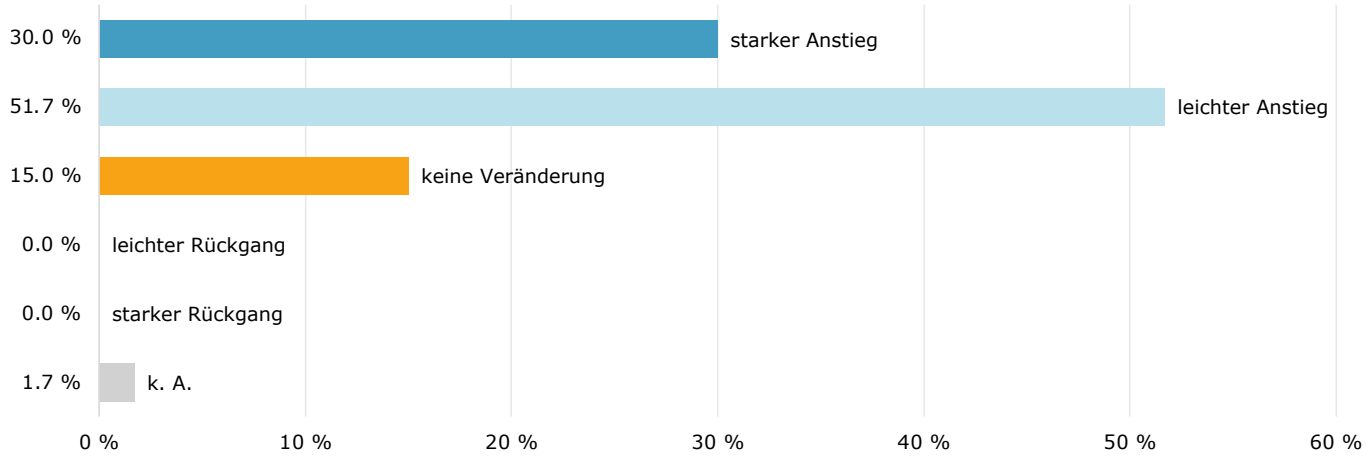


Mehr als 80 % rechnen mit einem Anstieg der Wirtschaftskriminalität in der Schweiz in den kommenden 12 Monaten.

Die Einschätzungen zur künftigen Entwicklung der Wirtschaftskriminalität in der Schweiz fallen eindeutig aus: 51.7 % der befragten Unternehmen rechnen mit einem leichten Anstieg wirtschaftskrimineller Vorfälle in den kommenden zwölf Monaten, während 30 % sogar von einem starken Anstieg ausgehen. Nur 15 % antizipieren keine Veränderung, Rückgänge werden nicht erwartet. Damit rechnen mehr als drei Viertel der Befragten mit einer Zunahme wirtschaftskrimineller Aktivitäten.

Diese Risikowahrnehmung spiegelt eine vergleichbare Tendenz wider, wie sie auch internationale Erhebungen festhalten. Gemäss der KPMG-Studie in Deutschland erwarten nahezu ein Drittel der Befragten eine Zunahme des Risikos für das eigene Unternehmen in den folgenden zwei Jahren, während nur 6 % von einer Reduktion ausgingen (KPMG 2020). Gesamtheitlich lassen diese Einschätzungen auf sich wandelnde Risikofaktoren schliessen, die potenziell als Nährboden für dolose Handlungen fungieren können (siehe folgende Frage).

Abb. 9: Einschätzung der Wirtschaftskriminalität in den kommenden 12 Monaten

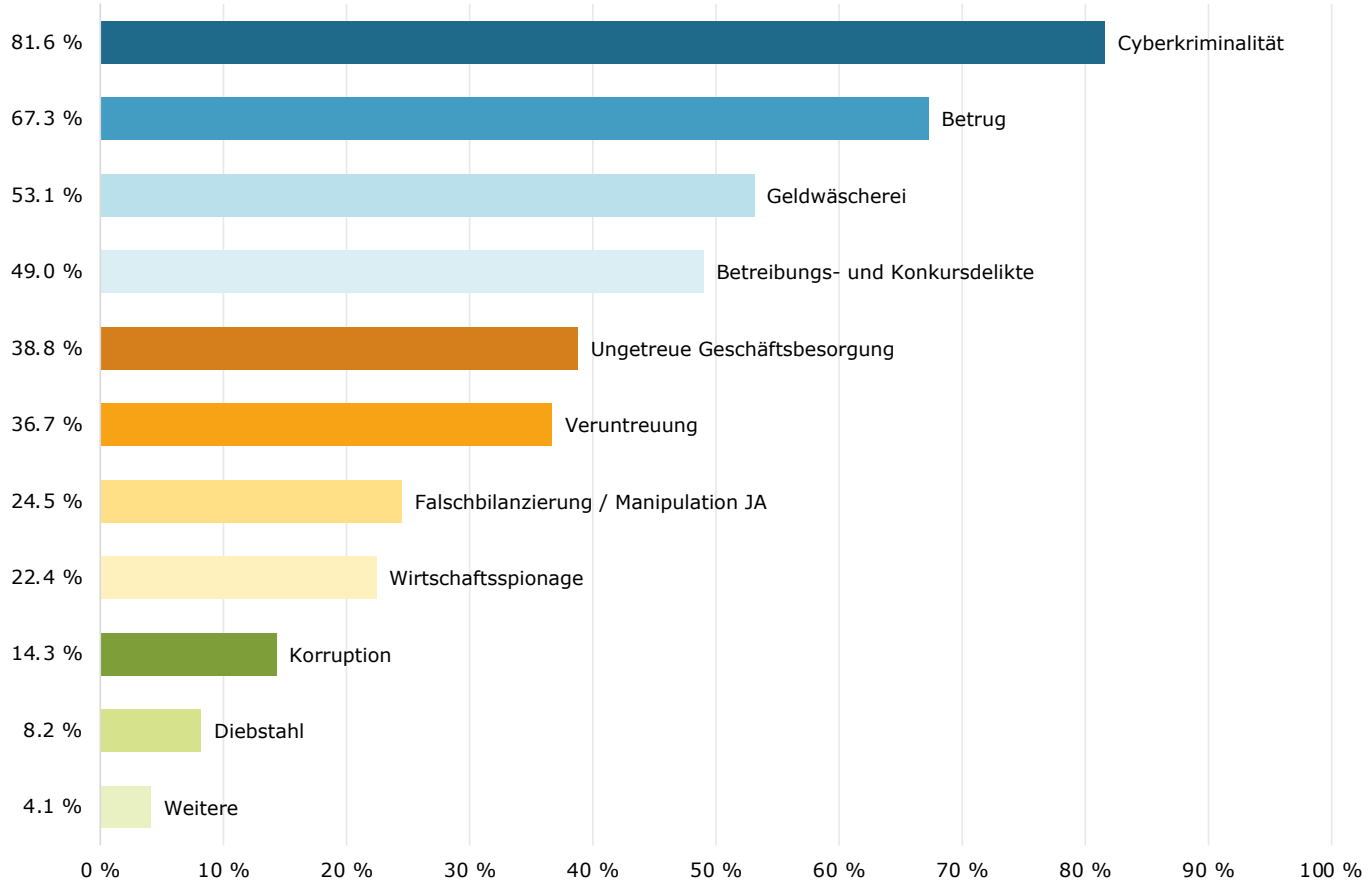


Unternehmen erwarten einen deutlichen Anstieg bei Cyberkriminalität – mehr als bei Betrug und Geldwäscherei.

Im Rahmen einer weiterführenden Fragestellung wurden ausschliesslich Teilnehmende befragt, die von einem Anstieg der Wirtschaftskriminalität in der Schweiz ausgehen. Die Ergebnisse zeigen eine klare Fokussierung auf bestimmte Deliktsformen: 81.6 % der Befragten erwarten einen Zuwachs bei der Cyberkriminalität – deutlich mehr als bei allen anderen Kategorien. An zweiter Stelle folgt Betrug mit 67.3 %, dicht gefolgt von Geldwäscherei mit 53.1 %. Auch Betreibungs- und Konkursdelikte werden von nahezu der Hälfte der Unternehmen (49.0 %) als zunehmend riskant eingeschätzt. Darüber hinaus betrachten die Teilnehmenden auch ungetreue Geschäftsbesorgung (38.8 %), Veruntreuung (36.7 %) sowie Falschbilanzierung oder Manipulation (24.5 %) als Delikte mit steigendem Gefährdungspotenzial. Im Vergleich dazu fallen die Einschätzungen für Korruption (14.3 %), Diebstahl (8.2 %) und Wirtschaftsspionage (22.4 %) deutlich niedriger aus, was darauf hindeutet, dass diese Deliktsformen in der aktuellen Risikowahrnehmung der Unternehmen eine nachgelagerte Rolle spielen.

Auch in der deutschen KMPG-Studie bereiten Datendelikte den Befragten die grössten Sorgen (86 %); Betrug und Untreue (53 %) sowie Falschbilanzierung (26 %) werden in Deutschland ähnlich bedeutend wahrgenommen. Unterschiede existieren bei dem Delikt Geldwäsche (33 % vs. 53.1 % Schweiz). (KPMG 2020) Die aktuelle und zukünftige Stellung der Cyberkriminalität im Unternehmenskontext ist keineswegs eine lokale Entwicklung. Auch der ACFE Report to the Nations 2024 weist auf eine Vulnerabilität der Unternehmen aufgrund der zunehmenden Verbreitung digitaler Formate (z. B. digitaler Dokumente) hin (ACFE 2024b).

Abb. 10: Erwarteter Anstieg von Wirtschaftsdelikten

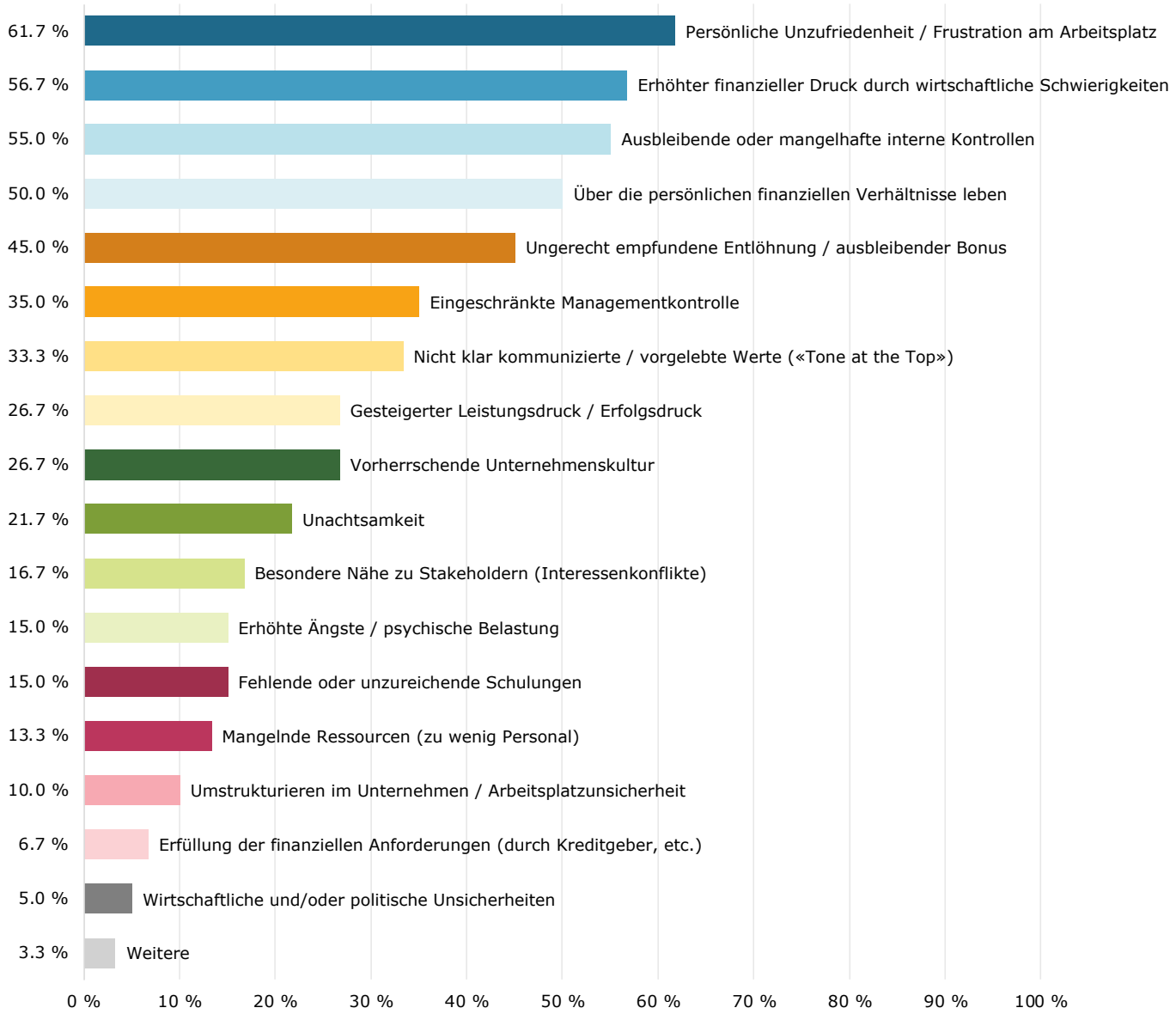


N = 196 Antworten

Risikofaktoren für wirtschaftskriminelle Vorfälle formen ein anschauliches Beispiel des „Fraud Triangle“.

Abschliessend in diesem Abschnitt 3.1 zur Risikoentwicklung erfolgt eine differenzierte Betrachtung der von den Befragten identifizierten Risikofaktoren. Sie werden anhand des Fraud Triangle nach Cressey (1950) eingeordnet; dieses Modell beschreibt drei zentrale Komponenten, die das Entstehen wirtschaftskrimineller Handlungen begünstigen: Druck (Pressure), Gelegenheit (Opportunity) und Rechtfertigung (Rationalization).

Abb. 11: Risikofaktoren für wirtschaftskriminelle Vorfälle



N = 298 Antworten

Druck (Pressure): Finanzielle und persönliche Belastungen als zentrale Treiber

An erster Stelle der wahrgenommenen Risikofaktoren steht mit 61.7 % die persönliche Unzufriedenheit oder Frustration am Arbeitsplatz. Diese kann – in Kombination mit finanziellen Schwierigkeiten (56.7 %) sowie einem Leben über den persönlichen Verhältnissen (50.0 %) – erheblichen Druck erzeugen, der die Bereitschaft zu wirtschaftskriminellen Handlungen begünstigt; dies zeigt auch der ACFE Report (2024b) auf.

Internationale Studien bestätigen diese Einschätzung: Leistungsdruck vom Management (45 %) sowie externer Druck aus der Makroebene (49 %), wie z. B. Inflation und Regulierung, werden im Rahmen der EY Studie (2024) als wichtige Treiber für Integritätsverletzungen bezeichnet. Eine konstante Zunahme dieser Faktoren ist auch in Deutschland ersichtlich, jedoch weniger signifikant (KPMG 2020).

Gelegenheit (Opportunity): Schwächen von internen Kontrollen

Neben dem persönlichen Druck spielt die Gelegenheit eine entscheidende Rolle. In der Umfrage wurden mangelhafte interne Kontrollen (55.0 %), eingeschränkte Managementkontrolle (35.0 %) und Unachtsamkeit (21.7 %) als wesentliche Treiber für wirtschaftskriminelle Vorfälle genannt. Diese Schwächen eröffnen Angriffsflächen für dolose Handlungen. Rückblickend bildet die Kenntnis um mangelhafte interne Kontrollen keine neue Erkenntnis (z. B. seit 2014, siehe KPMG 2020). Der „Gelegenheit“ präventiv durch interne Kontrollen vorzubeugen sollte jedem Schweizer Unternehmen bekannt sein (siehe ACFE 2024b).

Rechtfertigung (Rationalization): Legitimation des Fehlverhaltens

Der dritte Aspekt des Fraud Triangle, die Rechtfertigung, beschreibt den inneren Prozess, mit dem Täter ihr Handeln rationalisieren. Unzufriedenheit mit der Entlöhnung (45.0 %), Frustration am Arbeitsplatz (61.7 %, siehe auch Druck) oder ungerecht empfundene Entlöhnung (45 %) können als moralische Rechtfertigung von Fehlverhalten fungieren. Auch der „Tone at the Top“ (33.3 %) kann die intrinsische Rechtfertigung mit beeinflussen, ob Mitarbeitende wirtschaftskriminelles Verhalten als akzeptabel wahrnehmen.

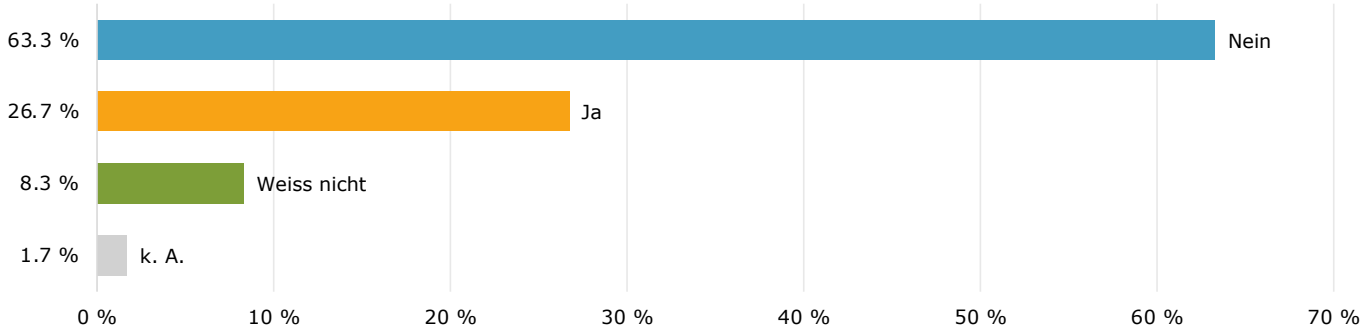
3.2 Eigene Betroffenheit

Nur 26.7 % der Unternehmen berichten über aufgedeckte Vorfälle von Wirtschaftskriminalität in den letzten 24 Monaten.

Die erste Frage in diesem Abschnitt 3.2. zur eigenen Betroffenheit beleuchtet die Häufigkeit identifizierter Vorfälle von Wirtschaftskriminalität in den vergangenen zwei Jahren. Lediglich 26.7 % der befragten Unternehmen gaben an, in diesem Zeitraum wirtschaftskriminelle Handlungen aufgedeckt zu haben. Der Grossteil der Unternehmen (63.3 %) berichtet hingegen, keine entsprechenden Vorfälle festgestellt zu haben. Weitere 8.3 % der Befragten konnten keine klare Einschätzung („weiss nicht“) diesbezüglich abgeben.

Damit stehen die Ergebnisse dieser Erhebung eher im Kontrast zu internationalen Studien. So zeigt die PwC Global Economic Crime and Fraud Survey 2022, dass weltweit rund 46 % der Unternehmen mindestens einen Fall von Wirtschaftskriminalität innerhalb der letzten 24 Monate entdeckten (PwC 2022).

Abb. 12: Identifizierte Vorfälle von Wirtschaftskriminalität in den vergangenen 2 Jahren



Betrug und Cyberkriminalität belegen in der Schweiz die ersten beiden Positionen der identifizierten Vorfälle wirtschaftskrimineller Handlungen.

Ein Block an Folgefragen adressierte die Unternehmen, die sich in den vergangenen zwei Jahren mit Vorfällen von Wirtschaftskriminalität konfrontiert sahen (d. h. 26.7 % der Befragten, siehe Abbildung 12). Die Erhebung zeigt, dass Betrug (bei 9 Unternehmen) und Cyberkriminalität (bei 7 Unternehmen) die am häufigsten aufgedeckten Deliktsformen in Schweizer Unternehmen darstellen (Abbildung 13); dieses Ergebnis kongruiert mit der Erwartung der Unternehmen, welche Wirtschaftsdelikte auch in Zukunft an Bedeutung zunehmen werden (siehe Abbildung 10).

Vorfälle von Geldwäscherei und Diebstahl wurden bei fünf Unternehmen aufgedeckt, während Veruntreuung nur in zwei Unternehmen vorlag. Weniger präsent waren Delikte wie Korruption, Falschbilanzierung und Wirtschaftsspionage, die jeweils nur einmal genannt wurden. Innerhalb der Kategorie Betrug verteilen sich die Vorfälle auf verschiedene Unterformen, wobei Beschaffungsbetrug (33 %), Anlagebetrug (22 %) sowie Sozialversicherungsbetrug (22 %) die höchsten Anteile aufweisen. Auch Rechnungsbetrug, Steuerbetrug und Investitionsbetrug wurden mehrfach gemeldet (jeweils 11 %). Im Bereich der Cyberkriminalität dominieren insbesondere Phishing-

Angriffe zu 86 %, gefolgt von Hacking (71 %) und Social Engineering (29 %). Weitere Bedrohungen wie Ransomware, DDoS-Attacken und betrügerische Anzeigen wurden in jeweils 29 % der Fälle genannt.

Die Gesamtschadenssumme ist dabei nicht immer eindeutig zu bemessen – dies zeigt auch diese Studie (siehe Abbildung 15). Das liegt einerseits an der Dunkelziffer (z. B. BKA 2024), die nur angenommen werden kann; das gleiche gilt für versteckte Kosten (z. B. Dyck et al. 2023; Beneish et al. 2013). Nach der ACFE (2024b) bemisst sich der Verlust allein durch Betrug auf 5 % der jährlichen Einnahmen eines Unternehmens.

Cyberkriminalität im internationalen Vergleich

Im internationalen Vergleich zeigt sich ein ähnliches Bild. Beispielsweise wird Cyberkriminalität (44 %) als weltweit häufigste Form wirtschaftskrimineller Handlungen im Rahmen der PwC Global Economic Crime and Fraud Survey 2024 genannt – in Deutschland sind es sogar 55 % (PwC 2024). Diese Beobachtungen knüpfen an die gleichnamige PwC Studien aus dem Jahr 2022 und 2020 an, in der Cyberkriminalität branchenübergreifend die ersten drei Positionen aufgedeckter Vorfälle von Wirtschaftskriminalität belegte (PwC 2022, 2020). Eine komplementäre Perspektive einnehmend bildet Cybersecurity nach den Ergebnissen des EY Global Integrity Report 2022 das wichtigste zu beachtende Risiko (27 %) für Unternehmen bei Partnerschaften mit anderen Unternehmen bzw. M&A-Prozessen (EY 2022). Die Gefahr für Unternehmen hervorgehend aus dem digitalen Raum ist demnach nicht neu – sie gewinnt jedoch insbesondere in der Schweiz rasant an Bedeutung.

Weitere Daten aus der Schweiz

Verdeutlicht wird die nationale Tragweite der Cyber Wirtschaftskriminalität unter Einbeziehung der Polizeilichen Kriminalstatistik (PKS). Im Jahr 2024 wurden in der Schweiz 55‘413 Straftaten von Cyber-Wirtschaftskriminalität polizeilich erfasst; dies entspricht 93.9 % aller erfassten Vorfälle digitaler Kriminalität. Im Vorjahr waren es noch 40‘496 Straftaten (+ 37 %). Damit scheinen Schweizer Unternehmen in den vergangenen 12 Monaten zunehmend häufiger von Cyberkriminalität betroffen gewesen zu sein als der Rest der DACH-Region. Beispielsweise wurden in Deutschland im Jahr 2024 131‘391 Fälle von Cyberkriminalität erfasst (- 2.2 %, 2023). In Österreich belief sich der Rückgang auf - 5.4 % auf 62‘328 Fälle im Jahr 2024.

Abb. 13: Aufgedeckte Arten von Wirtschaftskriminalität in den letzten 24 Monaten

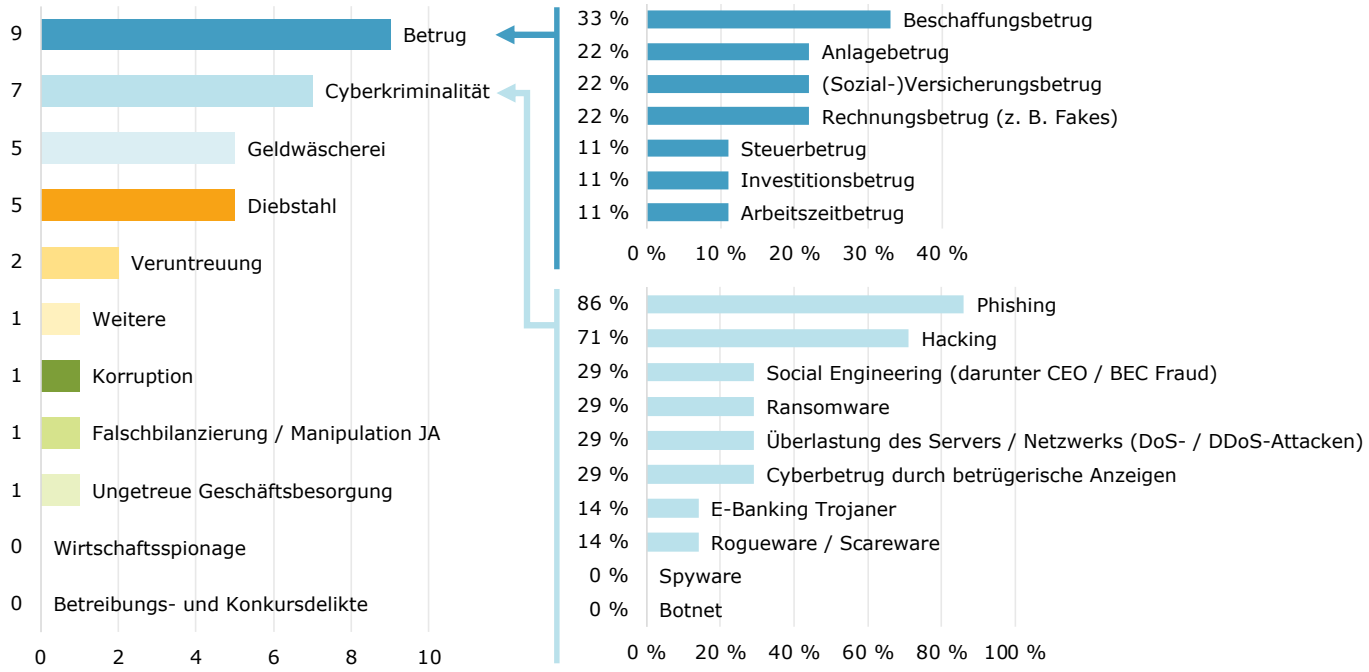


Abb. 14: Anzahl aufgedeckter Vorfälle von Wirtschaftskriminalität in den letzten 24 Monaten

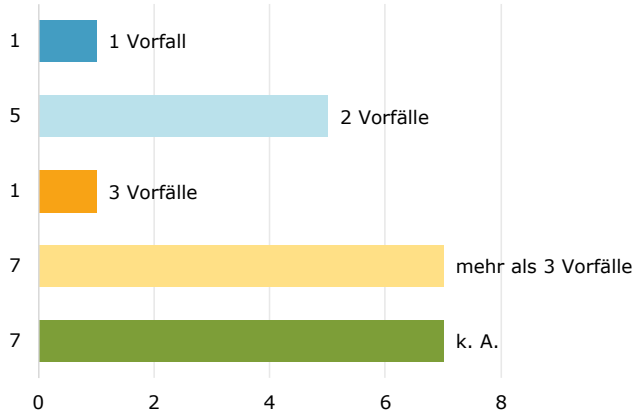
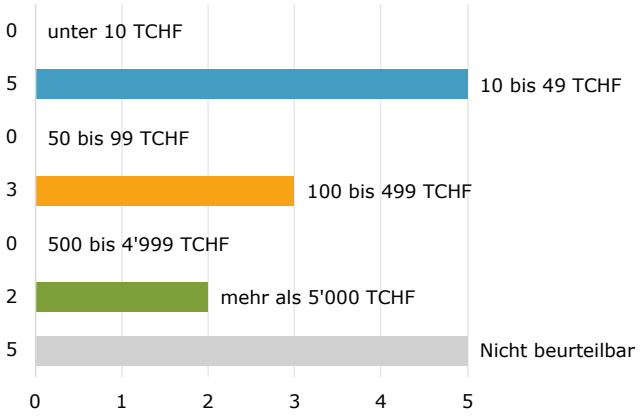


Abb. 15: Gesamtschaden durch Wirtschaftskriminalität in den letzten 24 Monaten

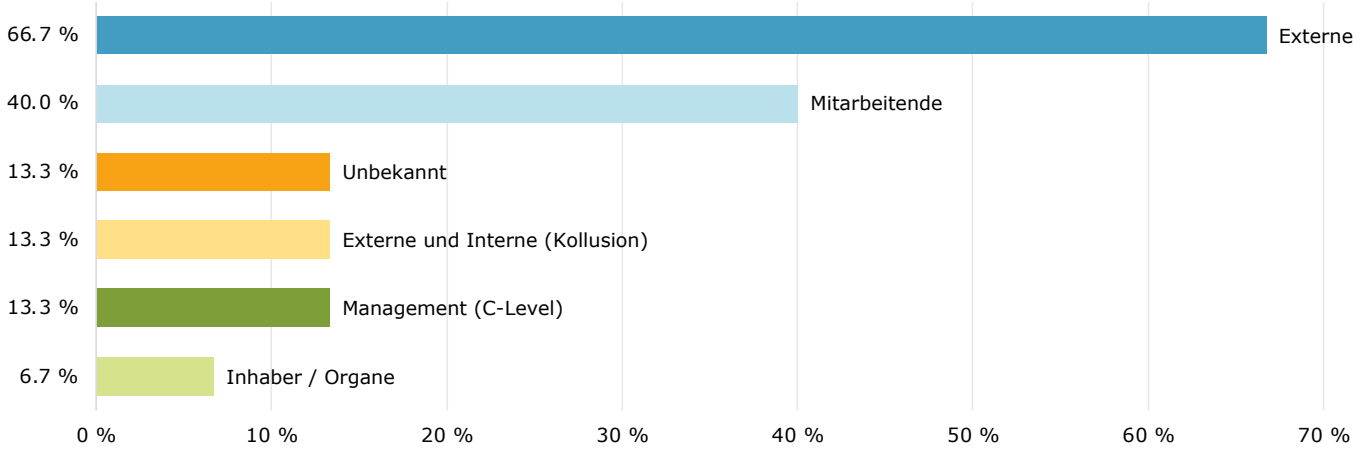


Externe Täter sind Hauptverursacher wirtschaftskrimineller Handlungen.

Die Umfrageergebnisse verdeutlichen, dass wirtschaftskriminelle Handlungen in Schweizer Unternehmen überwiegend durch externe Akteure begangen werden; 66.7 % der aufgedeckten Vorfälle sind auf externe Täter zurückzuführen. An zweiter Stelle folgen interne Mitarbeitende mit einem Anteil von 40.0 %. Weitere jeweils 13.3 % der Fälle entfallen auf die Kategorien unbekannt, externe und interne Täter in Kollusion sowie Management (C-Level). Lediglich 6.7 % der Vorfälle wurden Inhabern oder Organen zugeschrieben.

Diese Ergebnisse aus der Schweiz stehen im Einklang mit internationalen Erhebungen. Auch die Ergebnisse der PwC Global Economic Crime and Fraud Survey (2022) lassen zunehmend auf externe Akteure als dominierende Tätergruppe schliessen, wobei in Europa dieser Anteil mit 56 % am höchsten ist (weltweit 43 %). Auch der EY Global Integrity Report (2024) hebt eine zunehmende Beteiligung dritter Parteien (68 %) bei Integritätsverletzung hervor. Die Beteiligung interner Mitarbeitenden gestaltet sich im internationalen Vergleich stagnierend bis rückläufig (z. B. PwC 2022).

Abb. 16: Involvierte Tätergruppen



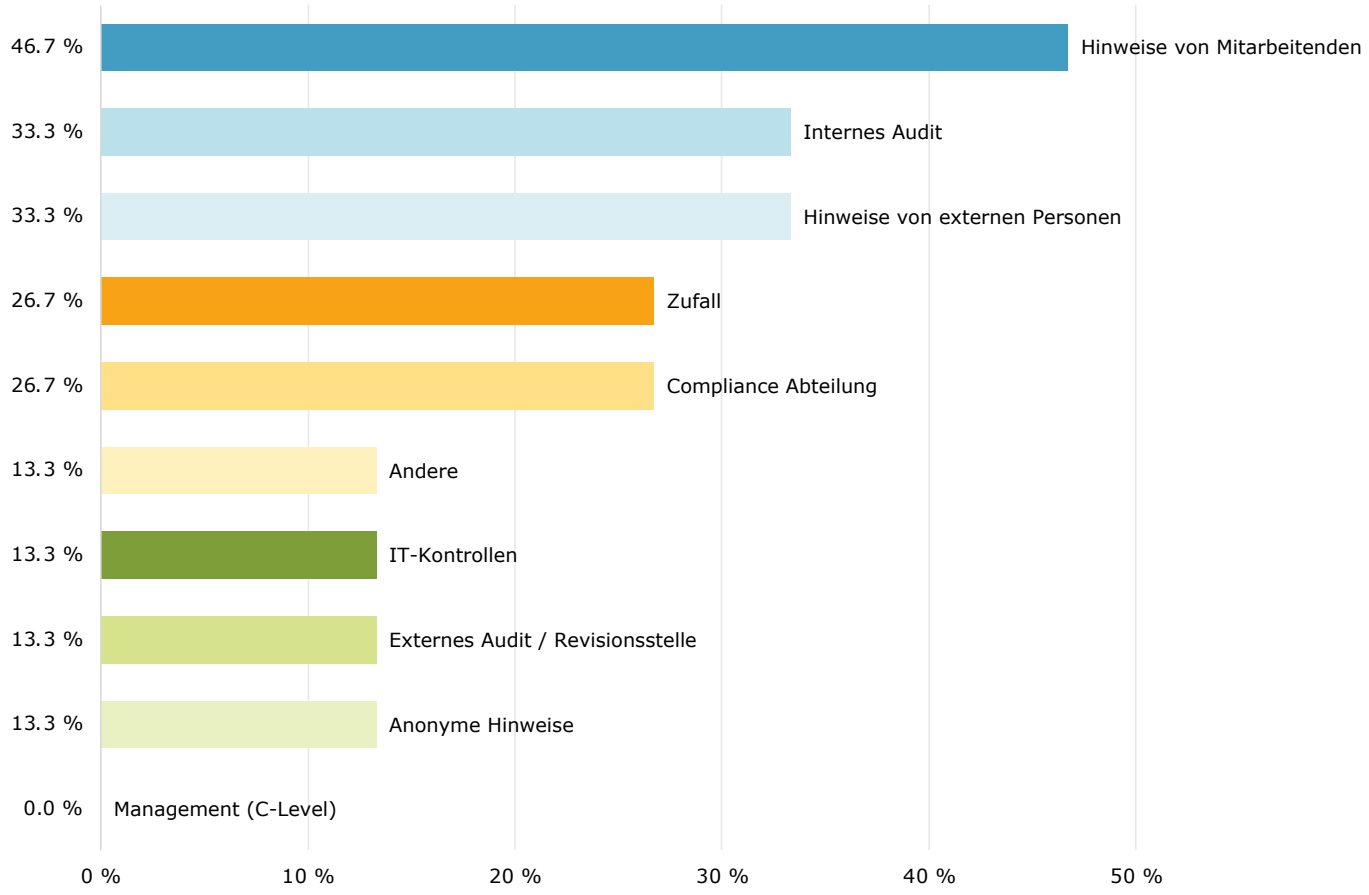
N = 23 Antworten

Hinweise von Mitarbeitenden als wichtigste Quelle zur Aufdeckung wirtschaftskrimineller Handlungen.

Eine Folgefrage zur Beteiligung an der Aufdeckung der Vorfälle zeigt, dass Hinweise von Mitarbeitenden (u.a. Whistleblower) die häufigste Quelle darstellen; 46.7 % der Fälle wurden durch interne Hinweise bekannt, was die Bedeutung eines etablierten Meldesystems und einer entsprechenden Unternehmenskultur unterstreicht. Ebenfalls häufig zur Aufklärung beigetragen haben das Interne Audit sowie Hinweise von externen Personen mit jeweils 33.3 %. Überraschend oft erfolgte die Aufdeckung auch durch Zufall (26.7 %), was auf das fortbestehende Risiko unentdeckter Delikte hindeutet. Die Compliance-Abteilung spielte ebenfalls eine bedeutende Rolle bei der Aufdeckung und erreichte ebenfalls 26.7 %. IT-Kontrollen, externes Audit bzw. Revisionsstellen, anonyme Hinweise sowie sonstige Quellen trugen mit jeweils 13.3 % zur Aufdeckung bei. Auffällig ist, dass Management-Ebenen (C-Level) in keinem einzigen Fall direkt an der Aufdeckung beteiligt waren.

Im internationalen Vergleich hebt der EY Global Integrity Report 2024 hervor, dass weltweit 43 % aller wirtschaftskriminellen Handlungen durch Hinweise von Whistleblowern aufgedeckt werden (EY 2024). Dies zeigt eine klare Parallele zu unseren Ergebnissen und betont die Wichtigkeit einer offenen Meldestruktur in Unternehmen. Auch die KPMG-Studie in Deutschland zeichnet ein vergleichbares Bild; laut der Erhebung werden 55 % der Delikte durch unternehmensinterne Hinweise entdeckt, während 40 % auf Informationen von externen Parteien zurückzuführen sind (KPMG 2020). Auch der ACFE Report (2024b) hebt hohe Beteiligung von Whistleblowern (43 %, intern und extern, wie z. B. Kunden und Verkäufer) und internes Audit (14 %) hervor.

Abb. 17: Beteiligung an der Aufdeckung der Vorfälle



N = 33 Antworten

4 Risikoprävention und Corporate Governance

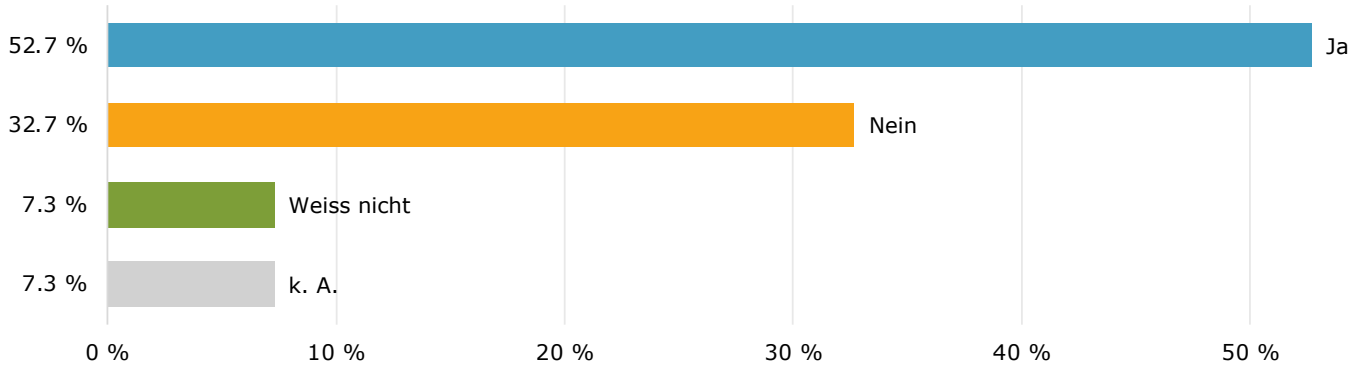
In diesem vierten und vorletzten Kapitel werden Inhalte der Studie in den Bereichen Prävention und Corporate Governance thematisiert. Dazu richtet sich der Fokus zunächst auf das Vorhandensein von Präventionsmechanismen und Verantwortlichkeiten sowie deren Zusammensetzung und abschliessend auf konkrete Massnahmen und zukünftige Herausforderungen.

Nur die Hälfte verfügt über ein systematisches Risikomanagement im Bereich Wirtschaftskriminalität.

Eine erste Frage in diesem Kapitel widmet sich der systematischen Erfassung von Risiken in Bezug auf Wirtschaftskriminalität. Lediglich 52.7 % der Befragten gaben an, dass Risiken in Bezug auf Wirtschaftskriminalität systematisch erfasst werden – etwa durch Instrumente wie einen Crisis Management Plan, ein Anti-Fraud-Programm oder ein Compliance-Management-System (CMS). Demgegenüber gibt jedes dritte Unternehmen an (32.7 %), dass derartige Risikomanagementstrukturen nicht implementiert sind. Weitere 7.3 % der Befragten wussten nicht, ob entsprechende Massnahmen im Unternehmen existieren.

Ein Blick auf internationale Erhebungen zeigt ähnliche Schwachstellen. Nach der deutschen KPMG Studie (2020) nutzen 50 % der Unternehmen ein System zur Erfassung und Bewertung von Risiken, die mit wirtschaftskriminellen Handlungen einhergehen; bei Unternehmen mit weniger als 100 Mitarbeitenden sind es sogar nur 36 %. Darauf aufbauend zeigt der ACFE Report (2024b) auf, dass über die Hälfte der untersuchten Betrugsfälle durch das Fehlen interner Kontrollen (32 %) oder durch die Umgehung bestehender Kontrollen (19 %) entstehen; aus diesem Grund sollten Unternehmen genau an dieser Stelle ansetzen bzw. nachbessern und ein regelmässig revidiertes Risikomanagementsystem in Bezug auf wirtschaftskriminelle Risiken implementieren, um wirtschaftskriminellen Vorfällen präventiv zu begegnen.

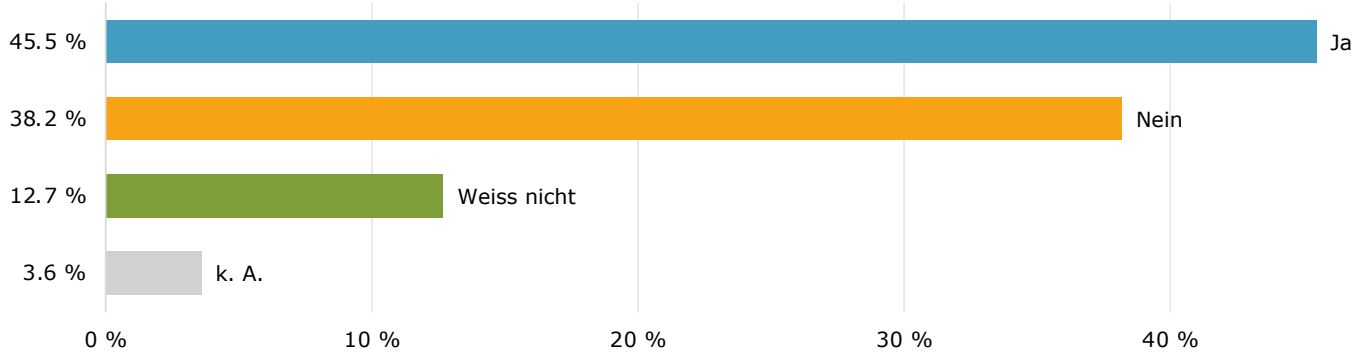
Abb. 18: Systematische Erfassung von Risiken in Bezug auf Wirtschaftskriminalität



Compliance-Verantwortung im Verwaltungsrat? – Ein geteiltes Bild.

Die Befragungsergebnisse zeigen, dass die Verankerung des Themas Compliance auf Verwaltungsratsebene nicht einheitlich festgelegt ist. 45.5 % der befragten Unternehmen gaben an, dass im Verwaltungsrat ein Mitglied spezifisch für Compliance-Fragen verantwortlich ist. 38.2 % verneinten die Frage; Hintergrund ist teilweise die Rechtsform der Unternehmen. Bei den als Aktiengesellschaft organisierten Unternehmen lässt eine Verneinung darauf schliessen, dass auf strategischer Unternehmensebene der Einhaltung von selbst- und fremdauferlegten Pflichten und Regeln, d. h. Compliance, teilweise kein gesonderter Raum eingeräumt wird. Hervorzuheben ist zudem, dass 12.7 % der Befragten angaben, nicht zu wissen, ob eine solche Verantwortlichkeit im Verwaltungsrat existiert; dies weist auf ein mögliches Defizit an Transparenz und Kommunikation innerhalb einiger Unternehmen hin.

Abb. 19: Compliance Verantwortung im Verwaltungsrat



Audit Committees in Schweizer Unternehmen lassen auf nicht erschlossene Potentiale schliessen.

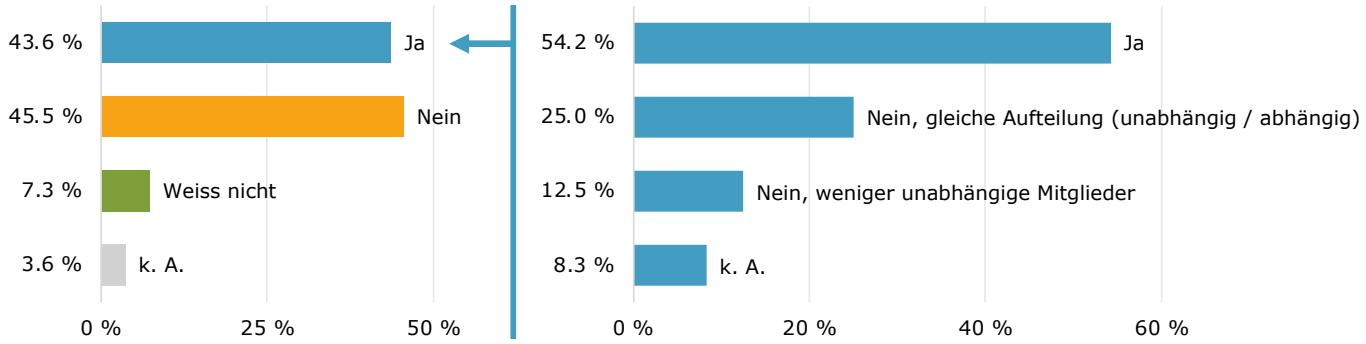
Die Umfrageergebnisse zeigen, dass bei 43.6 % der befragten Schweizer Unternehmen ein Audit Committee existiert; davon konnten 54.2 % (d. h. 23.6 % der Unternehmen) eine Zusammensetzung aus überwiegend unabhängigen Mitgliedern bzw. 25 % eine gleiche Aufteilung zwischen internen und unabhängigen Mitgliedern bestätigen. Demgegenüber gaben 45.5 % an, nicht über ein solches Gremium in ihrem Unternehmen zu verfügen. Weitere 7.3 % wussten nicht, ob ein Audit Committee eingerichtet ist.

Vor dem Hintergrund der hohen Beteiligung des Audits – insb. internes Audit, aber auch unabhängiges, externes Audit – an der Aufdeckung von Wirtschaftskriminalität im Unternehmen (siehe Abbildung 16), ist an dieser Stelle ein Verbesserungspotential ersichtlich; Unternehmen sollten nach Möglichkeit auf ein qualifiziertes Audit Committee zurückgreifen. Hierbei ist natürlich zu berücksichtigen, dass insbesondere grössere Unternehmen über geeignete finanzielle oder personelle Ressourcen verfügen, um eine entsprechend spezialisierte Abteilung zu führen (z. B. KPMG 2020).

Auch Beobachtungen auf internationaler Ebene bestätigen diese Feststellung. Im Rahmen des ACFE Report (2024b) wird beispielsweise aufgezeigt, dass interne Audit Abteilungen (80 %) und unabhängige Audit Committees zu den häufigsten Präventionskontrollen gehören und gemeinsam für das Aufdecken von 17 % der Fälle von Wirtschaftskriminalität verantwortlich sind. In Deutschland trägt die interne Revision alleine zu 35 % der Aufdeckungen bei (KPMG 2020); Grund hierfür ist

insbesondere die gesetzliche Verpflichtung zur Einrichtung einer internen Revision, hervorgehend aus dem deutschen Aktiengesetz. In der Schweiz existiert eine derartige Bestimmung nicht.

Abb. 20: Vorhandensein eines Audit Committees und Zusammensetzung aus >50 % unabhängigen Mitgliedern

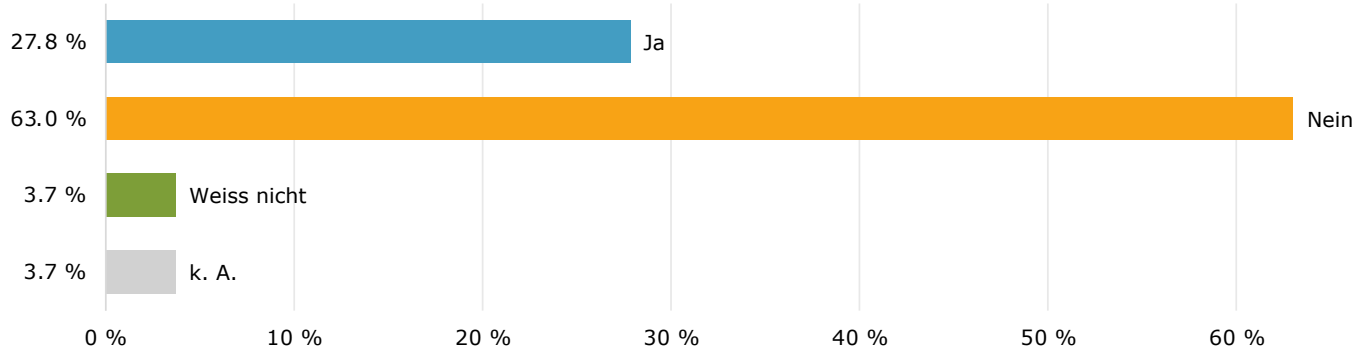


Trennung der Rollen von Verwaltungsratspräsident und Geschäftsführer – Schweiz kennt nach wie vor die Personalunion.

Die Trennung der Funktionen des Verwaltungsratspräsidenten (Chairman) und des Geschäftsführers (CEO) gilt international als bewährte Praxis zur Stärkung der Corporate Governance. In Deutschland ist diese Trennung gesetzlich vorgeschrieben und in Grossbritannien bildet sie einen integralen Bestandteil des UK Corporate Governance Code (Abschnitt 2 Nr. 2) – hervorgehend aus dem Cadbury Report von 1992. Sie dient der Vermeidung von Interessenkonflikten und der Sicherstellung einer effektiven Überwachung des Managements durch den Verwaltungsrat.

In der Schweiz existiert ein monistisches System, was keine Funktionstrennung vorschreibt. Die gleichzeitige Ausübung der Funktion des Verwaltungsratspräsidenten und des CEO ist in der Schweiz demnach rechtlich zulässig, steht jedoch nicht im Einklang mit international anerkannten Governance-Standards. Tatsächlich zeigt die Umfrage, dass in 27.8 % der befragten Unternehmen beide Funktionen in Personalunion ausgeübt werden. Eine Mehrheit von 63 % hingegen trennt die Rollen, was darauf hindeutet, dass viele Unternehmen die Notwendigkeit einer klaren Aufgabenverteilung erkannt haben.

Abb. 21: Trennung der Rollen von Verwaltungsratspräsident und Geschäftsführer



Umgesetzte Kontroll- und Präventionsmassnahmen in Schweizer Unternehmen – Hinweisgebersysteme mit viel Potential.

Implementierte Kontroll- und Präventionsmassnahmen bilden ein zentrales Element im Umgang mit Risiken in Bezug auf Wirtschaftskriminalität. Grosse Unternehmen verfügen aufgrund umfassenderer Ressourcen sowie, bedingt durch regulatorische Vorgaben, grundsätzlich über ein breiteres Spektrum an Kontroll- und Präventionsmassnahmen als kleine und mittlere Unternehmen (siehe ACFE 2024b). Aus der Erhebung geht hervor, dass die gesetzten Schwerpunkte heterogen ausfallen.

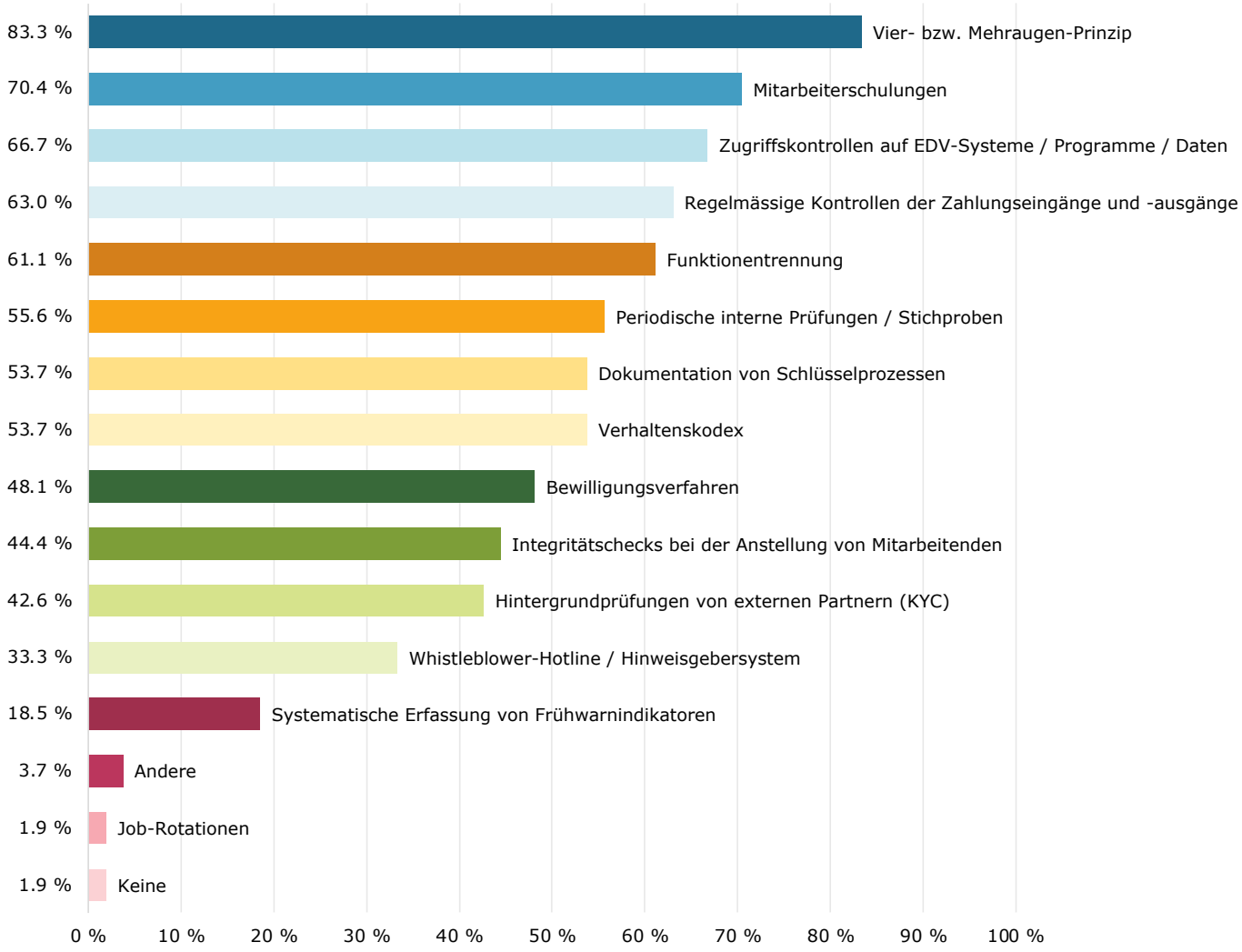
Das etablierte Vier- bzw. Mehraugenprinzip ist mit 83.3 % die am häufigsten umgesetzte Massnahme; sie bildet sowohl in Entscheidungsprozessen als auch digitalen Systemen, wie z. B. in Enterprise Ressource Planning (ERP) Systemen, grundsätzlich einen integralen Bestand. Zugriffskontrollen auf EDV-Systeme, Programme und Daten stehen mit diesem Prinzip in direkter Verbindung und nehmen mit 66.7 % eine entsprechend häufig umgesetzt Massnahme bei den befragten Schweizer Unternehmen ein.

Die Sensibilisierung der Belegschaft im Rahmen von Mitarbeiterschulungen gilt ebenfalls als bewährte Präventionsmassnahme und belegt den zweiten Platz (70.4 %). Hier zeigt sich, dass die befragten Schweizer Unternehmen im internationalen Vergleich tendenziell aktiver sind. Laut der KPMG-Studie 2020 in Deutschland setzen 59 % der Unternehmen auf Mitarbeiterschulungen (KPMG 2020); nach dem Global Integrity Report von PwC (2022) sind es ebenfalls 59 %. Auch der ACFE Report (2024b) betont auf internationaler Ebene die Relevanz von Fraud Trainings, die in 63 % der Fälle für Mitarbeitende und in 62 % für Führungskräfte angeboten werden.

Hintergrundprüfungen von externen Partnern (KYC) sind zentraler Bestandteil der Geldwäschereibekämpfung und insbesondere für Finanzinstitute verpflichtend (siehe GwG, FINMA). Andere KYC-Prüfungen, die der verkehrsüblichen Sorgfalt entsprechen sollen, können weniger umfangreich ausfallen. 42.6 % der Unternehmen geben an, derartige Hintergrundprüfungen von externen Partnern vornehmen zu lassen. Nach der deutschen KPMG Studie (2020) sind es 56 %, die auf Hintergrundrecherchen (u. A. KYC) zurückgreifen. Die Effektivität dieser Massnahme kann nach dem ACFE Report (2024b) diskutiert werden; 48 % der Täter wurden zuvor geprüft, ohne eine „Red Flag“ aufzuweisen. Demgegenüber scheint die Verbreitung von Hinweisgebersystemen (33.3 %) und Verhaltenskodizes (53.7 %) ein deutliches Verbesserungspotential aufzuweisen.

Mitarbeiterhinweise tragen nach dieser Erhebung im Allgemeinen mit am stärksten (siehe Abbildung 17) zur Aufdeckung wirtschaftskrimineller Handlungen bei, so dass Schulungen, Systeme und Dokumente zur Aufklärung als bedeutende Massnahmen anzusehen sind. Im Rahmen des Global Integrity Report von PwC (2022) geben 93 % der Unternehmen an, zumindest auf einen Mix aus Schulungen, Verhaltens-Codex (Codes of Conduct) und Whistleblowing zurückzugreifen. Bei den befragten Schweizer Unternehmen sind nur etwas mehr als drei von vier (78.8 %), die sich zumindest auf eine dieser Massnahmen stützen.

Abb. 22: Implementierte Kontroll- und Präventionsmassnahmen



N = 379 Antworten

Herausforderungen der nächsten zwei Jahre –
90 % der Unternehmen sehen Risiken im Bereich der Informationstechnologie in den kommenden 2 Jahren.

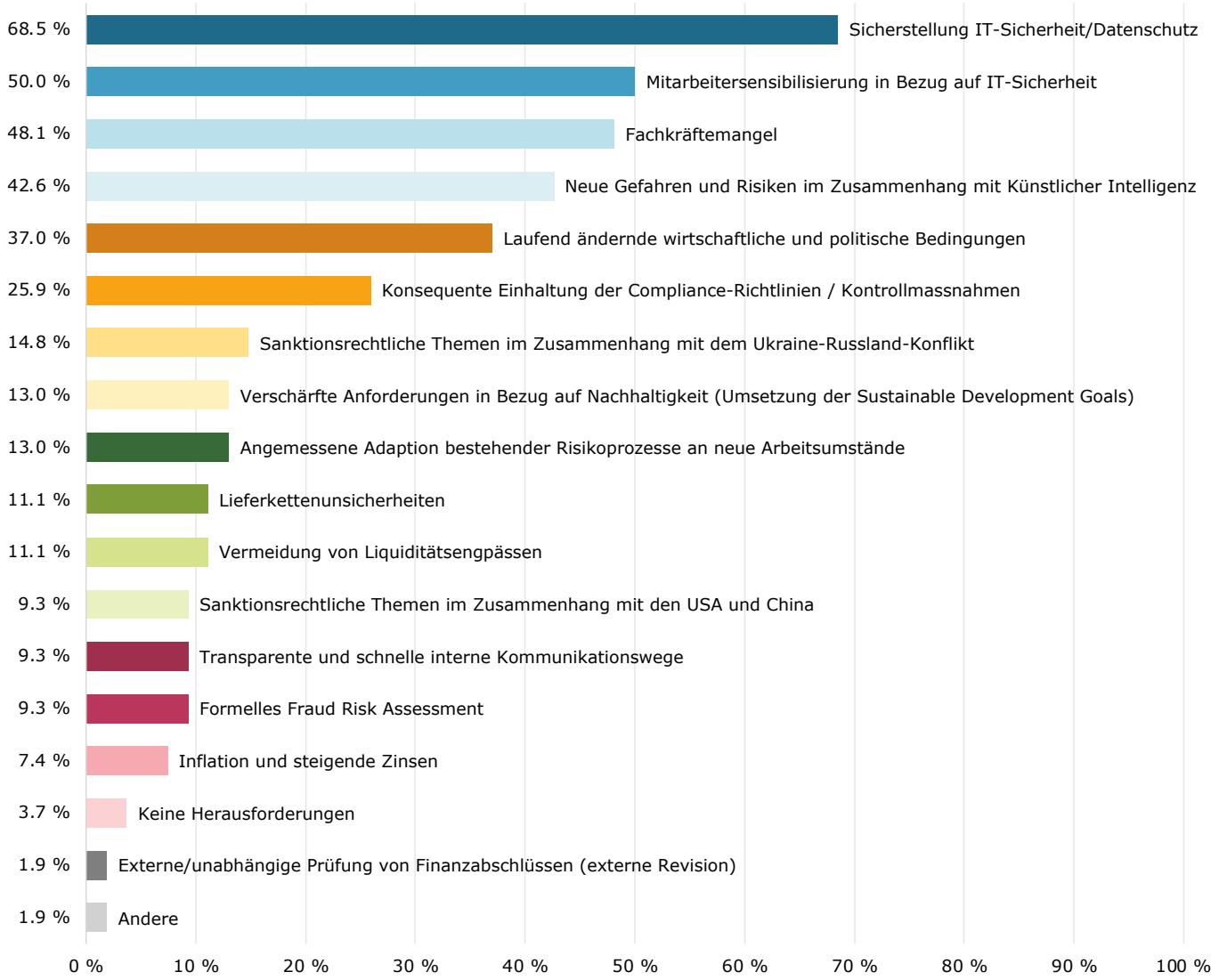
Die IT-Sicherheit/Datenschutz (68.5 %) Mitarbeitersensibilisierung im Bereich IT-Sicherheit (50.0 %) sowie Neue Gefahren und Risiken im Zusammenhang mit Künstlicher Intelligenz (42.6 %) werden von einem Grossteil der Unternehmen als zukünftige Herausforderung wahrgenommen. Dabei nennen 90 % der Unternehmen zumindest einen dieser drei Aspekte. Im Global Risks Report des World Economic Forum stehen Risiken zu Falschinformationen im Zusammenhang mit KI an zweiter Stelle (53 %) (WEF 2024).

Die zunehmende Abhängigkeit von digitalen Infrastrukturen und die Komplexität neuer Technologien erhöhen den Druck auf Unternehmen, ihre Schutzmechanismen auszubauen und ihre Mitarbeitenden im Bereich IT-Sicherheit umfassend zu schulen (siehe KPMG 2020). In diesem Kontext zeigt sich auch der Fachkräftemangel als ein wesentlicher Risikofaktor: 48.1 % der Unternehmen

(in Deutschland 55 %, KPMG 2020) sehen den Mangel an qualifiziertem Personal als bedeutende Herausforderung in den nächsten zwei Jahren. Dies verdeutlicht, dass nicht nur die Implementierung technischer Schutzmassnahmen, sondern auch der Aufbau entsprechender personeller Kompetenzen entscheidend für die Widerstandsfähigkeit gegenüber wirtschaftskriminellen Handlungen von innen und von aussen ist.

Neben Risiken, hervorgehend aus dem IT-Bereich, empfinden die befragten Schweizer Unternehmen auch laufend ändernde wirtschaftliche und politische Bedingungen (z. B. geopolitische Spannungen, Zollkrieg) mit einem Wert von 37 % als eine zentrale Herausforderungen der kommenden zwei Jahre – dieses Ergebnis spiegelt sich auch auf internationaler Ebene wider (z. B. WEF 2024).

Abb. 23: Herausforderungen in den folgenden 2 Jahren



N = 204 Antworten

GRID SLICE FN-3
CONTROLLER APB
NODE A
NODE B
GRID SLICE FN-3
CORE 07

5 Fokusthema 2025 – Künstliche Intelligenz

In diesem letzten Kapitel 5 der diesjährigen Studie wird das Fokusthema– Künstliche Intelligenz – analysiert. Zunächst richtet sich die Fragestellung auf die generelle Einschätzung von KI als Risiko und Chance für Unternehmen im Zusammenhang von Wirtschaftskriminalität, um darauf aufbauend den konkreten Erfahrungen sowie den Umsetzungsstand und Massnahmen zu thematisieren.

5.1 KI im Fokus der Unternehmen

Künstliche Intelligenz (KI) wird eher als Risiko als eine Chance wahrgenommen; Kompetenzen zur Prävention KI-generierter Betrugsversuche sind ausbaufähig.

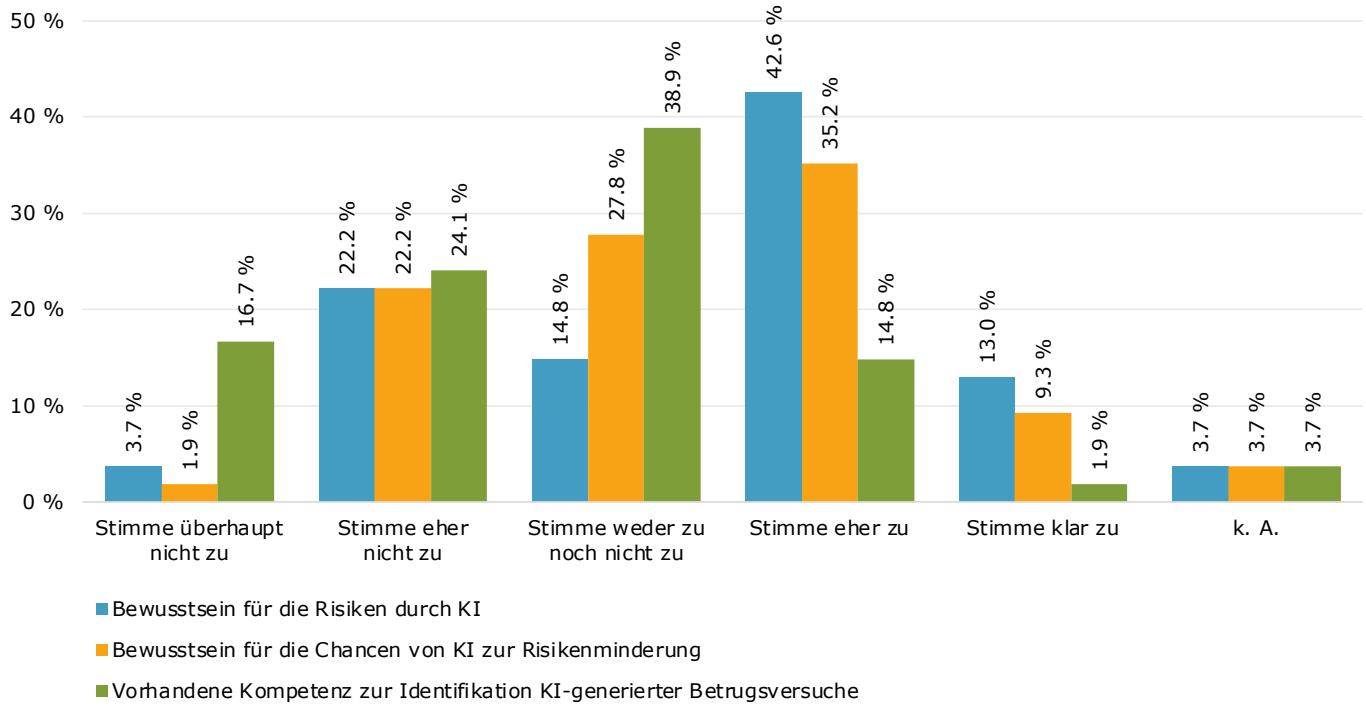
Die Ergebnisse der Umfrage verdeutlichen ein zweigeteiltes Bild hinsichtlich der Wahrnehmung von Künstlicher Intelligenz (KI) als Risiko oder als Chance im Kontext wirtschaftskrimineller Risiken. Einerseits erkennen viele Unternehmen die Gefahren und Risiken, die mit der verstärkten Nutzung von KI einhergehen. 55.6 % der Befragten stimmen der Aussage zumindest eher zu, dass diese Risiken im Unternehmen adressiert werden, während ein relevanter Anteil von 25.9 % angibt, dass diese Risiken als eher nicht oder gar nicht relevant betrachtet werden. Diese Diskrepanz zeigt, dass in einigen Unternehmen die Sensibilisierung für die potenziellen Bedrohungen durch technologische Fortschritte noch Verbesserungspotential aufweist.

Gleichzeitig wird die **Chance von KI zur Risikominderung** bei vielen Unternehmen anerkannt. 44.5 % der Teilnehmenden sieht in der verstärkten Nutzung von KI eher oder klar eine Chance, wirtschaftskriminelle Risiken zu minimieren und Vorfälle schneller aufzudecken. Gleichzeitig beurteilt ein Teil der Unternehmen die Aussage zur Nutzung von KI als Chance zurückhaltend – 27.8 % stehen den Chancen neutral gegenüber, während 22.2 % diesen sogar eher widersprechen. Das Potential von KI zur Bekämpfung von Wirtschaftskriminalität verdeutlicht auch die ACFE durch Online-Beiträge und -Schulungen sowie durch den ACFE Benchmarking Reporting (2024a) zu Anti-Fraud Technologie (n= 1´187) – mit 32 % an erster Stelle erwarten die Teilnehmenden KI zur Prävention einzusetzen.

Deutlich weniger ausgeprägt ist das Vertrauen in die eigenen Fähigkeiten zur **Erkennung von KI-generierten Betrugsversuchen**. Nur 14.8 % der Befragten stimmen der Aussage eher zu, dass ihr Unternehmen über die notwendigen Kompetenzen verfügt, solche Betrugsversuche systematisch zu identifizieren. 24.1 % der Teilnehmenden stimmen der Aussage eher nicht zu, weitere 3.7 % stimmen überhaupt nicht zu. Der Grossteil (38.9 %) zeigt sich unentschieden und gibt an, dies weder bestätigen noch verneinen zu können.

Internationale Vergleichsstudien, wie der EY Global Integrity Report (2024), bestätigen diese Ambivalenz; zwischen dem Wissen um das Risiko und den realisierten Massnahmen existiert häufig noch eine Lücke, die es zu schliessen gilt. Unternehmen, die bereits verstärkt auf KI-gestützte Systeme setzen, berichten von effizienteren Kontrollmechanismen und einer höheren Aufdeckungsrate wirtschaftskrimineller Handlungen. Schweizer Unternehmen haben hier die Möglichkeit, durch gezielte Investitionen und der Weiterentwicklung digitaler Systeme (Cyberkriminalität, s.o.) sowohl die Risiken zu minimieren als auch die Effizienz der Aufdeckung deutlich zu steigern. Eine damit einhergehende Sensibilisierung der Mitarbeitenden sollte gleichermassen erfolgen (ACFE 2024a).

Abb. 24: Beurteilung von Aussagen zu KI als Risiko und Chance

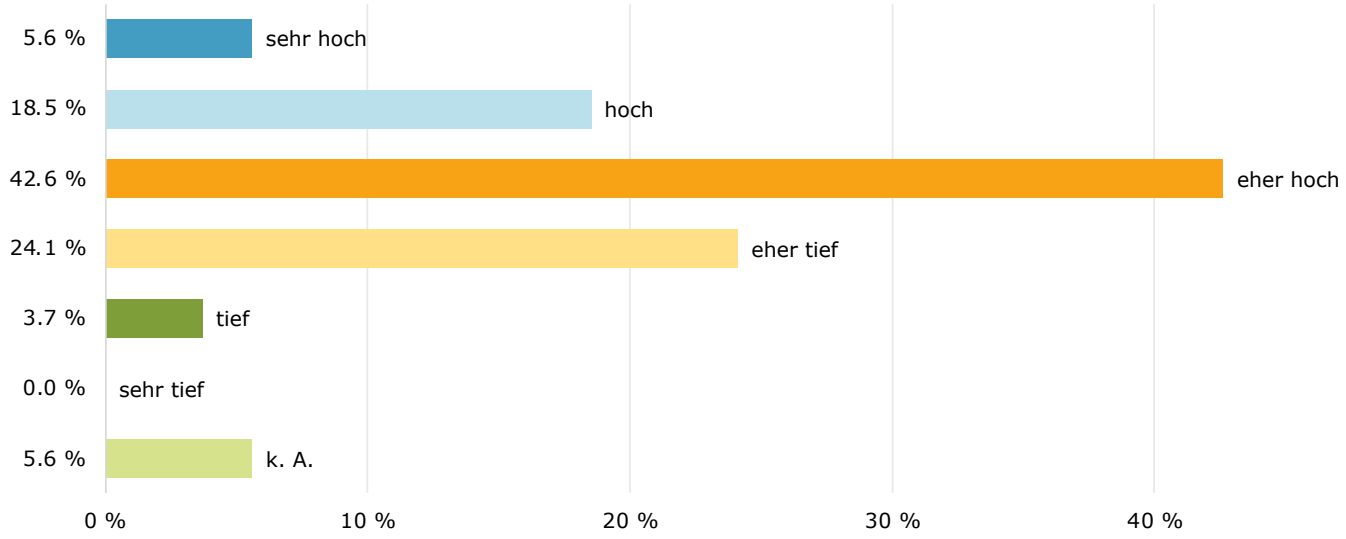


Die persönliche Betroffenheit von KI-generierten Betrugsversuchen wird von über zwei Drittel der Unternehmen zumindest als „eher hoch" eingeschätzt.

Die Ergebnisse der Umfrage zeigen ein differenziertes Bild hinsichtlich der Einschätzung des Risikos, durch Künstlichen Intelligenz (KI) selbst von Betrugsversuchen betroffen zu sein. 42.6 % der Befragten beurteilen das Risiko als eher hoch, weitere 18.5 % als hoch und 5.6 % als sehr hoch. Damit schätzen circa zwei Drittel der Unternehmen (66.7 %) das Risko, persönlich von KI-generierten Betrugsversuchen betroffen zu sein, zumindest als „eher hoch" ein. Demgegenüber betrachten 27.8 % der Unternehmen das Risiko als eher tief oder tief.

Die Ergebnisse verdeutlichen, dass Unternehmen die Risiken durch KI-generierte Betrugsversuche wahrnehmen, jedoch noch nicht flächendeckend darauf reagieren. Erfahrungswerte auf internationaler Ebene gestaltet sich noch fragmentarisch – u.a. bedingt durch die Geschwindigkeit, mit der insbesondere die GPTs (Generative Pretrained Transformer) aktuell weiterentwickelt werden: 2018 wurde die GPT-1 von OpenAI mit ca. 117 Millionen Parametern veröffentlicht. 2023, also 5 Jahre später, umfasste die GPT-4 ca. 1'800'000 Millionen (d. h. 1.8 Billionen) Parameter. Die GPT-4 verfügt damit über die 15'000-fache Anzahl an Parametern, um komplexe Sprachverarbeitungen vorzunehmen. Solche Modelle bergen ein erhebliches Missbrauchspotenzial für dolose Aktivitäten im digitalen Raum, weshalb auch die ACFE und ihre Mitglieder diesem Bereich besondere Aufmerksamkeit widmen.

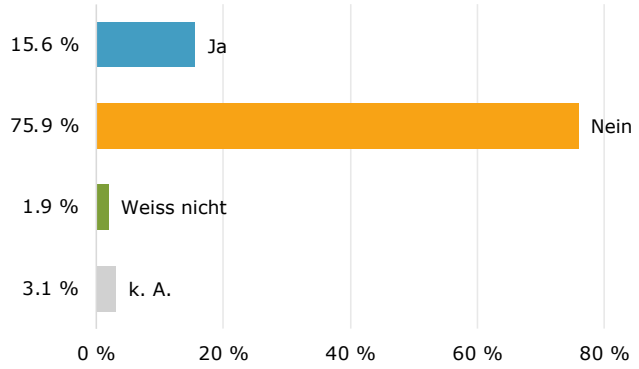
Abb. 25: Risiko der eigenen Betroffenheit von KI-generierten Betrugsversuchen



Künstliche Intelligenz wird (noch) selten systematisch genutzt und im Kontext wirtschaftskrimineller Vorfälle kaum involviert.

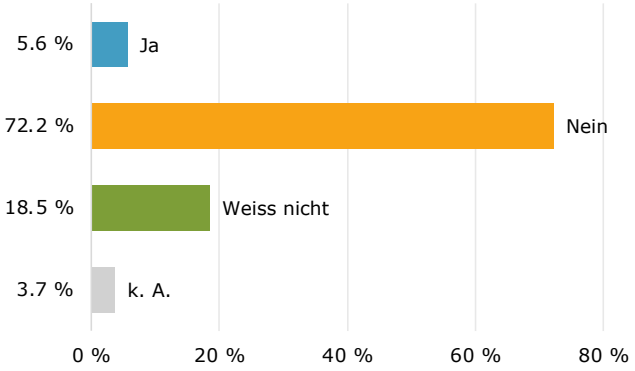
Die Zahlen verdeutlichen, dass der systematische Einsatz von KI in Geschäftsprozessen der befragten Schweizer Unternehmen bislang kaum verbreitet ist. Lediglich 15.6 % der Teilnehmenden gaben an, dass KI aktiv und strukturiert in ihren Unternehmensprozessen integriert ist (Abbildung 26). Im Gegensatz dazu verneinten 75.9 % der Befragten einen solchen Einsatz, während sich 5.3 % unsicher waren, ob KI im Unternehmen systematisch genutzt wird.

Abb. 26: Systematischer Einsatz von KI in Geschäftsprozessen



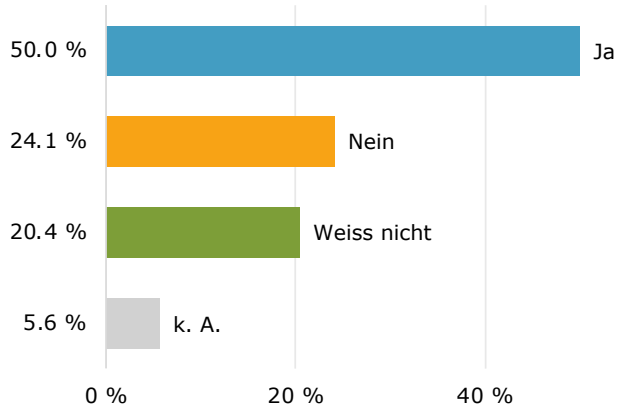
Auch die Betroffenheit von wirtschaftskriminellen Vorfällen mit KI-Einsatz ist bisher gering (Abbildung 27). Hier gaben 72.2 % der Befragten an, bislang nicht von wirtschaftskriminellen Handlungen betroffen gewesen zu sein, bei denen KI involviert war. Lediglich 5.6 % berichteten von entsprechenden Vorfällen, während sich 18.5 % unsicher waren.

Abb. 27: Betroffenheit von wirtschaftskriminellen Vorfällen mit KI-Einsatz



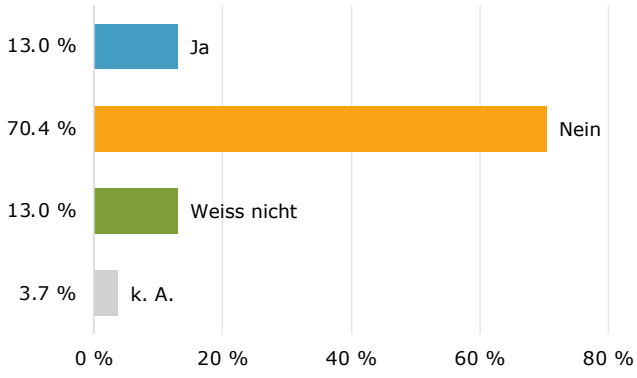
Diese Ergebnisse legen nahe, dass das Potenzial von KI zur Früherkennung und Prävention wirtschaftskrimineller Handlungen in der Schweiz noch nicht ausreichend genutzt wird. Vor dem Hintergrund des hohen Anstiegs im Bereich Cyberkriminalität im vergangenen Jahr (siehe Polizeiliche Kriminalstatistik) ist es nur eine Frage der Zeit, bis KI in diesem Bereich weiträumig Einzug hält (z. B. Stimmengeneratoren, Social-Engineering, personalisierte Bots, Deepfakes). Unternehmen sollten dieses aufkommende Risiko keineswegs unterschätzen. Dies geht aus den Antworten auf die Frage hervor, ob bereits Präventionsmassnahmen gegenüber KI-generierten Betrugsversuchen getroffen wurden (Abbildung 28); nur 50 % beantworten diese mit ja. Demgegenüber verneinte knapp ein Viertel der Unternehmen (24.1 %) den Einsatz von Massnahmen. Weitere 20.4 % sind sich nicht sicher, ob Massnahmen getroffen und umgesetzt wurde; insbesondere bei diesem Teil liesse sich das Bewusstsein und die Sensibilität gegenüber KI-generierten Betrugsversuchen durch erste Schulungen adhoc steigern.

Abb. 28: Massnahmen zur Verhinderung KI-generierter Betrugsversuche



Bezüglich der Aufdeckung und Prävention unter KI-Einsatz zeichnet sich ein deutliches Bild ab (Abbildung 29). Ein Grossteil der Unternehmen (70.4 %) gibt an, diese Technologien nicht zu verwenden; nur 13 % bestätigen den KI-unterstützten Einsatz zur Prävention wirtschaftskrimineller Handlungen. Auf internationaler Ebene legt der EY Global Integrity Report (2024) ein ähnliches Ergebnis dar. Innerhalb der Unternehmen sind die IT-Abteilung der erste Anwender (42 %) von KI-gestützten Werkzeugen; Compliance (31 %) und internes Audit (23 %) liegen bei der aktiven Nutzung von KI tendenziell etwas zurück; sie planen jedoch häufig, diese Lücke in den kommenden Jahren zu schliessen. Auch eine Studie von Roland Berger (2025) zeigt, dass Unternehmen bereits in ausgewählten Bereichen (hier: n > 550 Führungskräfte im Kundenservice) auf KI setzen. Vor diesem Hintergrund dürfte es nur eine Frage der Zeit sein, bis KI als Hilfstools zur Prävention von Wirtschaftskriminalität flächendeckend eingesetzt wird. Aktuell stehen dieser Etablierung neuer Präventionstechnologien jedoch insbesondere Budget und finanzielle Restriktionen gegenüber; dies geht aus dem 2024 Anti-Fraud Technology Benchmark Report (n = 1‘187) hervor (ACFE 2024a).

Abb. 29: Nutzung von KI zur Prävention von Wirtschaftskriminalität



Eine Anschlussfrage richtete sich nur an jene Unternehmen, die bereits Massnahmen zur Verhinderung von KI-basierten Betrugsversuchen ergriffen haben (50 % der Stichprobe), adressierte die spezifische Art dieser Vorkehrungen. Im Fokus steht bei vielen Unternehmen die soziale Dimension.

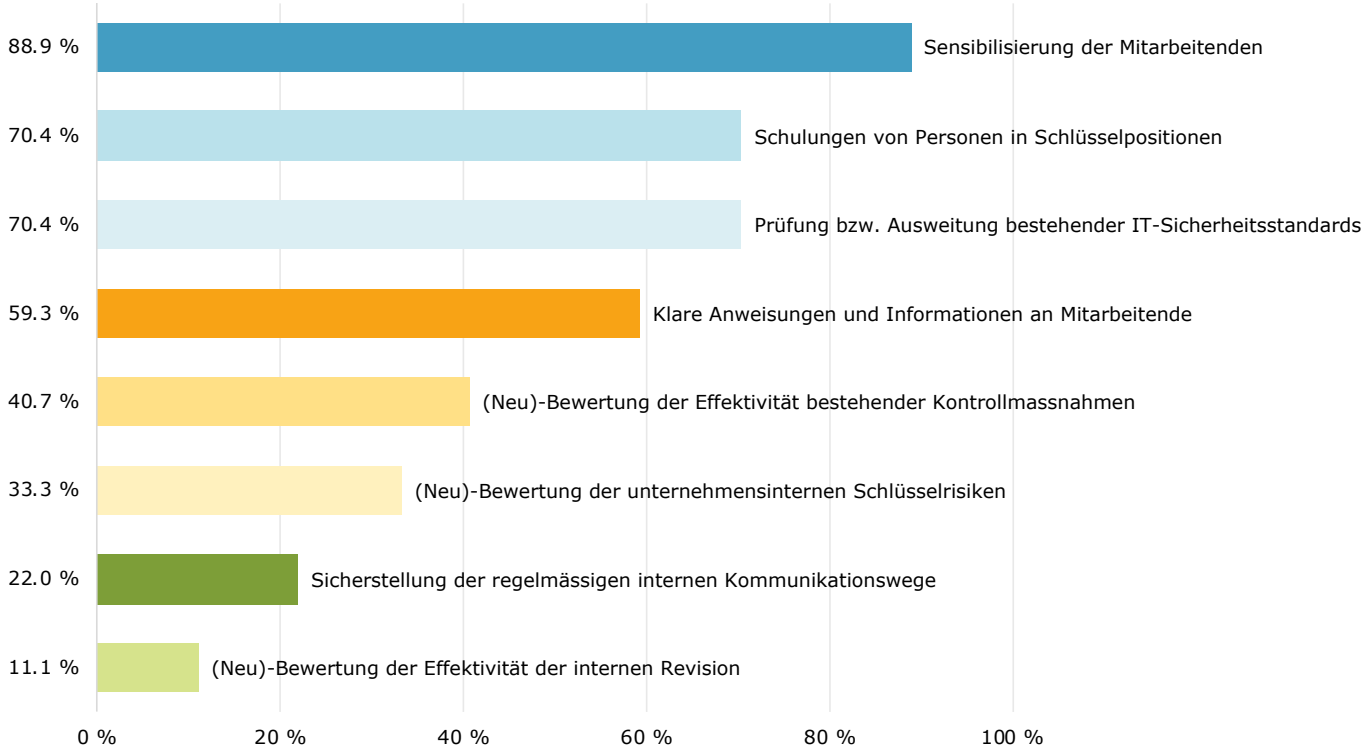
Sensibilisierung der Mitarbeitenden (88.9 %), Schulungen Personen in Schlüsselpositionen (70.4 %), klare Anweisungen und Information an Mitarbeitende (59.3 %)

Die häufigste Massnahme stellt die Sensibilisierung der Mitarbeitenden in Verbindung mit der Bereitstellung klarer Anweisungen und Informationen (59.3 %) bezüglich neuer Risiken im Kontext von KI dar – wie z. B. durch Deepfakes, Social Engineering über Anrufe oder Emails und automatisierte Phishing-Angriffe. Die Schulung von Personen in Schlüsselpositionen (70. 4 %) setzt ebenfalls am fragilsten Punkt vieler Unternehmen an, dem Menschen. Sie soll sicherstellen, dass Personen mit Entscheidungsbefugnissen über das notwendige Fachwissen verfügen. Dieses Ziel des Kompetenzaufbaus über zumindest eine dieser drei Massnahmen findet bei allen antwortenden Unternehmen (100 %) Anwendung – siehe auch Website der ACFE (z. B. online Schulungen). Dies zeugt von einem Bewusstsein bei den Unternehmen, dass grundsätzlich alle Mitarbeitenden durch gezielte Aufklärung in die Lage versetzt werden können, potenzielle Risiken frühzeitig zu erkennen, adäquat zu reagieren und zu melden.

Prüfung und Ausweitung bestehender IT-Sicherheitsstandards (70.4 %)

Weitere Massnahmen adressierten die technisch-organisatorische Dimension. Fast drei Viertel der befragten Unternehmen überprüfen regelmässig ihre IT-Sicherheitsrichtlinien (70.4 %). Ergänzend trägt die kontinuierliche Überprüfung der Effektivität bestehender Kontrollmassnahmen (40.7 %) sowie die (Neu-)Bewertung interner Schlüsselrisiken (33.3 %) prozessseitig zur Prävention von mit KI in Verbindung stehenden Gefahren bei. Die Sicherstellung der regelmässigen internen Kommunikationswege (22.2 %) sowie die (Neu-)Bewertung der Effektivität der internen Revision (11.1 %) sind weniger stark ausgeprägt, jedoch nicht weniger relevant.

Abb. 30: Art der Massnahme zur Prävention von KI-generierten Betrugsversuchen



N = 107 Antworten

5.2 Handlungsempfehlungen zu KI-generierten Betrugsversuchen

Hervorgehend aus den Studienergebnissen in diesem letzten Themenblock zum Fokusthema Künstliche Intelligenz haben wir eine Taxonomie an Handlungsempfehlungen erarbeitet. Diese Empfehlungen haben zum Ziel, Unternehmen und Organisationen – unabhängig ihrer Rechtsform – ein Instrument zur Verfügung zu stellen, um KI-generierten Betrugsversuchen vorzubeugen. Hierzu wird ein bewährtes Vorgehen aus dem Risikomanagement übernommen – Schutzmassnahmen sollen nach Möglichkeit gar nicht erst ein Risiko entstehen lassen bzw. möglichst nahe an der Gefahrenquelle anzusetzen. Teile dieses Prinzips gehören zur Sorgfaltspflicht eines ordentlichen Geschäftsmodells und können zur Minimierung von Haftungsrisiken beitragen.

SAFER

S Substitution
(Vermeidung von Risiken)

A Automatisierte Erkennung
(Technische Schutzmassnahmen)

F Fortbildung
(Organisatorische Schutzmassnahmen)

E Entschärfung
(Persönliche Schutzmassnahmen)

R Reaktionsfähigkeit
(Notfallplan)

Substitution: Die beste Methode, sich gegen KI-generierte Betrugsversuche zu schützen, ist die vollständige Vermeidung potenziell unsicherer Kommunikationswege und Technologien. Unternehmen sollten sichere Kommunikationsplattformen nutzen, die manipulationssicher sind und Verschlüsselungsprotokolle anwenden (z. B. Ende-zu-Ende bzw. Peer to Peer verschlüsselte Kommunikationstools). Eines der aktuell sichersten Peer-to-Peer-Netzwerke stellt z. B. eine gruppen- oder unternehmensinterne private Blockchain dar, in der nur zuvor verifizierte Akteure handlungsberechtigt sind; das Eindringen in diese Systemarchitektur oder das nachträgliche Fälschen bereits validierter Transaktionen (o.Ä.) ist grundsätzlich unmöglich (siehe z. B. Thies et al. 2023).
Der Verzicht auf unsichere Kommunikationsmethoden wie unverschlüsselte E-Mails kann ebenfalls zur Verringerung des Risikos beitragen. Zudem sollten interne Prozesse so gestaltet sein, dass sensible Informationen niemals ungesichert übermittelt werden (z. B. Zahlungsanweisungen nur über genehmigte, sichere Kanäle).

Automatisierte Erkennung: Auf zweiter Ebene sollten Technologien zur automatisierten Erkennung derartiger Bedrohungen zum Einsatz kommen. Technologien wie Anti-Phishing-Software, Deepfake-Detektionsprogramme und Echtzeit-Analyse-Tools können potenzielle Bedrohungen frühzeitig identifizieren und bewerten, bevor Schaden entsteht. Zusätzlich können KI-basierte Anomalie-Erkennungen eingesetzt werden, um verdächtige Aktivitäten im Netzwerk frühzeitig zu entdecken.

Fortbildung: Als weiteres Element bildet die Fortbildung und Sensibilisierung aller Mitarbeitenden einen essenziellen Bestandteil der Prävention. Eine informierte und sensibilisierte Belegschaft ist eine der stärksten Verteidigungslinien gegen KI-generierte Betrugsversuche. Regelmässige Schulungen zu aktuellen Betrugstrends, wie zum Beispiel zu Deepfake-Anrufe, bei denen sich Angreifer als Führungskräfte ausgeben, oder zu Phishing-Techniken mit leicht veränderten Domänennamen, helfen, bilden eine sowohl effektive als auch effiziente Schutzmassnahme auf menschlicher Ebene.

Entschärfung: Die Entschärfung der Problematik durch sichere Verhaltensweisen trägt zur individuellen Kompetenz der Mitarbeitenden bei, sich selbst und die Organisation aktiv zu schützen. Klare Richtlinien zur Überprüfung von Kommunikationsinhalten sowie etablierte Meldeketten für verdächtige Vorfälle sorgen dafür, dass Risiken schneller erkannt und gemeldet werden können. Hierzu gehört auch die Definition von Verantwortlichkeiten und Eskalationsstufen bei Verdachtsfällen. Ausserdem umfasst die Entschärfung die Stärkung des Bewusstseins für den Umgang mit verdächtigen Nachrichten und Inhalten, die Nutzung sicherer Passwörter sowie den regelmässigen Wechsel dieser. Auch der Schutz der eigenen digitalen Identität durch eine kontrollierte Weitergabe von Informationen spielt eine wesentliche Rolle bei der Entschärfung.

Reaktionsfähigkeit: Den letzten Baustein bilden die Reaktionsfähigkeit und das Krisenmanagement. Trotz aller Präventionsmassnahmen kann es zu Vorfällen kommen. Deshalb ist es von grosser Bedeutung, auf solche Situationen vorbereitet zu sein und schnell reagieren zu können. Ein klar definierter Notfallplan, der alle Schritte der Schadensbegrenzung enthält, hilft, Schäden zu minimieren (z. B. sofortiges Sperren von Zugängen bei vermuteten Sicherheitsverletzungen, Information der IT-Abteilung und aller betroffenen Parteien). Regelmässige Simulationen von Angriffsszenarien, wie Phishing-Tests oder Deepfake-Angriffe, erhöhen die Reaktionssicherheit und decken Schwachstellen auf.

Das **SAFER-Prinzip** bietet eine schlanke und zugleich strukturierte Herangehensweise zur Prävention von KI-generierten Betrugsversuchen. Durch die Kombination aus technischer Absicherung, organisatorischer Schulung und klaren Verhaltensregeln soll Risiken ganzheitlich betrachtet werden. In einem zunehmend digitalisierten Umfeld ist diese mehrschichtige Strategie zielführend, um Unternehmen und Einzelpersonen vor den Risiken der modernen KI-gestützten Betrugstechniken zu schützen.

85.00%
Discussion Outline
TODAYS HIGHLIGHTS
BASED ON A SURVEY
85.00%

6 Fazit und Ausblick zur Studie

Die Ergebnisse dieser Studie zur Wirtschaftskriminalität in der Schweiz bieten wertvolle Einblicke in die wachsenden Herausforderungen, denen sich Unternehmen in einem zunehmend dynamischen und technologisch geprägten Umfeld gegenübersehen. Es wird bestätigt, dass Wirtschaftskriminalität eine zunehmende Bedrohung für Unternehmen darstellt und sich nicht nur in traditionellen Formen wie Betrug, Veruntreuung und Korruption zeigt, sondern auch verstärkt in der Cyberkriminalität manifestiert. Angriffe über Phishing, Ransomware und Social Engineering sind dabei besonders dominant. Unternehmen erkennen diese Risiken und nehmen sie ernst, wobei vier von fünf der befragten Unternehmen von einem Anstieg wirtschaftskrimineller Aktivitäten in den kommenden zwölf Monaten ausgehen – mehr als 80 % davon im Bereich Cyberkriminalität.

Zudem wird deutlich, dass zunehmend auch externe Täter für wirtschaftskriminelle Handlungen verantwortlich sind. Das Aufdecken dieser Vorfälle ist häufig das Ergebnis von Hinweisen aus dem Unternehmen selbst, was die Bedeutung einer offenen und transparenten Unternehmenskultur unterstreicht. Demnach bilden der Einsatz von Whistleblower-Systemen und die Sensibilisierung der Mitarbeiter weiterhin eine der effektivsten Massnahmen zur Aufdeckung. Ausserdem zeigt sich, dass wirtschaftskriminelle Vorfälle häufig noch durch Zufall aufgedeckt werden, was auf eine hohe Dunkelziffer schliessen lässt.

Wenngleich die Betroffenheit der befragten Unternehmen im internationalen Vergleich geringer ausfällt, ist die Geschwindigkeit der Verbreitung von Cyberkriminalität in der Schweiz und weltweit besorgniserregend. Vor dem Hintergrund, dass nur etwa die Hälfte der Unternehmen einer systematischen Erfassung von Risiken in Bezug auf Wirtschaftskriminalität nachgeht, fehlt es jedem zweiten Unternehmen an Wissen über bestehende und auch neue Risiken. Es wird vielmehr an „Best Practice“ Massnahmen angelehnt, die sich in der Vergangenheit bewährt haben, aber gegenüber neuen Betrugsformen von aussen, wie z. B. KI-generierter Angriffe, nur bedingt Schutz versprechen. Gleichzeitig wird deutlich, dass das Risiko KI-generierter Angriffe nur teilweise erkannt wird. Gleichermassen verhält es sich mit der Verwendung dieser Technologien zur Prävention; dennoch wird sie von vielen Unternehmen als vielversprechendste Chance angesehen.

Das aus diesen Erkenntnissen abgeleitete sowie an etablierte Massnahmen angelehnte Framework (SAFER) im Umgang mit KI-generierten Betrugsversuchen hilft Unternehmen, einem systematischen Ansatz zu folgen. Es soll sie ermutigen, ihre Corporate Governance und Risikomanagementsysteme kontinuierlich zu überprüfen und weiterzuentwickeln, um den wachsenden Herausforderungen der Wirtschaftskriminalität – insbesondere in der digitalen Ära – proaktiv zu begegnen. Essenziell ist und bleibt dabei die Unternehmenskultur und ein vorbildlicher „Tone at the Top“, die alle Mitarbeitenden darin bestärkt, in ihrem Unternehmen die Compliance und persönliche Integrität aktiv zu stärken.

Literaturverzeichnis

ACFE (2024a): Anti-Fraud Technology Benchmarking Report. Online verfügbar unter https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report, zuletzt geprüft am 29.04.2025.

ACFE (2024b): Occupational Fraud 2024: A Report to the Nations. Online verfügbar unter https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf, zuletzt geprüft am 29.04.2025.

Beneish, Messod D.; Lee, Charles M.C.; Nichols, D. Craig (2013): Earnings Manipulation and Expected Returns. In: *Financial Analysts Journal* 69 (2), S. 57–82. DOI: 10.2469/faj.v69.n2.1.

BKA (2024): Forschungsbericht - Kosten und Schäden durch Cyber-Kriminalität in Deutschland. Referat IZ 36 - Cybercrimeforschung.

Brunner, Caudia V.; Grau, Susanne; Garcia, Tania (2024a): Wirtschaftskriminalität in der Schweiz. Online verfügbar unter https://hub.hslu.ch/economiccrime/wirtschaftskriminalitaet-in-der-schweiz/.

Brunner, Claudia V.; Grau, Susanne; Urbach, Katrin (2024b): Wirtschaftskriminalität. Entwicklung, Einflüsse und Erscheinungsformen. Wiesbaden: Springer Fachmedien Wiesbaden.

Bundesamt für Polizei fedpol (2023): Bestandesaufnahme der behördlichen Instrumente zur Bekämpfung der organisierten Kriminalität in der Schweiz.

Cressey, Donald R. (1950): The Criminal Violation of Financial Trust. In: *American Sociological Review* 15 (6), S. 738. DOI: 10.2307/2086606.

Dyck, I. AlexanderJ.; Morse, Adair; Zingales, Luigi (2023): How Pervasive is Corporate Fraud? In: *SSRN Journal*. DOI: 10.2139/ssrn.4590097.

Eurojust (2024): Economic crimes. European Union Agency for Criminal Justice Cooperation. Online verfügbar unter https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/economic-crimes#:~:text=Economic%20crimes%20often%20have%20a,major%20focus%20of%20Eurojust%E2%80%99s%20casework, zuletzt geprüft am 19.05.2025.

EY (2014): Overcoming compliance fatigue Reinforcing the commitment to ethical growth - 13th Global Fraud Survey. Ernst & Young (EY), zuletzt geprüft am 23.01.2025.

EY (2022): Global Integrity Report 2022 - Tunnel vision or the bigger picture? Ernst & Young (EY), zuletzt geprüft am 23.01.2025.

EY (2024): Global Integrity Report 2024 - How can trust survive without integrity? Ernst & Young (EY), zuletzt geprüft am 23.01.2025.

Grzybowski, Andrzej; Pawlikowska-Łagód, Katarzyna; Lambert, W. Clark (2024): A History of Artificial Intelligence. In: *Clinics in dermatology* 42 (3), S. 221–229. DOI: 10.1016/j.clindermatol.2023.12.016.

Karami, Behzad (2022): Wirecard: Das kollektive Kontrollversagen – ein Fall für die Lehrbücher. In: Behzad Karami (Hg.): Skandalfall Wirecard: Eine wissenschaftlich-fundierte interdisziplinäre Analyse : Problemaufriss – Rechtsrahmen – Lehren für die Zukunft. Wiesbaden: Springer Fachmedien Wiesbaden, S. 1–85.

KPMG (2020): Im Spannungsfeld - Wirtschaftskriminalität in Deutschland, zuletzt geprüft am 14.02.2025.

KPMG (2025): Global profiles of the fraudster. The enemy within - profiling the corporate fraudster. KPMG, zuletzt geprüft am 19.05.2025.

PKS (2025): Die Rubrik im Überblick. Online verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html, zuletzt geprüft am 19.05.2025.

PwC (2020): Economic Crime - When the boardroom becomes the battlefield (7th edition). PricewaterhouseCoopers (PwC).

PwC (2022): PwC's Global Economic Crime and Fraud Survey 2022 - Protecting the perimeter: The rise of external fraud. PricewaterhouseCoopers (PwC), zuletzt geprüft am 23.01.2025.

PwC (2024): PwC's Global Economic Crime Survey 2024. PricewaterhouseCoopers (PwC). Online verfügbar unter https://www.pwc.de/de/forensic-services/pwc-global-economic-crime-survey-2024-german-executive-summary.pdf, zuletzt geprüft am 23.01.2025.

Roland Berger (2025): Service with a silicon smile. Customer Service in the age of AI. Unter Mitarbeit von S. Schatto, S. Thiel, F. Huhle, M. Finkelshteyn und F. Neuen. Hg. v. Roland Berger, zuletzt geprüft am 04.06.2025.

Stryker, Cole; Kavlakoglu, Eda (2024): Was ist KI? Hg. v. IBM. Online verfügbar unter https://www.ibm.com/de-de/think/topics/artificial-intelligence, zuletzt geprüft am 19.05.2025.

Sutherland, Edwin H. (1949): White Collar Crime. New York.

Thies, Simon; Kureljusic, Marko; Karger, Erik; Krämer, Thilo (2023): Blockchain-Based Triple-Entry Accounting: A Systematic Literature Review and Future Research Agenda. In: *Journal of Information Systems* 37 (3), S. 101–118. DOI: 10.2308/ISYS-2022-029.

WEF (2024): The Global Risks Report. 19th Edition. World Economic Forum, zuletzt geprüft am 23.01.2025.

Abbildungsverzeichnis

11 Abb. 1: Rechtsform der Unternehmen

12 Abb. 2: Anzahl der beschäftigten Mitarbeiter im Unternehmen

12 Abb. 3: Position der Teilnehmenden im Unternehmen

12 Abb. 4: Branchenstruktur der befragten Unternehmen

13 Abb. 5: Räumliche Verteilung der Unternehmen in der Schweiz

13 Abb. 6: Erwirtschafteter Umsatz im letzten abgeschlossenen Geschäftsjahr

15 Abb. 7: Selbstwahrnehmung des Risikos hinsichtlich wirtschaftskrimineller Handlungen

16 Abb. 8: Selbstwahrnehmung des Risikos hinsichtlich wirtschaftskrimineller Handlungen

17 Abb. 9: Einschätzung der Wirtschaftskriminalität in den kommenden 12 Monaten

18 Abb. 10: Erwarteter Anstieg von Wirtschaftsdelikten

19 Abb. 11: Risikofaktoren für wirtschaftskriminelle Vorfälle

21 Abb. 12: Identifizierte Vorfälle von Wirtschaftskriminalität in den vergangenen 2 Jahren

22 Abb. 13: Aufgedeckte Arten von Wirtschaftskriminalität in den letzten 24 Monaten

23 Abb. 14: Anzahl aufgedeckter Vorfälle von Wirtschaftskriminalität in den letzten 24 Monaten

23 Abb. 15: Gesamtschaden durch Wirtschaftskriminalität in den letzten 24 Monaten

23 Abb. 16: Involvierte Tätergruppen

24 Abb. 17: Beteiligung an der Aufdeckung der Vorfälle

25 Abb. 18: Systematische Erfassung von Risiken in Bezug auf Wirtschaftskriminalität

26 Abb. 19: Compliance Verantwortung im Verwaltungsrat

27 Abb. 20: Vorhandensein eines Audit Committees und Zusammensetzung aus >50 % unabhängigen Mitgliedern

27 Abb. 21: Trennung der Rollen von Verwaltungsratspräsident und Geschäftsführer

29 Abb. 22: Implementierte Kontroll- und Präventionsmassnahmen

30 Abb. 23: Herausforderungen in den folgenden 2 Jahren

33 Abb. 24: Beurteilung von Aussagen zu KI als Risiko und Chance

34 Abb. 25: Risiko der eigenen Betroffenheit von KI-generierten Betrugsversuchen

34 Abb. 26: Systematischer Einsatz von KI in Geschäftsprozessen

34 Abb. 27: Betroffenheit von wirtschaftskriminellen Vorfällen mit KI-Einsatz

35 Abb. 28: Massnahmen zur Verhinderung KI-generierter Betrugsversuche

35 Abb. 29: Nutzung von KI zur Prävention von Wirtschaftskriminalität

37 Abb. 30: Art der Massnahme zur Prävention von KI-generierten Betrugsversuchen

Studienpartner

Die Association of Certified Fraud Examiners (ACFE) ist mit mehr als 95'000 Mitgliedern, verteilt auf über 200 Landes- und Regional-Chapters, die weltweit grösste Anti-Fraud-Organisation und führende Anbieterin von Fachveranstaltungen sowie Aus- und Weiterbildungen im Bereich der Betrugs- und Korruptionsbekämpfung.

Ein zentrales Ziel der ACFE besteht in der Förderung von Integrität und Objektivität im Berufsstand des **Certified Fraud Examiner (CFE)**, der international seit vielen Jahren als Qualitätsstandard und Gütesiegel für Anti-Fraud-Experten anerkannt ist.

Das **ACFE Switzerland Chapter** ist die nationale Vertretung von ACFE in der Schweiz. Es bietet eine Plattform für Fachpersonen aus Forensik, Compliance, Revision, Recht, Data Analytics und Risikomanagement im Kampf gegen Wirtschaftskriminalität.

Durch regelmässige Konferenzen, Seminare und Workshops ermöglicht ACFE Switzerland den Austausch über aktuelle Entwicklungen, die Vernetzung mit Expertinnen und Experten sowie die Vermittlung von praxisnahen Werkzeugen. Dabei werden internationale Best Practices an den Schweizer Kontext angepasst und Synergien mit Unternehmen, Behörden und Hochschulen gefördert.

Ein zentrales Thema der letzten Jahre ist die **Künstliche Intelligenz (KI)**. KI eröffnet im Bereich der Betrugs- und Missbrauchsbekämpfung grosse Chancen, bringt indessen auch neue Herausforderungen. Einerseits ermöglichen KI-gestützte forensische Methoden tiefere Einblicke in komplexe Datenmengen, wodurch Muster möglicher Unregelmässigkeiten besser erkannt werden können. Algorithmen unterstützen bei der Früherkennung von Auffälligkeiten in Finanztransaktionen, beim Screening von Mitarbeitenden und Geschäftspartnern oder bei der Untersuchung von Cybercrime. Damit eröffnen sich neue Möglichkeiten für Prävention und Effizienzsteigerung in forensischen Prüfungen.

Andererseits stellen KI-gestützte Technologien auch neue Risikofelder dar. Betrügerische Aktivitäten können durch den Einsatz von KI effizienter ausgeführt und raffinierter verschleiert werden – etwa durch täuschend echte Deepfakes, automatisierte Phishing-Angriffe oder manipulierte Dokumente.

Für Organisationen bedeutet dies, dass Kontrollsysteme kontinuierlich angepasst und Mitarbeitende geschult werden müssen, um den steigenden Anforderungen standzuhalten.
ACFE Switzerland nimmt in diesem Spannungsfeld eine zentrale Rolle ein: Sie fördert den Wissens- und Erfahrungsaustausch unter Fachpersonen und trägt dazu bei, dass die Chancen von KI verantwortungsvoll genutzt und die Risiken frühzeitig erkannt werden. Aus diesem Grund engagiert sich ACFE Switzerland auch als Studienpartner der Hochschule Luzern bei der vorliegenden Studie zur Entwicklung der Wirtschaftskriminalität in der Schweiz.

HSLU Hochschule Luzern

Hochschule Luzern – Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Campus Zug-Rotkreuz
Suurstoffi 1, CH-6343 Rotkreuz