Studie 2024

Risikomanagement und interne Kontrollen – Der Status quo im Schweizer Mittelstand

forvis mazars x Zürcher Hochschule für Angewandte Wissenschaften zh aw School of Management and Law

Vorwort

In einer Zeit, die von wachsender Komplexität und Unsicherheit sowie strenger werdenden rechtlichen und regulatorischen Anforderungen geprägt ist, gewinnen effektives Risikomanagement und ein wirksames internes Kontrollsystem zunehmend an Bedeutung.

Gleichzeitig erkennen immer mehr Unternehmen die Notwendigkeit, auch in diesen Bereichen die Chancen der digitalen Transformation zu nutzen. Mit der vorliegenden Studie wird untersucht, in welchem Ausmass diese Themen auch beim Schweizer Mittelstand relevant und aktuell sind.

Während grössere Unternehmen oft nur schon aufgrund zwingender regulatorischer Vorschriften über einen formalisierten Risikomanagementprozess und ein gut ausgebautes internes Kontrollsystem verfügen, sind viele Schweizer KMU nicht verpflichtet, ein solches System zu unterhalten. Dennoch liegen die Vorteile eines effektiven Risikomanagements und eines wirksamen internen Kontrollsystems auch für diese Unternehmen auf der Hand. Doch wird dies im praktischen Alltag der Schweizer KMU tatsächlich so wahrgenommen und auf sinnvolle Weise gelebt? Und wo stehen kleinere und mittlere Unternehmen in Bezug auf die digitale Transformation?

Die vorliegende Studie nimmt diese Fragen auf. Sie wurde vom Institut für Financial Management der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) in Zusammenarbeit mit Forvis Mazars durchgeführt und untersucht, welchen Stellenwert Risikomanagement und interne Kontrollen in der heutigen Praxis der Schweizer KMU haben und wie ausgeprägt der Trend zur Digitalisierung auch bei den KMU feststellbar ist.

Allen, die in irgendeiner Form an der Studie mitgewirkt haben – sei es über die Teilnahme an der Umfrage, den Interviews, den fundierten Diskussionen oder der Aufbereitung der Daten – gilt an dieser Stelle ein herzlicher Dank. Ihr geschätzter Beitrag hat diese Studie ermöglicht.

Wir wünschen Ihnen viel Spass und interessante Erkenntnisse bei der Lektüre.

Die Autorenschaft

Management Summary

Die aus der Befragung gewonnenen Erkenntnisse zeigen, dass Risikomanagement und interne Kontrollen bei den meisten Unternehmen einen hohen Stellenwert geniessen, wobei sich die befragten Unternehmen im Moment stark mit den Themen IT-Sicherheit und Cyberrisken beschäftigen. Obwohl eine klare Mehrheit der Unternehmen offen für Digitalisierungs- und Automatisierungsvorhaben ist, werden diese noch zögerlich angegangen, insbesondere in den Bereichen Advanced Analytics und Künstliche Intelligenz.

Für die Studie wurden mehrere Tausend Schweizer Unternehmen angeschrieben und aus dem erfreulichen Rücklauf konnten 278 Fragebogen ausgewertet werden. Die Ergebnisse zeigen, dass Risikomanagement und interne Kontrollen für die Mehrheit der befragten Unternehmen von hoher Bedeutung sind. Dies zeigt sich daran, dass Risikomanagement und – in etwas abgeschwächtem Ausmass – interne Kontrollen Bereiche sind, die von der obersten Führungsebene der Unternehmen koordiniert und überwacht werden und dass bei rund der Hälfte der befragten Unternehmen zumindest klare Zuständigkeiten in übergeordneten Stellenprofilen oder, in selteneren Fällen, sogar dedizierte Stellen für diese Bereiche bestehen.

Bei rund drei Vierteln der befragten Unternehmen ist das interne Kontrollsystem (IKS) Bestandteil des Risikomanagements oder es erfolgt zumindest eine regelmässige Abstimmung zwischen den beiden Bereichen. Unternehmen, die das IKS nicht in das Risikomanagement integriert haben und bei denen keine regelmässige Abstimmung erfolgt, sind fast ausschliesslich solche mit weniger als 100 Mitarbeitenden. Auf den Einsatz einer internen Revision oder einer vergleichbaren Stelle (d.h. auf die die vollständige Umsetzung des «Three Lines of Defense»-Modells) setzen nicht ganz unerwartet vor allem grössere Unternehmen.

Die Umfrageergebnisse zum Thema Risikomanagement zeigen, dass formalisierte unternehmensweite Risikomanagementprozesse vor allem in Unternehmen mit mehr als 100 Mitarbeitenden etabliert sind. Die befragten Unternehmen nennen als wichtigste Gründe für die Durchführung eines Risikomanagements die Früherkennung und verbesserte Kontrolle von Risiken, die Sicherung des Fortbestands der Unternehmung sowie die Erkennung und Abwägung von Chancen und Risiken. Auf der kritischen Seite werden im Zusammenhang mit formalisierten Risikomanagementprozessen übermässige Bürokratie und eine zu hohe Bindung personeller Ressourcen aufgebracht. Hinsichtlich der Risikoarten stehen bei den befragten Unternehmen vor allem die IT-Sicherheit und Cyberrisiken im Fokus.

Die Umfrageergebnisse bestätigen, dass grössere Unternehmen tendenziell über ein aktuelles, formalisiertes und standardisiertes internes Kontrollsystem (IKS) verfügen. Diese Unternehmen setzen häufiger auf automatische Kontrollen und systemseitige Unterstützung, wie beispielsweise bei der Funktionstrennung. Der Hauptnutzen eines formalisierten und standardisierten IKS wird von den befragten Unternehmen vor allem im Schutz des Geschäftsvermögens vor Verlust, der Sicherung einer ordnungsgemässen und effizienten Geschäftsführung sowie in der Identifikation und Überwachung finanzieller Risiken

gesehen. Zeitdruck und Personalmangel werden als Hauptursachen für Schwachstellen in den internen Kontrollen genannt. Zu den grössten Herausforderungen im Bereich der internen Kontrollen zählen die laufende Pflege des internen Kontrollsystem, die Digitalisierung und Automatisierung sowie die tägliche Umsetzung der Vorgaben im operativen Geschäft.

Über 80% der befragten Unternehmen stehen Digitalisierungs- und Automatisierungsvorhaben offen bis sehr offen gegenüber. Gleichzeitig fehlt bei fast der Hälfte der Unternehmen eine klar definierte und kommunizierte Digitalisierungsstrategie. Der wichtigste Treiber für die Digitalisierung im internen Kontrollsystem ist die Effizienzsteigerung bei der Durchführung und Überwachung von Kontrollen. Die grösste Herausforderung sehen die befragten Unternehmen in den fehlenden personellen Ressourcen. Während digitale Unterstützung, wie die digitale Ablage von Kontrollnachweisen, bei der Dokumentation von Prozessen und Kontrollen bereits genutzt wird, sind die Unternehmen bei der Automatisierung des internen Kontrollsystems, insbesondere bei Advanced Analytics und Künstlicher Intelligenz/ Maschinellem Lernen, noch zurückhaltend.

Aus den Interviews mit den Expertinnen und Experten wurde deutlich, dass Risikomanagement und interne Kontrollen essenziell für eine effektive Unternehmensführung sind. Ein systematisches Vorgehen ist bei der Ausgestaltung zentral, wobei kleinere Organisationen auch pragmatische Ansätze verfolgen können. Wichtiger als die Umsetzung einer formalisierten Methodik ist, dass ein Risikobewusstsein vorhanden ist und eine angebrachte Risikokultur gelebt wird. Die Ausgestaltung des Risikomanagements und der internen Kontrollen hängt dabei nicht nur von der Unternehmensgrösse, sondern von der Komplexität des Geschäftsmodells ab – es ist allgemein zu beobachten, dass kleine und mittlere Unternehmen in regulierten Branchen oder mit Kunden aus diesen Branchen mit steigenden regulatorischen Anforderungen konfrontiert sind. Die Befragten sehen die grössten zukünftigen Herausforderungen in der Digitalisierung und Automatisierung des internen Kontrollsystems und stellen gleichzeitig fest, dass die Schweizer KMU in diesem Bereich oft noch nicht weit fortgeschritten sind. Dabei sehen sie die fehlenden Ressourcen, die fehlende Standardisierung der Prozesse und mit der Digitalisierung einhergehende Risiken (IT-Sicherheit, Cyberrisiken) als die grössten Herausforderungen. Trotz dieser Herausforderungen sind die Befragten überzeugt, dass sich die Digitalisierung und Automatisierung der Risikomanagement- und Kontrollprozesse auch in der KMU-Welt zukünftig immer stärker durchsetzen wird.

Zusammefassend lässt sich festhalten, dass auch in der KMU-Welt die Chancen und Risiken identifiziert und gesteuert werden müssen. Je nach Komplexität des Geschäftsmodells braucht es hierfür ausgefeiltere Prozesse. Der Grossteil der KMUs ist sich dessen bewusst und hat die Hauptthemen auf dem Radar. Bezüglich systematischer Umsetzung und Automatisierung gibt es nach wie vor Verbesserungspotenzial. Nicht regelkonform zu sein oder sich der Risiken gar nicht bewusst zu sein, können sich auch KMUs in einer Welt, in der die Regulierung ständig zunimmt, nicht leisten.

Inhalt

Grundlagen und Einführung in das Risikomanagement und das interne Kontrollsystem (IKS)

«Risikomanagement» und «Internes Kontrollsystem» (IKS) sind zwei zentrale Konzepte der Unternehmensführung und -steuerung, die eng miteinander verknüpft sind.

Was versteht man unter diesen Begriffen und welche Ziele verfolgen sie? Welche Konzepte, Methoden und Werkzeuge stehen in diesen Bereichen zur Verfügung? Neben der Beantwortung dieser grundlegenden Fragen wird in diesem Kapitel auch auf die spezifischen Anforderungen von KMU eingegangen und ein Überblick über die Möglichkeiten der Digitalisierung und Automatisierung des internen Kontrollsystems gegeben.

Wesen und Zweck

Geht es um die Führung und Steuerung eines Unternehmens, spielen «Corporate Governance» (Führungsstrukturen und -verständnis), «Risikomanagement» und «Internes Kontrollsystem» (IKS) zentrale Rollen. In der Tat sind diese Begriffe eng miteinander verknüpft und ergänzen sich gegenseitig, um die Effizienz, Transparenz und Sicherheit eines Unternehmens zu gewährleisten. Zusammen bilden diese Elemente ein integriertes System, das als **Governance, Risk & Compliance (GRC)** bekannt ist.

Während die **Corporate Governance** der übergeordnete Rahmen ist, der die Regeln, Praktiken und Prozesse definiert, durch die ein Unternehmen geführt und kontrolliert wird, geht es beim **Risikomanagement**, das als zentrales Element von guter Corporate Governance gilt, in erster Linie um den Prozess der Identifikation, Analyse und Bewertung potenzieller Risiken, welche die Vermögens-, Finanz- und Ertragslage eines Unternehmens mittel- und langfristig gefährden könnten. Das Ziel des Risikomanagements besteht hauptsächlich in der Sicherung des Fortbestandes eines Unternehmens, der Absicherung der Unternehmensziele gegen störende Ereignisse und in der Steigerung des Unternehmenswertes (Romeike, 2018, S. 237).

Das **interne Kontrollsystem (IKS)** ist als ein vom Verwaltungsrat, der Geschäftsleitung, den Führungsverantwortlichen und anderen Mitarbeitenden konzipierter, implementierter und betriebener Prozess zu betrachten, welcher der Erlangung einer zweckmässigen Sicherheit zur Erreichung der Unternehmensziele in den Bereichen Effektivität und Effizienz der Tätigkeiten («Operations»), Verlässlichkeit der Berichterstattung («Reporting») und der Gesetzes- und Normenkonformität («Compliance») dient (COSO (2013), S. 2). Das IKS ist ein wesentlicher Bestandteil des Risikomanagements und damit auch einer guten Corporate Governance.

Im Schweizerischen Obligationenrecht (OR) ist die Definition des internen Kontrollsystems enger gefasst – sie beschränkt sich auf die finanzielle Berichterstattung («Financial Reporting»). Gemäss OR ist das Ziel eines IKS, die Übereinstimmung der Jahresrechnung mit den Rechnungslegungsregeln sowie die Ordnungsmässigkeit der Finanzberichterstattung zu gewährleisten und die Gefahr von Fehldarstellungen und Falschaussagen auf ein angemessenen Mass zu reduzieren (Pfaff/Ruud, 2020, S. 26).

Die Corporate Governance bildet somit den Rahmen, in dem Risikomanagement und internes Kontrollsystem integrale Bestandteile darstellen, um eine nachhaltige und verantwortungsbewusste Unternehmensführung sicherzustellen. Eine gute Corporate Governance umfasst automatisch ein wirksames Risikomanagement und ein wirksames internes Kontrollsystem, wobei die Gemeinsamkeiten zwischen dem IKS und dem Risikomanagement am grössten sind, da das IKS einen zentralen Bestandteil des Risikomanagements darstellt (Pfaff/Ruud, 2020, S. 27).

Rahmenkonzepte und Ausgestaltung

Mangels gesetzlicher oder anderer konkreter Vorgaben können die meisten Unternehmen in der Schweiz die konkrete Ausgestaltung ihres Risikomanagements und des internen Kontrollsystems (IKS) weitgehend selber bestimmen.

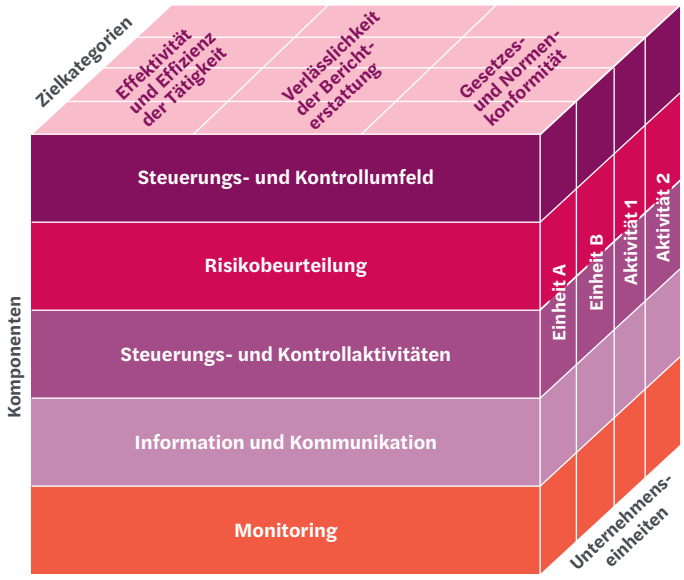
Zur Sicherstellung einer strukturierten Herangehensweise und eines systematischen Aufbaus existieren verschiedene Rahmenkonzepte. Die beiden international etablierten Rahmenwerke ISO 31000 und COSO werden nachfolgend kurz umschrieben. Sie werden von Unternehmen in den häufig als Grundlage genutzt und dann mehr oder weniger stark an die eigenen Strukturen und Prozesse angepasst.

ISO 31000[1] ist ein international anerkannter Standard für Risikomanagement und wird weltweit in verschiedenen Branchen und Organisationen angewendet. Das Rahmenwerk bietet umfassende Leitlinien für das Risikomanagement und stellt sicher, dass das Risikomanagement in alle Aspekte einer Organisation integriert wird und umfasst die Gestaltung, Implementierung, Bewertung sowie die kontinuierliche Verbesserung des Risikomanagements.

Das vom **COSO**[2] entwickelte «Internal Control Framework» ist das weltweit und auch in der Schweiz am weitesten verbreitete Rahmenkonzept zum IKS (Pfaff/Ruud, 2020, S. 36). Das «Internal Control Framework» basiert auf den Dimensionen Zielkategorie, Komponenten und Organisations- bzw. Unternehmenseinheiten und berücksichtigt eine prozessorientierte Betrachtungsweise mit den fünf Komponenten Steuerungs- und Kontrollumfeld, Risikobeurteilung, Steuerungs- und Kontrollaktivitäten, Information und Kommunikation sowie Monitoring (siehe den sog. COSO-Würfel in Abbildung 1). COSO II, auch bekannt als das COSO Enterprise Risk Management Framework (ERM) ist eine Weiterentwicklung des ursprünglichen COSO-Modells und zielt darauf ab, Unternehmen bei der Entwicklung und Verbesserung ihres Risikomanagementsystems zu unterstützen.

Zu beachten ist, dass Schweizer Tochtergesellschaften je nach Konstellation den regulatorischen Vorgaben des Landes unterliegen können, in dem die Muttergesellschaft ihren Hauptsitz hat (z.B. US-SOX, J-SOX, K-SOX).

Abbildung 1: Internal Control Framework des COSO



[1] Vgl. https://www.iso.org/iso-31000-risk-management.html/

[2] COSO steht für das «Committee of Sponsoring Organizations of the Treadway Commission». Diese Organisation wurde gegründet, um die Qualität der Finanzberichterstattung durch ethisches Handeln, wirksame interne Kontrollen und gute Unternehmensführung zu verbessern (vgl. https://www.coso.org/guidance-on-ic).

Methoden und Werkzeuge

Risikomanagement

Eine der zentralen übergeordneten Aufgaben des (strategischen) Risikomanagements ist die Schaffung einer unternehmensweiten Risikokultur, um das Risikobewusstsein der Mitarbeitenden zu stärken und diese zu einem risikoadäquaten Verhalten anzuleiten (Vanini/Rieg, 2021, S. 37). Das operative Risikomanagement umfasst die folgenden Aufgaben:

- **Risikoidentifikation:** Ziel der Risikoidentifikation ist die Erfassung aller Gefahrenquellen, Schadenursachen, Störpotenziale und Chancen sowie deren wechselseitige Abhängigkeiten (Vanini/Rieg, 2021, S. 199).
- **Risikobewertung/-analyse:** Die Risikobewertung umfasst die Analyse der Risikoursachen bzw. -faktoren, die Quantifizierung der Auswirkungen von Risiken auf die Unternehmensziele sowie die Einschätzung der Relevanz des Risikos (Vanini/Rieg, 2021, S. 232).
- **Risikoberichterstattung/-reporting:** Das Ziel der Risikoberichterstattung ist die Schaffung von Transparenz über die Risikosituation der Unternehmung zur Vorbereitung von Entscheidungen über notwendigen Massnahmen und zur Unterstützung der Risikoüberwachung (Vanini/Rieg, 2021, S. 299).
- **Risikosteuerung:** Durch die Risikosteuerung werden die identifizierten und bewerteten Risiken unter Berücksichtigung der Risikostrategie, der Risikotragfähigkeit und der Risikoneigung der Unternehmensführung («Risikoappetit») durch geeignete Massnahmen beeinflusst (gemindert) oder im unwesentlichen Fall bewusst getragen (Vanini/Rieg, 2021, S. 311).
- **Risikokontrolle:** Im Rahmen der Risikoüberwachung werden die Funktionsfähigkeit und die Umsetzung des Risikomanagements regelmässig überprüft und bei Bedarf angepasst (Vanini/Rieg, 2021, S. 339).

Zur Erreichung der Ziele des Risikomanagements stehen verschiedenste Methoden zur Verfügung, wobei für ein effektives Risikomanagement insbesondere die Werkzeuge zur Risikoidentifikation, -analyse und -bewertung im Fokus stehen (Romeike, 2018, S. 55). Die Methoden zur Risikoidentifikation, Risikoanalyse und Risikobewertung lassen sich in Kollektionsmethoden sowie Suchmethoden unterteilen (Romeike, 2018, S. 56 ff.):

- **Kollektionsmethoden** sind vor allem für Risiken geeignet, die offensichtlich oder bereits bekannt sind (beispielsweise aufgrund einer bereits in der Vergangenheit durchgeführten Risikoidentifikation) und dienen im Wesentlichen einer strukturierten Darstellung bzw. Zusammenfassung von Ergebnissen, die mit Hilfe anderer Methoden (wie Brainstorming) erfasst wurden. Die Kollektionsmethoden umfassen Instrumente wie die SWOT-Analyse, das Self-Assessment oder die Risiko-Identifikationsmatrix (RIM) – in der Praxis erfolgt die Identifikation von Risiken jedoch häufig unter Verwendung von Checklisten.
- **Suchmethoden** werden dagegen vor allem für bisher unbekannte Risiken eingesetzt und können in analytische Methoden und Kreativitätsmethoden eingeteilt werden. Alle analytischen Suchverfahren sind darauf fokussiert, zukünftige und bisher unbekannte Risikopotenziale zu identifizieren und beinhalten eine Vielzahl etablierter Methoden wie die Bow-tie Analysis, die empirische Datenanalyse, die Fehlerbaumanalyse (Fault Tree Analysis, FTA), die Fehlermöglichkeits- und Einflussanalyse (FMEA), Hazard and Operability Studies (HAZOP) und die Fehler-Ursachen-Analyse (Root Cause Analysis, RCA). Kreativitätsmethoden hingegen basieren auf kreativen Prozessen, die durch divergentes Denken charakterisiert sind, um flexibel zu neuartigen Einfällen und originellen Lösungen zu gelangen, um so bisher unbekannte Risikopotenziale zu identifizieren. Unter die Kreativitätstechniken fallen Methoden wie das Brainstorming/-writing, die morphologische Analyse, die Methode 365, Mind Mapping, die Flip-Flow-Technik (Kopfstandtechnik), World-Café, die Delphi-Methode sowie die deterministische oder die stochastische Szenarioanalyse.

Welche Methoden zur Anwendung kommen, hängt insbesondere von der Risikoart, aber auch vom angestrebten Reifegrad des Risikomanagements ab.

Internes Kontrollsystem

Ein internes Kontrollsystem (IKS) ist ein systematisches Konzept, welches sicherstellt, dass entlang der wesentlichen Risiken eines Geschäftsmodells adäquate Kontrollen installiert sind. Es umfasst verschiedene Kontrollarten, die in zwei Hauptkategorien unterteilt werden können: Während **präventive Kontrollen** darauf abzielen, Fehler oder Unregelmässigkeiten zu verhindern, **bevor** sie auftreten (z.B. durch Zugriffskontrollen), sind **detektive Kontrollen** darauf ausgelegt, Fehler oder Unregelmässigkeiten zu entdecken, **nachdem** sie aufgetreten sind (Beispiele hier-

für sind Überwachungs- und Prüfungsaktivitäten wie regelmässige Überprüfungen/Reviews oder Audits und Abstimmungen und Analysen). Beide Kontrollarten können sowohl manuell als auch automatisiert durchgeführt werden. **Manuelle Kontrollen** werden von Mitarbeitenden durchgeführt und erfordern menschliches Eingreifen. Beispiele sind die manuelle Kontrolle von Dokumenten (Rechnungen, Verträge), manuelle Genehmigungen oder die physische Inventur. **Automatische Kontrollen** werden durch IT-Systeme nach einem definierten, standardisierten System ausgeführt. Beispiele dafür sind systembasierte Prüfungen (z.B. automatische Überwachung von Transaktionen in einer Datenbank), Zugriffskontrollen (z.B. Beschränkung des Zugriffs auf bestimmte Systeme oder Daten) oder die automatische Erkennung von Anomalien oder Fehlern bei der Datenerfassung bzw. -verarbeitung.

Dabei lassen sich folgen Arten von Kontrolltätigkeiten auseinander halten (EXPERTsuisse, 2022, PS-CH 890, IV Bst. j):

- Die **Genehmigung** bezieht sich auf die Autorisierung von Transaktionen und Aktivitäten durch befugte Personen. Ziel ist es, sicherzustellen, dass nur autorisierte Transaktionen durchgeführt werden.
- Bei der **Ergebniskontrolle** handelt es sich um die Überwachung und Bewertung der Leistung von Mitarbeitenden und Prozessen. Dies kann durch regelmässige Überprüfungen, Audits und Berichte erfolgen.
- Die **Informationsverarbeitung** umfasst die Sicherstellung der Genauigkeit, Vollständigkeit und Verlässlichkeit von Daten und Informationen, die in den Unternehmensprozessen verwendet werden. Dazu gehören auch IT-Kontrollen (IT General Controls, «ITGC»), die den Zugang zu und die Verarbeitung von Daten überwachen.
- Die **physischen Kontrollen** beinhalten Massnahmen zum Schutz physischer Vermögenswerte des Unternehmens. Beispiele sind räumliche Zugangsbeschränkungen und regelmässige Bestandesaufnahmen (Inventur).
- Die **Funktionstrennung** zielt darauf ab, Interessenkonflikte und Betrug zuverhindern, indem kritische Aufgaben und Verantwortlichkeiten auf verschiedene Personen verteilt werden («Vier-Augen-Prinzip»). Zum Beispiel sollten die Aufgaben der Buchführung, der Genehmigung von Transaktionen und der Überprüfung von Berichten nicht von derselben Person ausgeführt werden.

Verantwortlichkeiten

In Bezug auf Risikomanagement und interne Kontrollen sind in einem Unternehmen in der Regel verschiedene Akteure bzw. Funktionen für bestimmte Aufgaben verantwortlich bzw. zuständig. Nachfolgend werden diese anhand des Beispiels einer Aktiengesellschaft beschrieben.

Generalversammlung

Der Generalversammlung als oberstes Organ einer Aktiengesellschaft (OR 698 Abs. 1) obliegt die unübertragbare Befugnis, die Jahresrechnung zu genehmigen (OR 698 Abs. 2 Ziff. 4). Demgegenüber sind insbesondere die Oberleitung der Gesellschaft, die Festlegung der Organisation und die Ausgestaltung des Rechnungswesens gemäss OR 716a Abs. 1 unübertragbare Aufgaben des Verwaltungsrats. Die Generalversammlung ist nicht befugt, über die Ausgestaltung des IKS zu befinden (Pfaff/Ruud, 2020, S. 54). Dennoch sind die Aktionäre sehr daran interessiert, dass ein effektives Risikomanagement und ein gut funktionierendes IKS zum Schutz ihres investierten Kapitals vorhanden sind.

Verwaltungsrat

Der Verwaltungsrat ist gemäss Art. 716a, Abs. 1, Ziff. 5 OR in der Verantwortung, die mit der Geschäftsführung betrauten Personen im Hinblick auf Einhaltung von Gesetz, Statuten, Reglementen und Weisungen zu überwachen. Das bedeutet, dass die aus der Risikoidentifikation ermittelten Risiken entsprechend zu reglementieren und die Einhaltung der Reglemente zu überwachen sind. Die Pflicht des Verwaltungsrates für die Ausgestaltung, Implementierung und Aufrechterhaltung eines geeigneten und angemessenen IKS lässt sich auch aus Art. 716a, Abs. 1, Ziff. 3 i. V. m. Art. 957 ff. OR ableiten[3]. Er hat damit in erster Linie zu verantworten, dass geeignete Steuerungs- und Kontrollaktivitäten implementiert sind, um wesentliche Fehler in der finanziellen Berichterstattung zu verhindern, aufzudecken und zu korrigieren (EXPERTsuisse, 2022, PS-CH 890 III Bst. c). Zur Unterstützung der Wahrnehmung seiner Aufgaben betreffend dem IKS kann der Verwaltungsrat aus seiner Mitte einen Ausschuss einsetzen, der sich primär mit der Rechnungslegung, der Abschlussprüfung, dem Risikomanagement, den IKS und der internen Revision befasst (z.B. ein «Audit Committee» oder ein «Risk Committee»).

[3] Vgl. auch EXPERTsuisse, 2022. PS-CH 890, A I Bst. b

Geschäftsleitung

Die Geschäftsleitung ist für die Umsetzung der Vorgaben des Verwaltungsrats sowie das Erfüllen von dessen Anforderungen bezüglich Ausgestaltung und Aufrechterhaltung des IKS zuständig, sofern diese Aufgaben nicht vom Verwaltungsrat selbst wahrgenommen werden (Ruud/Friebe 2013, S. 27 und Art. 716b OR). Gemäss PS-CH 890 beinhaltet dies insbesondere folgende Aufgaben (EXPERT-suisse, 2022. PS-CH 890 III Bst. e.):

- Entwicklung geeigneter Prozesse zur Identifikation, Einschätzung und Überwachung der eingegangenen Risiken;
- Aufrechterhaltung und Dokumentation einer Organisationsstruktur, welche Verantwortlichkeiten, Kompetenzen und Informationsflüsse festhält;
- Identifikation von Schlüsselkontrollen und deren Überwachung;
- Sicherstellung der Vornahme von Korrekturmassnahmen bei vorliegenden Mängeln;
- Sicherstellung der Erfüllung delegierter Aufgaben.

Zudem stellt die Geschäftsleitung die nötigen personellen Ressourcen mit der entsprechenden Qualität hinsichtlich Ausbildung und Erfahrung zur Verfügung.

Verteidigungslinien

Das Modell der drei Verteidigungslinien («Three-Lines-of-Defense»-Modell, siehe Abbildung 2), das ursprünglich 2013 vom Institute of Internal Auditors (IIA) veröffentlicht wurde, hat sich international als Konzept zur organisatorischen Einbettung der Kontrollfunktion etabliert. Es beschreibt, wie das inhärente Risiko durch drei sogenannte Verteidigungs- oder Kontrolllinien («Lines of Defense») auf das vom Verwaltungsrat akzeptierte Restrisiko reduziert wird. Diese drei Linien arbeiten wie nachfolgend beschrieben zusammen, um ein effektives Risikomanagement sicherzustellen und eine unabhängige Überprüfung sowie Verbesserung der Risikomanagementprozesse zu ermöglichen:

- **Erste Verteidigungslinie (operatives Management):** Die operativen Einheiten bzw. das operative Management sind für die Identifizierung und Steuerung von Risiken im Tagesgeschäft verantwortlich und für die Implementierung und Durchführung von Kontrollmassnahmen zuständig, um Risiken frühzeitig zu erkennen und zu minimieren.
- **Zweite Verteidigungslinie (Risikomanagement und Compliance):** Diese Linie überwacht und unterstützt die Kontrollaktivitäten der ersten Linie und ist für die Entwicklung von Richtlinien und Verfahren, die Überwachung der Einhaltung von Vorschriften und für die Unterstützung des operativen Managements bei der Risikobewertung zuständig.
- **Dritte Verteidigungslinie (Interne Revision):** Die interne Revision prüft unabhängig die Wirksamkeit der ersten und zweiten Linie, indem sie entsprechende Audits durchführt und die Effizienz und Effektivität des Risikomanagements und der internen Kontrollen bewertet. Im Gegensatz zu den ersten beiden Linien berichtet die dritte Linie nicht an die Geschäftsleitung, sondern direkt an den Verwaltungsrat bzw. wenn vorhanden an das Audit Committee.

Revisionsstelle

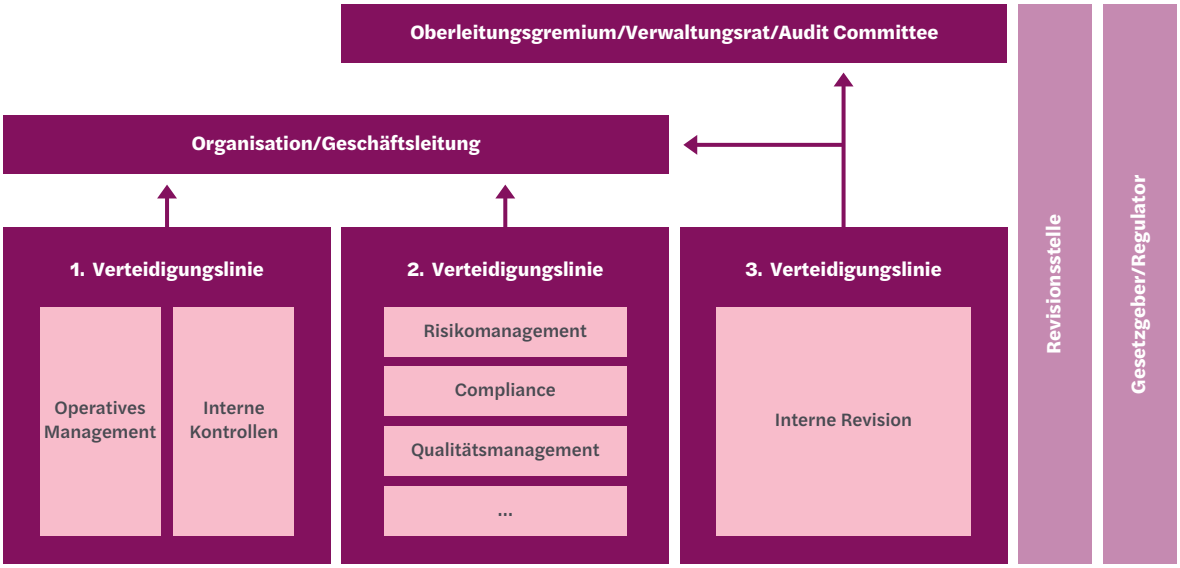
Die Revisionsstelle kann als eine unternehmensexterne weitere, «vierte» Verteidigungslinie verstanden werden. Sie stellt als unabhängige Partei im Auftrag des Verwaltungsrates gegenüber den Kapitalgebern sicher, dass die Rechnungslegung gesetzes- und statutenkonform erfolgt. Bei Gesellschaften, die der ordentlichen Revision unterstellt sind[4], hat die Revisionsstelle gemäss OR 728a Abs. 1 Ziff. 3 zu prüfen, ob ein IKS existiert. Bei der Durchführung und der Festlegung des Umfangs der Prüfung berücksichtigt die Revisionsstelle das interne Kontrollsystem (Art. 728a, Abs. 2 OR). Ein solides IKS mindert das Risiko negativer Einflüsse auf die Vermögens- und Finanzlage eines Unternehmens und bietet der Revisionsstelle eine wertvolle Basis für ihre Prüfarbeit und das daraus abgeleitete Prüfurteil.

Damit die Revisionsstelle beurteilen kann, ob ein IKS existiert, müssen die Unternehmen – in erster Linie der Verwaltungsrat und die Geschäftsleitung – folgende Voraussetzungen sicherstellen (EXPERT-suisse, 2022, PS-CH 890 VII Bst. a):

- Das interne Kontrollsystem (IKS) ist vorhanden und überprüfbar, also dokumentiert.
- Das IKS ist den jeweiligen Risiken und der Geschäftstätigkeit des Unternehmens angemessen.
- Das IKS ist den zuständigen Mitarbeitenden bekannt.
- Das definierte IKS wird angewendet.
- In der Einheit ist ein Kontrollbewusstsein vorhanden.

Können diese fünf Punkt positiv beantwortet werden, kann die Existenz eines IKS bestätigt werden. Die Schweizerischen Vorschriften gehen nicht soweit, dass auch die Wirksamkeit überprüft und bestätigt werden muss, wie das internationale Regeln wie beispielsweise die SOX-Bestimmungen[5] verlangen. Für den nachhaltigen Unternehmenserfolg ist es jedoch eine zwingende Voraussetzung, dass Unternehmen ihre Risiken kennen, steuern und überwachen. Die Organe der Gesellschaft haben also auch ohne eine solche gesetzliche Vorschrift ein grosses Interesse daran, über ein ihrem Geschäftsmodell angepasstes wirksames IKS zu verfügen.

Abbildung 2: «Three-Lines-of-Defense»-Modell (in Anlehnung an: Pfaff/Ruud, 2020, S. 54)



[4] Dazu gehören gemäss OR 727 insbesondere Publikumsgesellschaften und Unternehmen, die zwei der nachstehenden Grössen in zwei aufeinanderfolgenden Geschäftsjahren überschreiten: CHF 20 Mio. Bilanzsumme, CHF 40 Mio. Umsatz, 250 Vollzeitstellen im Jahresdurchschnitt

[5] SOX steht für Sarbanes-Oxley Act. Er wurde 2002 nach diversen Bilanzskandalen amerikanischer Unternehmen verabschiedet mit dem Ziel, die Verlässlichkeit der Berichterstattung von Unternehmen, die den Kapitalmarkt der USA in Anspruch nehmen, zu verbessern.

Gesetzliche und regulatorische Bestimmungen zu Risikomanagement und IKS

Gesetzliche Vorschriften

Bezüglich Risikomanagement und dem internen Kontrollsystem sind in der Schweiz die folgenden gesetzliche Vorschriften zu berücksichtigen:

Durchführung einer Risikobeurteilung

Gemäss OR Art. 967 müssen Unternehmen, die von Gesetzes wegen zu einer ordentlichen Revision verpflichtet sind, einen Lagebericht verfassen, im Rahmen dessen Aufschluss über die Durchführung einer Risikobeurteilung gegeben werden muss (OR 961c Abs. 2 Ziff. 2). Eine konkrete Regelung zu dazu notwendigen Angaben findet sich im OR nicht, gemäss dem Handbuch der Wirtschaftsprüfung können aber folgende Aspekte relevant sein, um über die Durchführung einer Risikobeurteilung Aufschluss zu geben (EXPERTsuisse (2023), Ziff. 269, S. 93):

- Ziele des Risikomanagements;
- Organisation, Zuständigkeit und Instrumente des Risikomanagements;
- Risikofaktoren im laufenden Geschäftsjahr: Quantifizierung und Spezifizierung der Risiken;
- wesentliche Massnahmen zur Steuerung der Risiken (Absicherungsgeschäfte, Versicherungen, Risikogrundsätze);
- wesentliche Unternehmensrisiken, insbesondere Markt- und operationelle Risiken sowie Gegenparteirisiken.

Da der Lagebericht in erster Linie Aufschluss über wichtige Einflussfaktoren für die Entwicklung des Geschäftsgangs sowie Indikatoren der künftigen Geschäftsentwicklung geben soll und es somit um die Vermittlung des Gesamtbilds der Unternehmenslage geht, bezieht sich die Angabepflicht auf die allgemeinen Unternehmensrisiken und geht damit über die finanziellen Risiken hinaus (Glanz/Pfaff, 2013, S. 30-32).

Existenz eines internen Kontrollsystems

Gemäss den obligationenrechtlichen Bestimmungen muss die Revisionsstelle wie bereits oben erwähnt im Rahmen der ordentlichen Revision prüfen, ob ein internes Kontrollsystem existiert (OR 728a Abs. 1 Ziff. 3). Entsprechend ist auch diese Bestimmung nur dann zwingend anwendbar, wenn das Unternehmen von Gesetzes wegen zu einer ordentlichen Revision verpflichtet ist.

Aus den gesetzlichen Bestimmungen finden sich keine Angaben dazu, wie die Ausgestaltung eines IKS konkret aussehen könnte. Es ist also an den Unternehmen selber zu entscheiden, welche Steuerungs- und Kontrollaktivitäten sie für ihre Situation als angemessen erachten, wobei die Grösse des Unternehmens, die Komplexität der Geschäftstätigkeit und das Risikoprofil für diesen Entscheid relevant sind (EXPERTsuisse, 2022, PS-CH 890 A I Bst. b.). Damit ein IKS als «existent» bezeichnet werden kann, muss es – wie in Abschnitt «Verantwortlichkeiten» ausgeführt – dokumentiert, den Geschäftsrisiken und dem Umfang der Geschäftstätigkeit angepasst und den Mitarbeitenden bekannt sowie durch diese umgesetzt sein, was ein Kontrollbewusstsein auf allen Stufen des Unternehmens bedingt (EXPERTsuisse, 2023, Ziff. 145, S. 60/61).

Weitere regulatorische Bestimmungen und Empfehlungen

Swiss Code of Best Practice for Corporate Governance

Der «Swiss Code of Best Practice for Corporate Governance» (kurz «Swiss Code») wurde von economiesuisse (Verband der Schweizer Unternehmen aus allen Branchen) veröffentlicht und wendet sich in Form von Leitlinien und Empfehlungen in erster Linie an die schweizerischen Publikumsgesellschaften, aber auch nichtkotierte Gesellschaften oder Organisationen können ihm zweckmässige Leitideen entnehmen (economiesuisse, 2024, S. 6).

Bezüglich dem internen Kontrollsystem (IKS) konkretisiert der «Swiss Code», dass dem Verwaltungsrat die Verantwortung für die Ausgestaltung des IKS obliegt, während die konkrete Umsetzung unter Berücksichtigung der Effektivität und Effizienz der Tätigkeiten («Operations»), der Verlässlichkeit der finanziellen und nichtfinanziellen Berichterstattung («Reporting») sowie der Gesetzes- und Normenkonformität («Compliance») im Zuständigkeitsbereich der Geschäftsleitung liegt (economiesuisse, 2024, S. 18). In Bezug auf das Risikomanagement gibt der «Swiss Code» vor, dass der Verwaltungsrat mindestens einmal jährlich eine Risikobeurteilung vornimmt und deren Ergebnis für seine Leitungs- und Aufsichtsaufgaben sowie für die Weiterentwicklung des internen Kontrollsystems berücksichtigt (economiesuisse, 2024, S. 18). Zudem empfiehlt der «Swiss Code», eine Interne Revision einzurichten, die an das «Audit Committee» oder dem Verwaltungsrat Bericht erstattet (economiesuisse, 2024, S. 19).

Corporate Governance Richtlinie der SIX Swiss Exchange

Die «Richtlinie betreffend Informationen zur Corporate Governance» (RLCG) gilt für alle Unternehmen, die an der Schweizer Börse SIX Swiss Exchange kotiert sind.

Nach der RLCG sollen die Emittenten den Anlegern im jährlichen Geschäftsbericht grundlegende Informationen zur Corporate Governance zugänglich machen. Dazu gehören u.a. auch Angaben zu den Grundzügen der Kompetenzregelung zwischen Verwaltungsrat und Geschäftsleitung sowie zu den Informations- und Kontrollinstrumenten des Verwaltungsrats gegenüber der Geschäftsleitung (Ziffern 3.5, 3.6 und 3.7 des Anhangs zur RLCG).

Allerdings enthält die RLCG keine Vorschriften darüber, wann und in welcher Ausgestaltung ein IKS vorhanden sein muss – es geht lediglich um die Offenlegung der konkret vorhandenen Kontrollinstrumente. Die genannten Bestimmungen dürften im Markt aber durchaus die Erwartung fördern, dass die börsenkotierten Gesellschaften dem IKS eine ausreichend grosse Bedeutung beimessen. Zudem gilt für sämtliche von der Richtlinie geforderten Angaben zum Anhang der «comply or explain»-Grundsatz (vgl. RLCG Art. 7). Sieht der Emittent von der Offenlegung bestimmter Informationen ab, so ist im Bericht ausdrücklich auf diesen Umstand hinzuweisen und die Abweichung einzeln und substanziell zu begründen.

Bestimmungen für Unternehmen aus regulierten Branchen und Organisationen im öffentlichen Sektor

Für Unternehmen im Finanzsektor, insbesondere Banken, Effektenhändler und Versicherungen, bestehen bereits seit einiger Zeit konkrete gesetzliche und aufsichtsrechtliche Bestimmungen, die das Risikomanagement und das IKS betreffen und das Vorhandensein eines IKS oder eines Risikomanagements sehr konkret vorschreiben.[7] Auch für öffentlich-rechtliche Organisationen bestehen teilweise spezifische Vorschriften über das interne Kontrollsystem.[8] Es wird hier nicht weiter darauf eingegangen, weil in der vorliegenden Studie diese Unternehmen nicht Teil der befragten Gruppe waren.

Schweizer Prüfstandard PS-CH 890

Der Schweizer Prüfstandard 890 der EXPERTsuisse stellt den Standard dar, der in der Schweiz allgemein für die Prüfung eines IKS verwendet wird. Die Standards der EXPERTsuisse haben zwar nicht Gesetzescharakter, stellen aber die hilfreiche Umsetzungsleitlinien zur Verfügung für Themen, welche das Obligationenrecht nicht oder zu rudimentär regelt. PS-CH 890 bietet Empfehlungen zur Struktur und den Elementen eines effektiven IKS und wird sowohl für privatrechtliche wie auch öffentliche-rechtliche Organisationen verwendet.

Der Zweck des PS-CH 890 besteht darin, das Vorgehen zur Erlangung eines Prüfungsurteils über die Existenz eines internen Kontrollsystems (IKS) in der Finanzberichterstattung gemäss Art. 728a, Abs. 1, Ziff. 3 OR (PS-CH 890, A I Bst. a) zu beschreiben

Einleitend werden die Aufgaben und Verantwortlichkeiten des Verwaltungsrats, des Managements und der Revisionsstelle in Bezug auf das IKS erläutert. Weiter werden die Komponenten eines IKS beleuchtet, die folgende sind: Kontrollumfeld, Risikobeurteilungsprozess der Einheit, rechnungslegungsbezogene Informationssysteme, Kontrollaktivitäten und Überwachung der Kontrollen. Zudem werden die Grenzen eines IKS aufgezeigt und eine Abgrenzung zwischen der Berücksichtigung des IKS im Rahmen der Abschlussprüfung und der Prüfung der Existenz eines IKS vorgenommen. Darüber hinaus werden die Anforderungen an die Prüfbarkeit eines IKS dargelegt. Diese Kriterien sind auch für die geprüften Unternehmen relevant, da sie wissen müssen, welche Mindestanforderungen erfüllt sein müssen, damit die Revisionsstelle die Existenz eines IKS bestätigen kann.

[7] Vgl. z. B. Rundschreiben 2017/1 Corporate Governance – Banken oder Rundschreiben 2017/2 Corporate Governance – Versicherer.
[8] Vgl. z. B. Finanzhaushaltgesetz (FHG) i. V. m. Verordnung über das Finanzhaushaltsrecht (FHV).

Besonderheiten bei KMU

Kleine und mittlere Unternehmen (KMU) weisen gegenüber grösseren Unternehmen verschiedene Besonderheiten auf, die bei der Implementierung und Aufrechterhaltung eines internen Kontrollsystems (IKS) zu beachten sind und die die Anwendung von «Best Practice»-Anforderungen an die Ausgestaltung eines IKS zur Herausforderung machen:

- **Begrenzte Ressourcen:** KMU haben oft weniger finanzielle und personelle Ressourcen – insbesondere Managementressourcen – zur Verfügung, was die Implementierung eines umfassenden IKS erschwert. Aufgrund begrenzter Ressourcen besteht in KMU oft keine eigenständige Interne Revision oder eine vergleichbare Stelle.
- **Governance-Strukturen:** In vielen KMUs sind die Führungsstrukturen organisch mit der Geschäftsentwicklung gewachsen und die Schlüsselpersonen übernehmen entsprechend viele Aufgaben. Bewusste Führungsstrukturen im Sinne von «checks and balances»[9] werden, wenn überhaupt, vielfach erst später eingeführt. Das Vereinen vieler Aufgaben auf ein und die selbe Person kann zudem dazu führen, dass jemand seine eigene Arbeit kontrollieren müsste.
- **Flache Hierarchien:** In KMU sind die Hierarchien oft flacher, was zu einer engeren Zusammenarbeit und direkteren Kommunikationswegen führt. Dies kann die Überwachung und Kontrolle erleichtern, aber auch Herausforderungen bei der Trennung von Verantwortlichkeiten (Funktionstrennung/ «Vier-Augen-Prinzip») mit sich bringen.
- **Dokumentation:** Aufgrund knapper Ressourcen müssen KMU oft pragmatische und kosteneffiziente Ansätze wählen, um ein passendes IKS zu schaffen. Dies bedeutet, dass die Systeme oft weniger formalisiert und dokumentiert sind als in grösseren Unternehmen. Eine Dokumentation der unternehmensinternen Regelungen zum IKS oder von Vorgaben des Unternehmens in den Arbeitsrichtlinien oder -bestimmungen ist gerade bei KMU häufig nicht oder nur partiell vorhanden (Pfaff/Ruud, 2020, S. 118).
- **Fokus auf externe Anforderungen:** Wenn KMU externe Anforderung wie die Existenz eines IKS gemäss Obligationenrecht (OR) erfüllen müssen, kann dies dazu führen, dass das IKS infolge der Priorisierung von Aufgaben primär zur Erfüllung dieser Anforderungen implementiert wird, anstatt als umfassendes Managementinstrument genutzt zu werden.

Auf der anderen Seite können KMU in verschiedenen Bereichen auch Vorteile haben. So ist es zum Beispiel im Rahmen des Monitoring aufgrund der engen Einbindung der Geschäftsleitung ins Tagesgeschäft häufig leichter, Abweichungen vom Soll-Zustand und potenzielle Fehler zu identifizieren (Pfaff/Ruud, 2020, S. 123). Ebenso kann sich die Information und Kommunikation in kleineren Unternehmen aufgrund der flacheren Hierarchiestrukturen, der geringeren Zahl an Mitarbeitenden, der schnelleren Verfügbarkeit der Geschäftsleitung sowie des persönlich informellen Verhältnisses aller Mitarbeitenden einfacher gestalten als in grösseren Unternehmen (Pfaff/Ruud, 2020, S. 123). Und sofern die Geschäftsleitung bzw. die Eigentümerschaft den internen Kontrollen eine grosse Bedeutung zumisst und dies auch kommuniziert und vorlebt, kann aufgrund des persönlicheren Umgangs, der flacheren Hierarchien sowie der informellen Organisationsstruktur das notwendige Kontrollbewusstsein massgeblich positiv geprägt werden (Pfaff/Ruud, 2020, S. 119). Schliesslich können die Risiken für das Privatvermögen des Unternehmers das Ziel der langfristigen Existenzsicherung des Unternehmens stärker in den Fokus setzen und sich dadurch positiv auf den Risikobeurteilungsprozess auswirken (Pfaff/Ruud, 2020, S. 121).

Zur Stärkung der internen Kontrollen können bei KMU folgende Möglichkeiten beitragen (Pfaff/Ruud, 2020, S. 124):

- Besondere Beachtung des Steuerungs- und Kontrollumfelds: Auch im KMU-Umfeld lohnt sich ein explizites Bekenntnis zu Integrität und ethischen Werten, die Sicherstellung der Unabhängigkeit aufsichtsrechtlicher Stellen sowie die Etablierung angemessener Strukturen und Verantwortlichkeiten.
- Integration der Steuerungs- und Kontrollaktivitäten in das Weisungswesen und in die Unternehmenskultur zur Sicherstellung der Identifikation und Überwachung der wesentlichen Risiken.
- Erhöhung der Verlässlichkeit von Buchführung und Rechnungslegung durch Einsatz von Standardsoftware und externer Expertise (zum Beispiel Steuerberatung, Outsourcing von Teilen des Informationsmanagements).
- Outsourcing und damit Absicherung bestimmter Aktivitäten, die nicht zu den primären wertschöpfenden Prozessen des Unternehmens zählen.
- Fokussierung auf bedeutende Risiken und Verzicht auf mathematisch oder statistisch fundierte Risikoanalysen (Vermeidung Scheingenauigkeit).

[9] Ausgewogenes Verhältnis von Anordnung und Kontrolle.

- Einhaltung des «Vier-Augen-Prinzips» trotz begrenzter Personalressourcen wo immer möglich (insbesondere im Zahlungsverkehr, wo der Schutz des Vermögens in besonderer Weise betroffen ist) und Vermeidung personeller Klumpenrisiken in diesen Bereichen.
- Stärkung des Verwaltungsrats durch Finanzexperten und gegebenenfalls (bei hinreichender Grösse) Einrichtung eines «Audit Committee».
- Einbezug der Geschäftsleitung (der Unternehmerpersönlichkeit) in die Überwachung des IKS und Wahrnehmung einer Funktion im Sinne eines Chief Operating Officers (COO), um die Prozesssicht zu gewährleisten.
- Verzicht auf das Opting-out[10]: obschon im Rahmen der eingeschränkten Revision die Existenz des IKS nicht explizit geprüft wird, bietet die eingeschränkte Revision der Geschäftsleitung eine zusätzliche Sicherheit.

Zusammenfassend lässt sich festhalten, dass KMUs von ihrer Ausstattung her eher pragmatischere interne Kontrollsysteme implementiert haben. Nichtsdestotrotz müssen Unternehmen egal welcher Grösse die zentralen Risiken ihres Geschäftsmodells kennen und in geeigneter Form steuern. Dabei ist vielfach gar nicht so sehr nur die Grösse ein entscheidendes Kriterium, sondern vielmehr die Frage, wie komplex das Geschäftsmodell des KMUs ist und/oder ob es Teil einer Lieferkette in regulierten Branchen ist.

Digitalisierung im Bereich des internen Kontrollsystems

Die Digitalisierung und Automatisierung eines internen Kontrollsystems (IKS) bietet zahlreiche Möglichkeiten, um Effizienz und Genauigkeit zu steigern. Nachfolgend werden – ohne Anspruch auf Vollständigkeit – einige ausgewählte etablierte Digitalisierungsmöglichkeiten aufgeführt:

- **GRC-Tools und Workflow-Management-Lösungen:** Der Einsatz von GRC-Tools ermöglicht die Digitalisierung der Kontrollverwaltung. Dies umfasst unter anderem das zentrale Management von Kontrollen, Verantwortlichkeiten und Kontrolldurchführungen sowie die digitale Ablage von Kontrollnachweisen. Diese Systeme unterstützen auch die Digitalisierung von Richtlinien und beschleunigen die Durchlaufzeiten von IKS-Standardprozessen. Darüber hinaus ermöglichen sie eine effizientere Verwaltung und Nachverfolgung von Freigabeprozessen.
- **Robotic Process Automation (RPA):** RPA kann repetitive, manuelle Kontroll- und IKS-bezogene Tätigkeiten automatisieren. Dies reduziert Fehler und spart Zeit, indem Routineaufgaben von Software-Robotern übernommen werden.
- **Advanced Analytics:** Durch den Einsatz von Advanced Analytics können Unternehmen Daten in Echtzeit analysieren und überwachen. Dies ermöglicht eine proaktive Identifikation von Risiken und Unregelmässigkeiten, aber auch von Chancen.
- **ERP-Systeme:** Enterprise Resource Planning (ERP)-Systeme integrieren verschiedene Geschäftsprozesse und bieten eine zentrale Plattform für die Überwachung und Steuerung von Kontrollen. Sie unterstützen die Automatisierung von Finanz- und Betriebsprozessen und ermöglichen häufig die Implementierung automatischer Kontrollen. Darüber hinaus bieten sie die Möglichkeit, organisatorische Funktionstrennungen über das Berechtigungskonzept abzubilden, was zur Stärkung des internen Kontrollsystems (IKS) beiträgt.
- **Decision Modelling:** Diese Technologie hilft bei der Erstellung von Entscheidungsmodellen, die komplexe Kontrollprozesse unterstützen und automatisieren können.
- **Digitale Eingangsrechnungsbearbeitung:** Durch das digitale Erfassen und Auslesen von Rechnungen können Fehler minimiert und die Datenqualität verbessert werden. Dies führt zu einer höheren Effizienz und Konsistenz in den Freigabeprozessen.
- **Cloud-basierte Lösungen:** Cloud-Technologien ermöglichen eine flexible und skalierbare Implementierung von IKS-Lösungen. Sie bieten zudem die Möglichkeit, Daten sicher zu speichern und von überall darauf zuzugreifen.
- **Continuous Monitoring und Auditing:** Diese Ansätze ermöglichen die kontinuierliche Überwachung und Bewertung interner Kontrollen in Echtzeit oder nahezu Echtzeit. Der Schwerpunkt liegt auf Datenanalysen und der Nutzung automatischer Kontrollen. Der Vorteil besteht darin, dass die gesamte Population von Geschäftstransaktionen analysiert werden kann, Ausreisser leicht identifiziert und monetär bewertet werden können und manuelle Kontrollaktivitäten reduziert werden. Darüber hinaus bieten diese Ansätze die Möglichkeit zur kontinuierlichen Verbesserung (Continuous Improvement) von Unternehmensabläufen.

[10] Gemäss OR 727a Ziff. 2 kann mit der Zustimmung sämtlicher Aktionäre auf die eingeschränkte Revision verzichtet werden, wenn die Gesellschaft nicht mehr als zehn Vollzeitstellen im Jahresdurchschnitt hat.

- **Datenanalyse mittels Large Language Models (LLMs):** Datenanalyse-Tools in Verbindung mit Large Language Models (LLMs) wie GPT-4 von OpenAI, PaLM2 von Google oder Llama 2 von Meta bieten leistungsstarke Möglichkeiten zur Verarbeitung und Analyse grosser Datenmengen.
- **Process Mining:** Process-Mining-Tools helfen dabei, Geschäftsprozesse auf Datenbasis End-to-End zu visualisieren. Sie ermöglichen die effiziente und effektive Identifikation von Geschäftsprozessrisiken, wie beispielsweise Prozessunterbrechungen oder nicht erlaubten Prozessaktivitäten (Non-Compliance).

Diese und viele weitere Tools unterstützen die Prozesse und Arbeitsabläufe in Unternehmen und tragen dabei zu mehr Effizienz bei, indem sie Schnelligkeit erhöhen und Fehleranfälligkeit reduzieren. Die Automatisierung von Prozessen setzt jedoch voraus, dass diese zunächst überdacht und so effektiv wie möglich gestaltet werden.

Erst dann macht eine Digitalisierung überhaupt Sinn. Digitalisierung bedeutet auch, dass sich das Unternehmen für eine Investition entscheidet. Daher eignen sich vor allem repetitive Prozesse für die Überführung in einen digitalen Prozess. Das heisst, es ist im Voraus eine stringente Standardisierung vorzunehmen, was von den Markteinheiten in der Regel weniger gern gesehen wird. Diese gehen lieber sehr individuell auf die Wünsche ihrer Kunden ein. Diese unterschiedlichen Haltungen führen nicht selten zu grossen Diskussionen in Unternehmen.

Studiendesign und Untersuchungsgruppe

Die Methodik der vorliegenden Studie basiert auf einer Kombination aus quantitativen und qualitativen Befragungen. Als Resultat der standardisierten Umfrage konnten Antworten von insgesamt 278 Unternehmen – vom Kleinbetrieb bis zum Grossunternehmen – ausgewertet werden. Zudem wurden sechs Interviews mit Fachexpertinnen und -experten geführt.

Methodik

Die Fragestellung dieser Studie wurde mittels quantitativer und qualitativer Befragungen bearbeitet. Die quantitative Befragung erfolgte im Juni 2024 in schriftlicher Form anhand eines sowohl digitalen als auch physischen Fragebogens, der in Deutsch und Französisch schweizweit verschickt wurde. Insgesamt wurden beantwortete Fragebögen von 278 in der Schweiz domizilierten Unternehmen ausgewertet.

Neben dieser Umfrage haben die Autorinnen und Autoren mit verschiedenen Fachexpertinnen und -experten, welche in ihrer täglichen Arbeit aus verschiedenen Gründen mit den Themen aus dem Risikomanagement und der internen Kontrollen konfrontiert sind, Interviews geführt. Dies waren nebst Anwendern auch Beraterinnen und Berater im Bereich des Risikomanagements und der internen Kontrollen sowie Expertinnen und Experten aus der Forschung (Interviewpartnerinnen und -partner siehe Seite 58). Aussagen aus diesen Gesprächen finden sich sinngemäss im Text integriert. Die Autorenschaft bedankt sich auch an der Stelle bei allen, die mit ihrer Teilnahme an den Interviews zur empirischen Abstützung dieser Studie beigetragen haben.

Untersuchungsgruppe

Insgesamt wurden Fragebögen aus 28 verschiedenen Branchen ausgewertet, wobei die meisten der befragten Unternehmen in den Bereichen «Maschinenbau und Herstellung von Metallerzeugnissen» (19%), «Baugewerbe, Bau» (17%) und «Gross- und Detailhandel» (8%) tätig sind. Die befragten Unternehmen tragen hinsichtlich Rechtskleid mehrheitlich die Form der Aktiengesellschaft (92%).

Bezüglich der Anzahl Mitarbeitenden sind Unternehmen mit 50 bis 99 Mitarbeitenden (40%) und solche mit 100 bis 250 Mitarbeitenden (28%) am stärksten vertreten (siehe Abbildung 3).

Gemessen am Umsatz sind überwiegend Unternehmen mit einem jährlichen Umsatz bis CHF 100 Mio. vertreten (siehe Abbildung 4).

Dabei sind die befragten Unternehmen mehrheitlich national ausgerichtet: rund 60% sind fast ausschliesslich in der Schweiz tätig, nur 20% erzielen mehr als die Hälfte ihres Umsatzes im Ausland. Nur ausnahmsweise (in 6% der Fälle) handelt es sich um börsenkotierte Unternehmen.

Abbildung 3: Verteilung der Unternehmen nach Anzahl Mitarbeitenden (n=278)

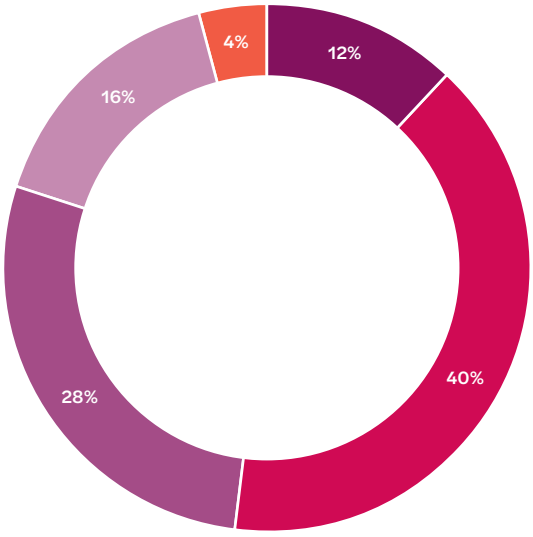
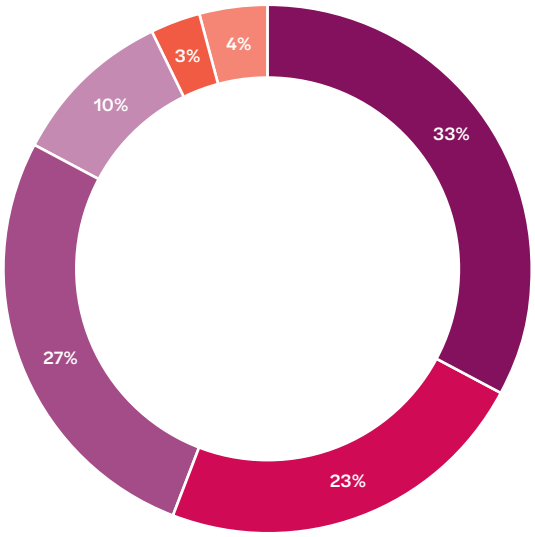


Abbildung 4: Verteilung der Unternehmen nach Umsatz in CHF Mio. (n=278)



Ergebnisse der Umfrage
Allgemeine Fragen zu Risiko und internen Kontrollen

Die Umfrageergebnisse lassen den Schluss zu, dass Risikomanagement und interne Kontrollen bei den Befragten einen hohen Stellenwert geniessen. Ein umfassendes Organisationskonzept, welches auch eine interne Revision oder eine vergleichbare Stelle umfasst, findet sich wenig überraschend vor allem bei grösseren Unternehmen.

Während die **Koordination und Überwachung des Risikomanagements** bei den befragten Unternehmen in erster Linie bei der Gesamtgeschäftsleitung (34%) oder bei dem Gesamtverwaltungsrat (31%) angesiedelt ist (siehe Abbildung 5), wurde bezüglich **Koordination und Überwachung des internen Kontrollsytems** mehrheitlich die finanzielle Leitung/CFO (33%) vor wiederum der gesamten Geschäftsleitung (28%) genannt und der Verwaltungsrat wurde mit 10% deutlich seltener angegeben (siehe Abbildung 6). Das Risikomanagement scheint im Vergleich zum internen Kontrollsystem demnach stärker von der strategischen Unternehmensführung getrieben zu werden, während die internen Kontrollen vergleichsweise häufiger von operativen Funktionen wie insbesondere der finanziellen Leitung koordiniert und überwacht werden.

Vor dem Hintergrund der gesetzlichen Vorschriften in der Schweiz, die dem Verwaltungsrat die Verantwortung für das Aufsetzen eines Risikomanagementsystems sowie die Möglichkeit der Delegation an die Geschäftsleitung zur Umsetzung und Überwachung übertragen, sind die Ergebnisse sehr stimmig.

In jeweils gegen der Hälfte der Fälle bestehen bei den befragten Unternehmen bezüglich Unterhalt des internen Kontrollsystems (49%), des Risikomanagements/Enterprise Risk Management und der Prüfung des internen Kontrollsystems (jeweils 45%) **dedizierte Stellen.** Nur in Ausnahmefällen handelt es sich hierbei jedoch um eine klar definierte und spezifisch zugewiesene Position, die diesen Aufgaben gewidmet ist – vielmehr sind die Tätigkeiten im Zusammenhang mit dem Risikomanagement und dem internen Kontrollsystem häufig im Stellenbeschrieb einer breiten gefassten Funktion (zum Beispiel CEO, CFO, COO oder Qualitätsmanagement) integriert.

Abbildung 5: Wer ist in Ihrem Unternehmen in erster Linie zuständig für die Koordination und die Überwachung des Risikomanagements? (n=278)

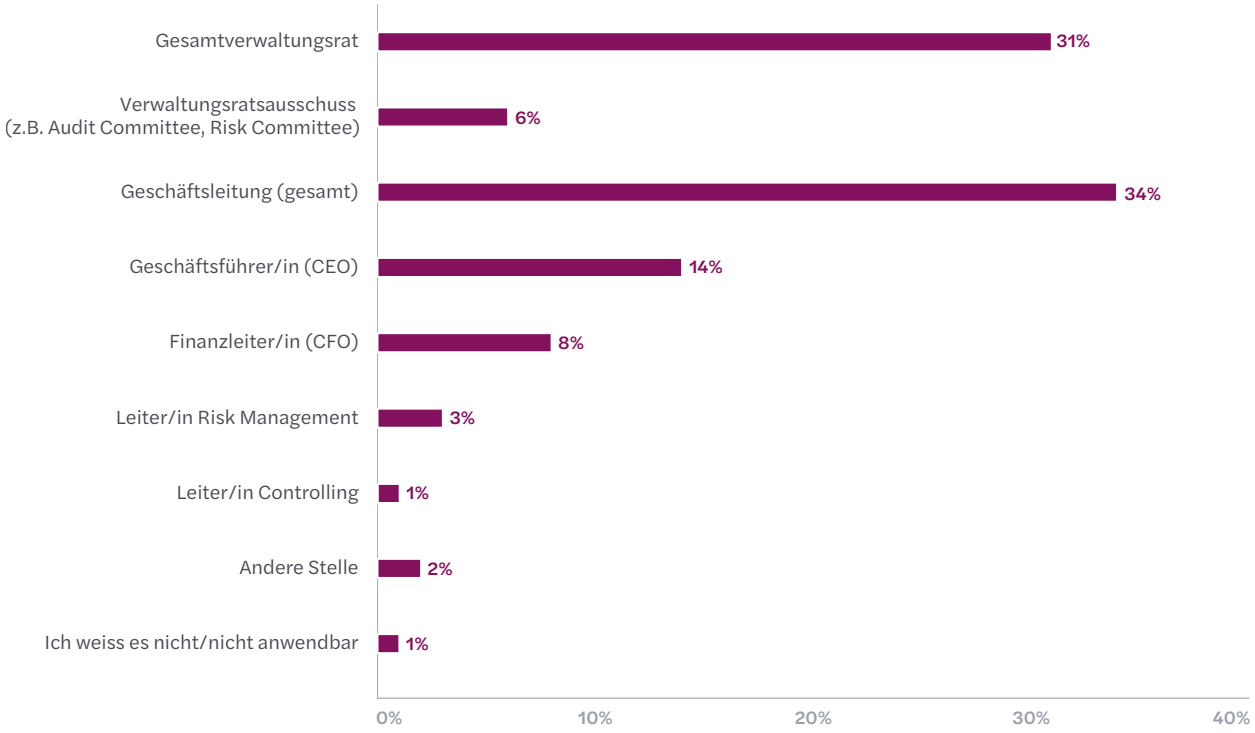
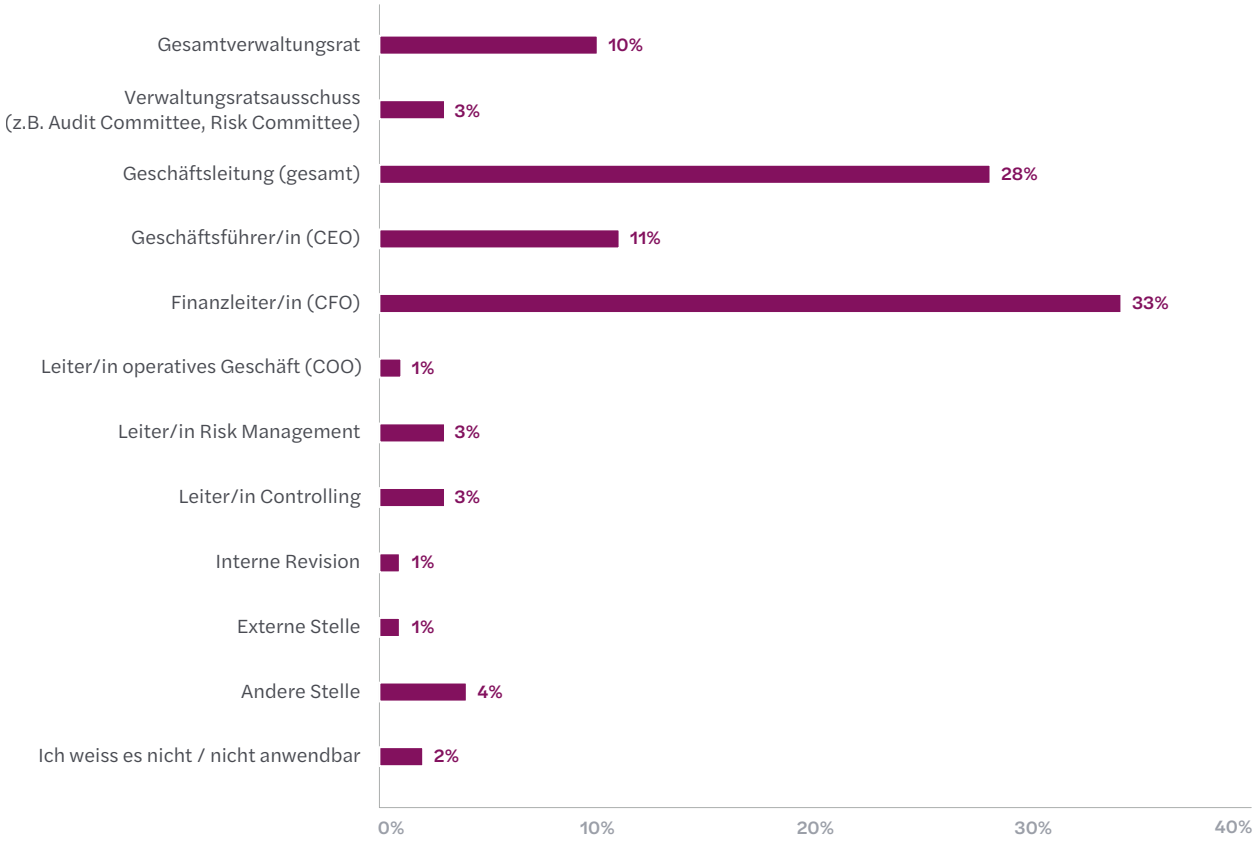


Abbildung 6: Wer ist in Ihrem Unternehmen in erster Linie zuständig für die Koordination und die Überwachung des internen Kontrollsystems? (n=278)



49% der befragten Unternehmen geben an, dass ihr **internes Kontrollsystem (IKS) Bestandteil des unternehmensweiten Risikomanagements** ist (siehe Abbildung 7). Bei weiteren 25% erfolgt zumindest eine regelmässige Abstimmung zwischen dem internen Kontrollsystem und dem Risikomanagement. Bei den Unternehmen, die das interne Kontrollsystem nicht in das Risikomanagement integriert haben und bei denen auch keine regelmässige Abstimmung zwischen den zwei Bereichen erfolgt, handelt es sich fast ausschliesslich um solche mit weniger als 100 Mitarbeitenden.

Während bei fast der Hälfte der befragten Unternehmen das **«Three Lines of Defense»-Modell**[11] nicht bekannt (26%) oder eine Umsetzung bisher kein Thema ist (22%), haben 24% das Modell vollständig mit allen drei Verteidigungslinien umgesetzt (siehe Abbildung 8). Bei rund 20% der Unternehmen ist die erste und zweite Verteidigungslinie umgesetzt, es besteht jedoch keine interne Revision oder eine andere vergleichbare Stelle. Weitere 8% geben an, dass bei ihnen die erste Linie im Rahmen ihrer operativen Aufgaben ein risikobewusstes Vorgehen pflegt und es eine zweite und dritte Linie bei ihnen nicht braucht.

Werden die Antworten auf diese Frage nach Unternehmensgrösse aufgeschlüsselt, zeigt sich nicht ganz unerwartet, dass grössere Unternehmen das «Three Lines of Defense»-Modell eher kennen und umsetzen als kleinere Unternehmen (siehe Abbildung 9).

Folgendes lässt sich aus den Antworten ableiten:

- Während bei den Unternehmen mit mehr als 1'000 Mitarbeitenden bei über 90% alle drei Verteidigungslinien (d.h. einschliesslich einer internen Revision oder einer vergleichbaren Stelle) umgesetzt sind, sind es bei den Unternehmen mit weniger als 50 Mitarbeitenden noch 12%. Dass aber selbst kleine Unternehmen damit auch eine interne Revision oder eine vergleichbare Stelle unterhalten, erscheint doch eher überraschend, mag aber mit der im Theorieteil erwähnten Komplexität eines Geschäftsmodells bzw. der Integration der Lieferkette in eine regulierte Branche zu tun haben.
- Kleinere Unternehmen sind deutlich häufiger der Ansicht, dass die erste Verteidigungslinie genug Risikobewusstsein pflegt und es weder eine zweite noch eine dritte Linie braucht.
- Je kleiner das Unternehmen, desto häufiger ist das «Three Lines of Defense»-Modell nicht bekannt – so geben 43% der Unternehmen mit weniger als 50 Mitarbeitenden an, dass ihnen das Modell in dieser Form nicht bekannt ist.
- Nur die wenigsten der befragten Unternehmen (2%) haben bewusst auf eine Einführung des Modells verzichtet.

[11] siehe Seiten 12/13 für weitere Ausführungen zum «Three Lines of Defense»-Modell

Abbildung 7: Ist bei Ihrem Unternehmen das interne Kontrollsystem (IKS) ausdrücklich in das Risikomanagement integriert? (n=278)

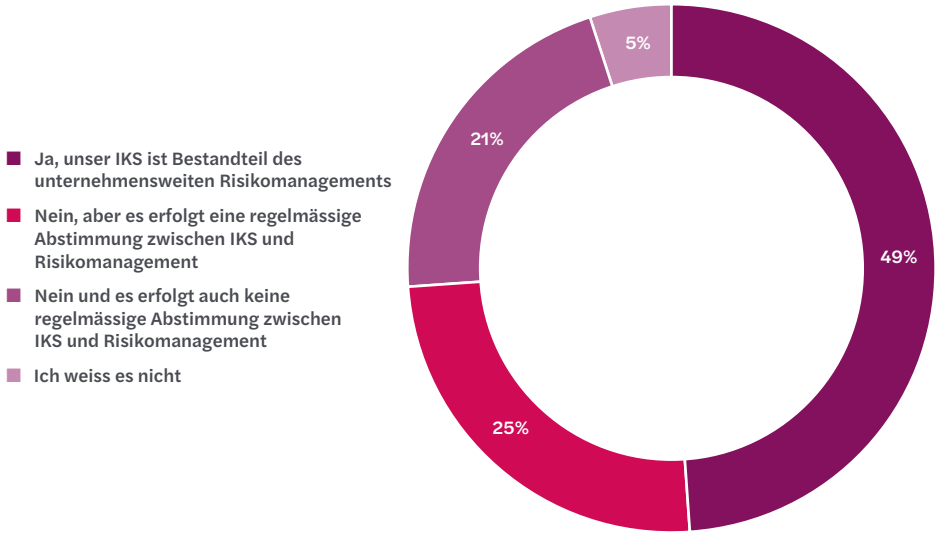


Abbildung 8: Inwieweit wurde in Ihrem Unternehmen das «Three-Lines-of-Defense»-Modell (Drei-Verteidigungslinien-Konzept) umgesetzt? (n=278)

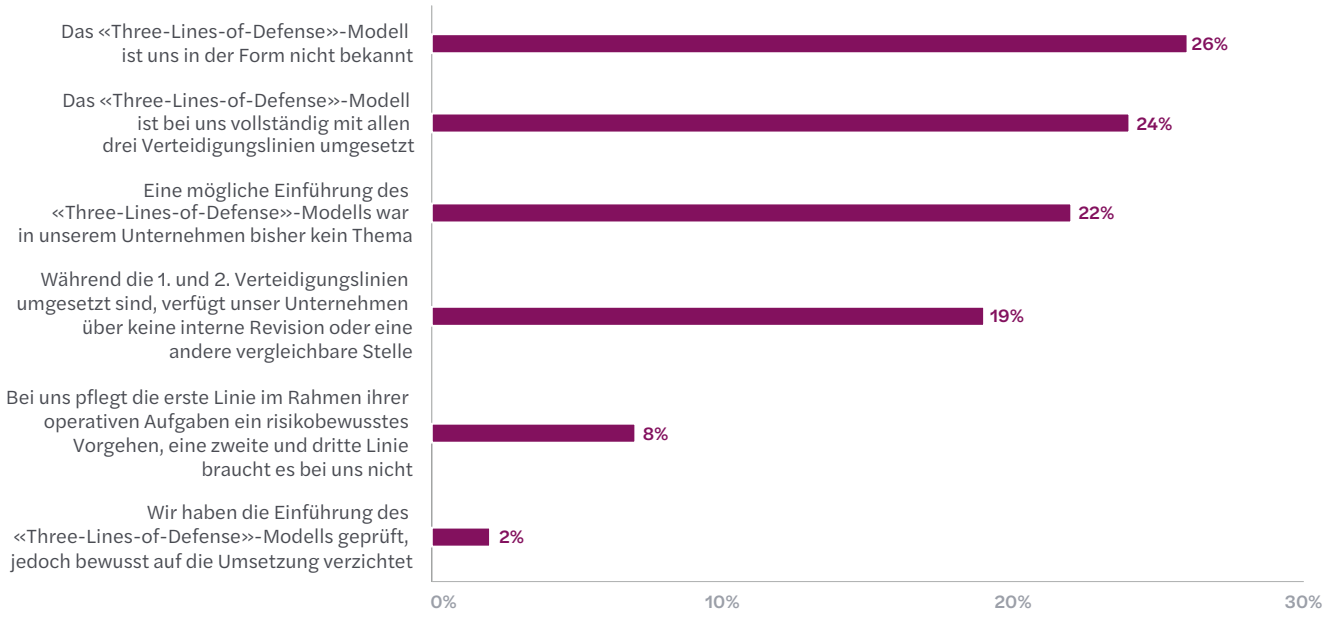
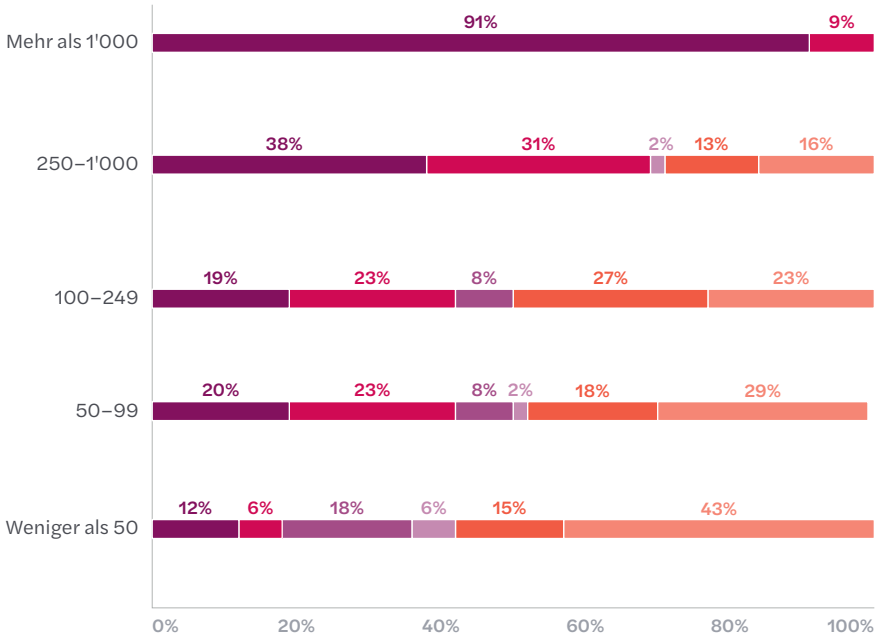


Abbildung 9: Inwieweit wurde in Ihrem Unternehmen das «Three-Lines-of-Defense»-Modell (Drei-Verteidigungslinien-Konzept) umgesetzt (nach Anzahl Mitarbeitende)? (n=278)



- Das «Three-Lines-of-Defense»-Modell ist bei uns vollständig mit allen drei Verteidigungslinien umgesetzt
- Während die 1. und 2. Verteidigungslinien umgesetzt sind, verfügt unser Unternehmen über keine interne Revision oder eine andere vergleichbare Stelle
- Bei uns pflegt die erste Linie im Rahmen ihrer operativen Aufgaben ein risikobewusstes Vorgehen, eine zweite und dritte Linie braucht es bei uns nicht
- Wir haben die Einführung des «Three-Lines-of-Defense»-Modells geprüft, jedoch bewusst auf die Umsetzung verzichtet
- Eine mögliche Einführung des «Three-Lines-of-Defense»-Modells war in unserem Unternehmen bisher kein Thema
- Das «Three-Lines-of-Defense»-Modell ist uns in der Form nicht bekannt

Risikomanagement

Die Umfrageergebnisse zeigen, dass formalisierte unternehmensweite Risikomanagementprozesse vor allem in Unternehmen mit mehr als 100 Mitarbeitenden etabliert sind. Als wichtigste Gründe für das Implementieren eines Risikomanagementsystems werden von den befragten Unternehmen die Früherkennung und die verbesserte Kontrolle von Risiken, die Sicherung des Fortbestandes der Unternehmung und die Erkennung und Abwägung von Chancen und Risiken gesehen. Auf der kritischen Seite werden (zu) formalisierte Risikomanagementprozesse mit übermässiger Bürokratie und einer zu hohen Bindung personeller Ressourcen in Verbindung gebracht. Hinsichtlich der Risikoarten stehen IT-Sicherheit und Cyberrisiken im Fokus.

Fast 60% der befragten Unternehmen geben an, dass in ihrem Unternehmen ein formalisierter unternehmensweiter **Risikomanagementprozess** zur Risikoidentifikation, -bewertung, -steuerung und -überwachung existiert (siehe Abbildung 10). Bei weiteren 11% besteht zumindest ein informeller Prozess. Während weitere 25% die Einführung eines formalisierten Risikomanagementprozesses planen, existiert bei nur 5% kein Risikomanagementprozess und es ist auch keine Einführung eines solchen Prozesses geplant.

Wenig überraschend sind formalisierte Risikomanagementprozesse vor allem bei Unternehmen ab einer Mitarbeitendenzahl von 100 etabliert, während Unternehmen mit weniger als 50 Mitarbeitenden häufiger keinen formalisierte Risikomanagementprozesse eingeführt haben und dies auch nicht planen (siehe Abbildung 11).

Von den 163 Unternehmen, die einen formalisierten Risikomanagementprozess unterhalten, wendet fast die Hälfte (47%) keine spezifische **Methode für das Risikomanagement** an. Kommt eine Methode für das Risikomanagement zur Anwendung, findet das COSO-Framework mit 36% den grössten Anklang. ISO 9001 und ISO 31000 wurden in jeweils rund 15% der Fälle genannt, während bei 16% eine eigene/interne Entwicklung zur Anwendung kommt.

Den wichtigsten **Grund für die Durchführung eines Risikomanagements** sehen 61% der befragten Unternehmen in der Früherkennung und verbesserten Kontrolle von Risiken, gefolgt von der Erfüllung regulatorischer oder gesetzlicher Anforderungen (50%), der Sicherung des Fortbestandes des Unternehmens (47%) und der Erkennung und Abwägung von Chancen und Risiken (45%). Kostenoptimierungen im Zusammenhang mit Risikomassnahmen (z.B. die Optimierung von Versicherungskosten) werden hingegen nur selten (10%) genannt (siehe Abbildung 12).

Abbildung 10: Existiert in Ihrem Unternehmen ein formalisierter unternehmensweiter Risikomanagementprozess? (n=278)

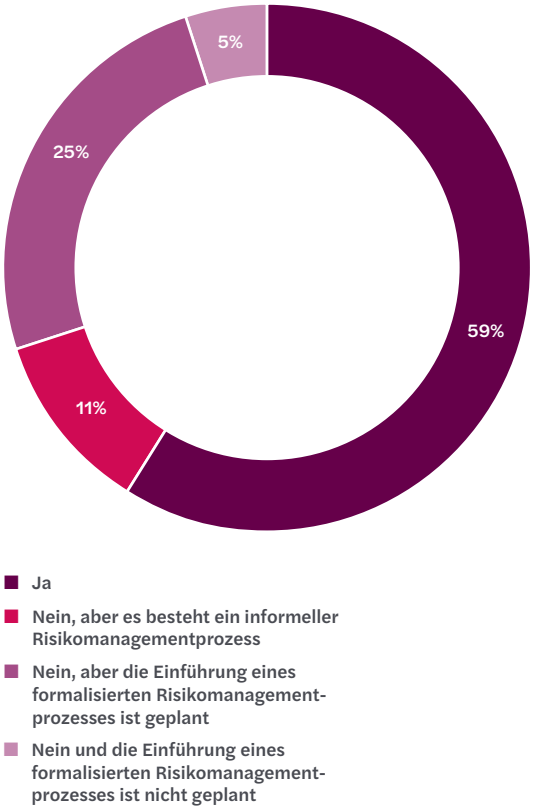
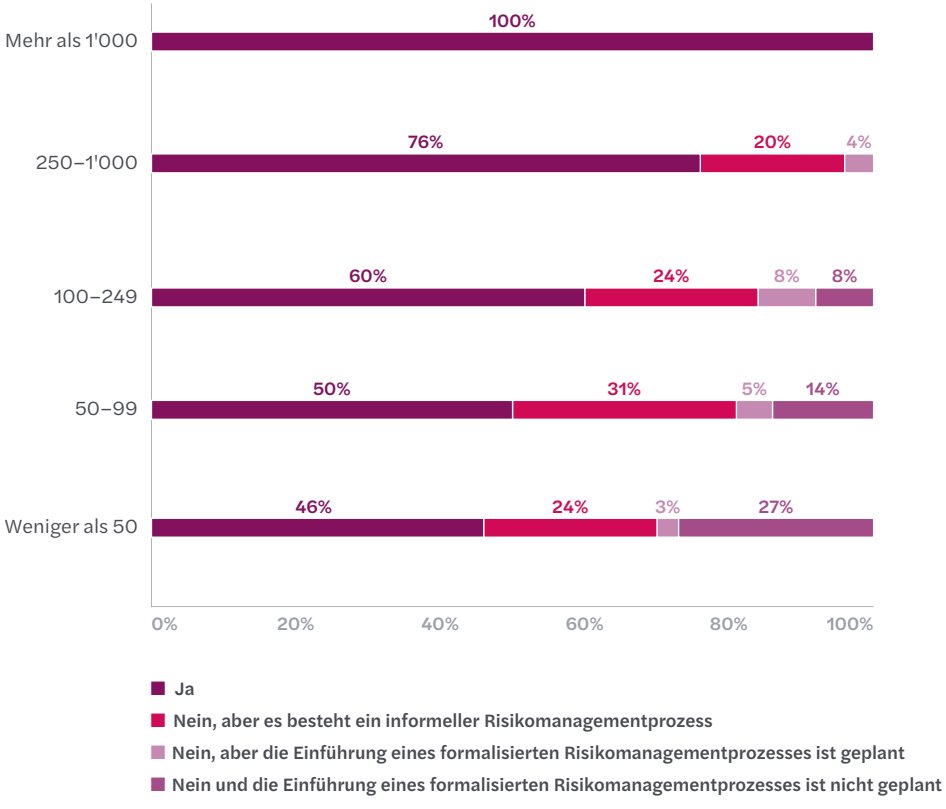


Abbildung 11: Existiert in Ihrem Unternehmen ein formalisierter unternehmensweiter Risikomanagementprozess (nach Anzahl Mitarbeitende)? (n=278)

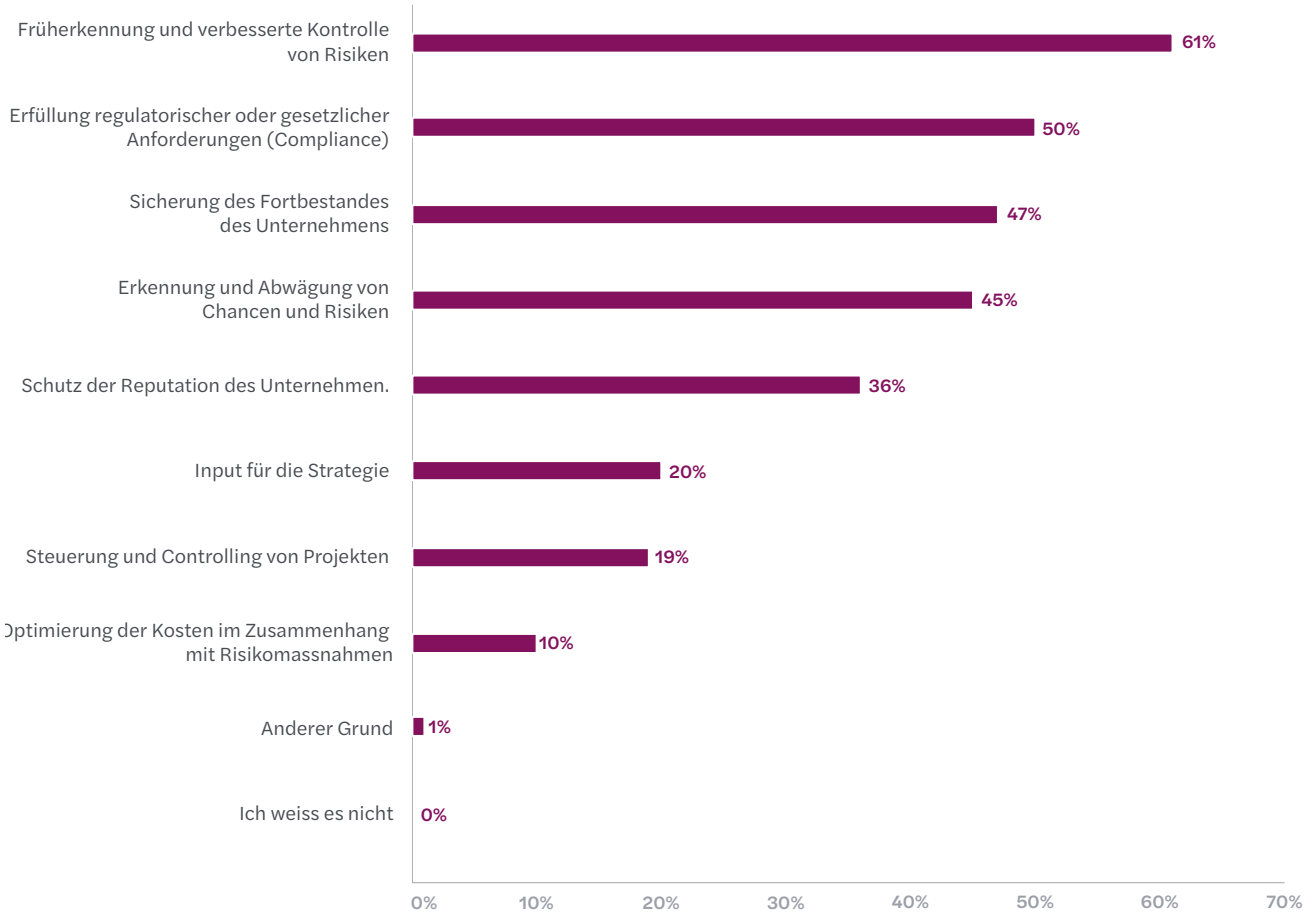


Diejenigen Unternehmen, die keinen formalisierten Risikomanagementprozess eingeführt haben, begründen dies mehrheitlich damit, dass ein zu formalisiertes Risikomanagement zu Überregulierung und übermässiger Bürokratie führt (37%) und dass die Implementierung eines Risikomanagementprozesses zu viele personelle Ressourcen erfordert (33%). 20% geben an, dass ein zu starkes Risikomanagement zu verzerrten Prioritäten führen kann, indem sich das Unternehmen auf unwichtige Risiken konzentriert und dabei wesentliche Aspekte übersieht. Demgegenüber stehen insbesondere finanzielle Aspekte (13%) weniger im Vordergrund (siehe Abbildung 13).

Bezüglich **Risikoarten, die regelmässig aktiv identifiziert, analysiert und überwacht** werden, stehen bei den Unternehmen, bei denen ein formalisierter Risikomanagementprozess existiert oder dessen Einführung geplant ist, vor allem operative Risiken (z.B. Ausfall eines Schlüssellieferanten, Cyber Security) und finanzielle Risiken (z.B. Liquiditäts-/Kreditrisiken) im Vordergrund – jeweils über 90% der befragten Unternehmen haben diese Risikoarten genannt (siehe Abbildung 14).

Strategische Risiken (z.B. veränderte Marktbedingungen und Kundenbedürfnisse, neue Technologie und Trends, neue Wettbewerber) und Compliance-Risiken (Nichteinhaltung von Gesetzen, Vorschriften und Regeln wie z.B. Steuergesetze, Umweltgesetze, Geldwäscherei, Datenschutz, Kartellrecht, Produktehaftung, ESG-Richtlinien) sind bei den befragten Unternehmen etwas weniger im Fokus, wurden aber jeweils ebenfalls häufig (von rund Dreiviertel der Befragten) genannt.

Abbildung 12: Aus welchen Gründen wird bei Ihrem Unternehmen ein Risikomanagement hauptsächlich durchgeführt? (n=233)



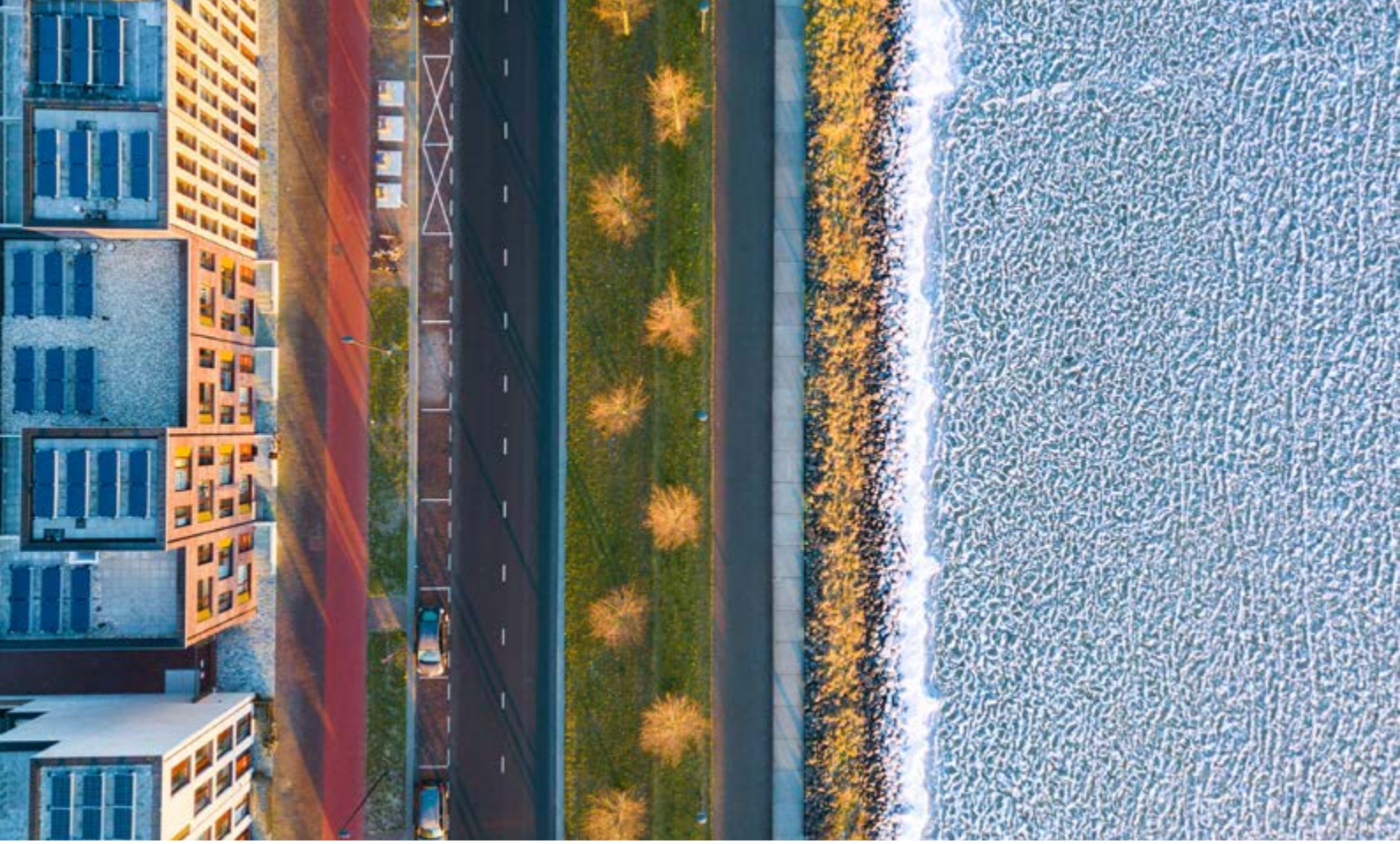
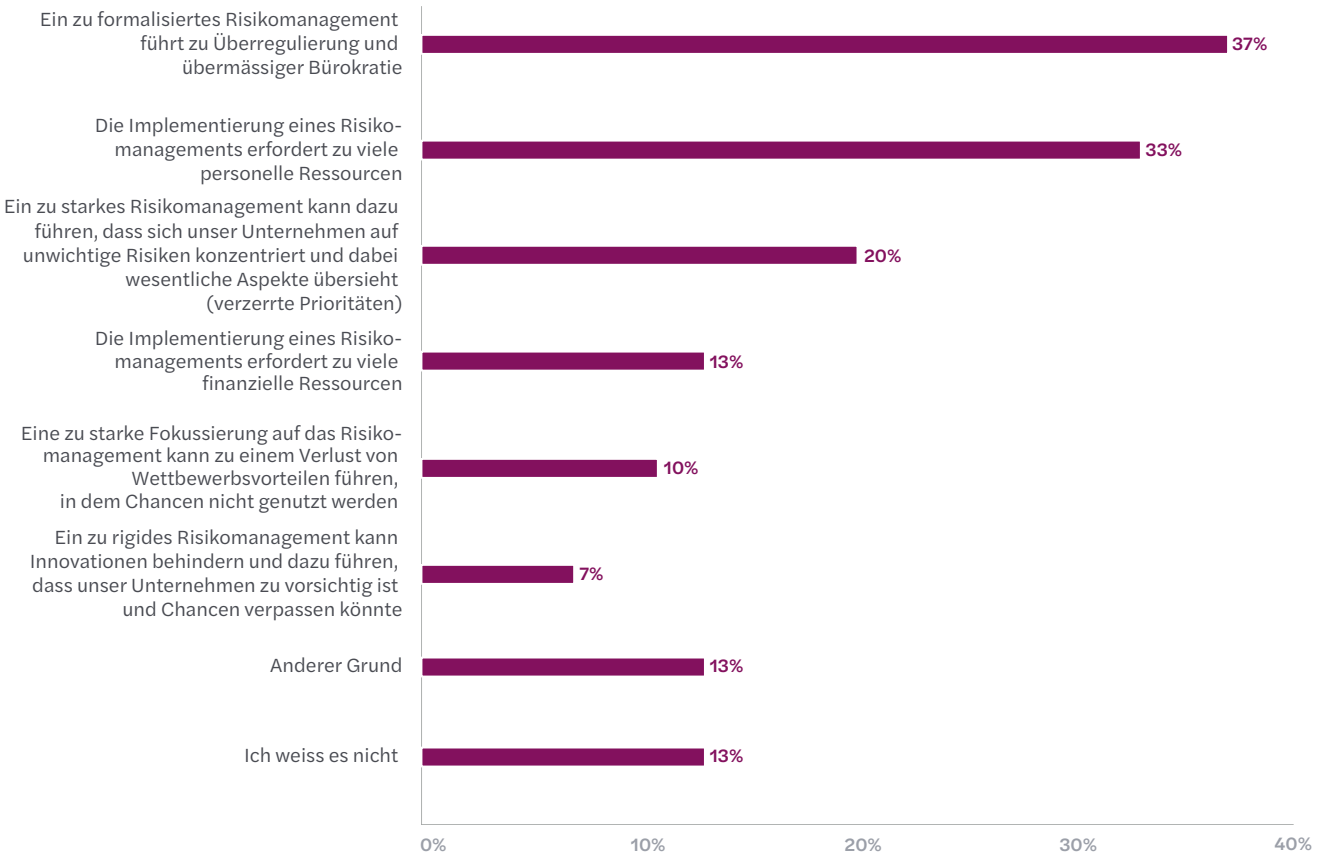


Abbildung 13: Aus welchen Gründen hat Ihr Unternehmen auf die Einführung eines formalisierten Risikomanagementprozesses verzichtet? (n=30)



Bei der Frage, in welcher **Regelmässigkeit** sich die Verantwortlichen der befragten Unternehmen mit gewissen Risiken befassen, zeigt sich, dass die IT-Sicherheit und Cyberrisiken im Vordergrund stehen: 33% der befragten Unternehmen geben an, sich mindestens monatlich mit diesem Thema auseinanderzusetzen, weitere 25% tun dies mindestens einmal pro Quartal und kaum ein Unternehmen (1%) beschäftigt sich nie damit. Weiter lässt sich feststellen, dass viele der in der Frage genannten Risiken wie Rechtsrisiken/Compliance, gesamtwirtschaftliche Entwicklungen (z.B. Inflation, Geldpolitik, Wirtschaftspolitik), Drittparteienrisiken (z.B. Lieferanten- oder Kundenabhängigkeit), Änderungen in Gesetzgebung und Regulierung, Marktentwicklung (z.B. verschärfter Wettbewerb, neue Marktteilnehmer, Fusionen und Übernahmen), Betriebsunterbrechung (inkl. Unterbrechung der Lieferkette), Reputationsrisiken, Fachkräftemangel und Datenschutz vorwiegend mindestens einmal jährlich adressiert werden. Demgegenüber befassen sich die Unternehmen mehrheitlich nur unregelmässig bzw. bei Bedarf oder im Anlassfall mit den Risiken bezüglich Naturkatastrophen (z.B. Sturm, Überschwemmung, extreme Wetterereignisse). Eher weniger im Fokus steht das Risiko der mangelnden systematischen Einbindung von Künstlicher Intelligenz (KI) in das Geschäftsmodell: Fast 30% der befragten Unternehmen befasst sich nie mit diesem Thema und für 14% ist es nicht relevant (siehe Abbildung 15).

Abbildung 14: Welche Arten von Risiken werden in Ihrem Unternehmen regelmässig aktiv identifiziert, analysiert und überwacht? (n=178)

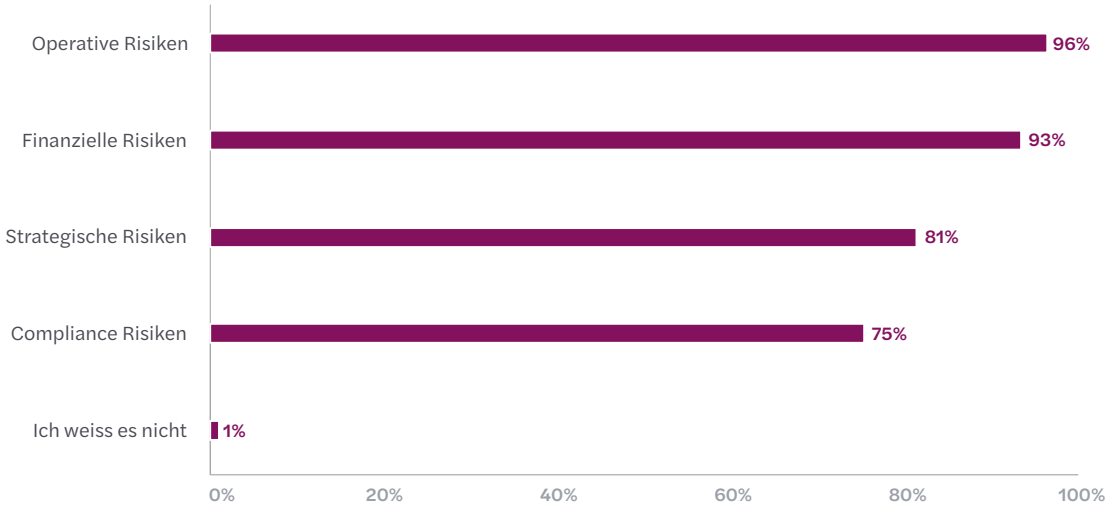
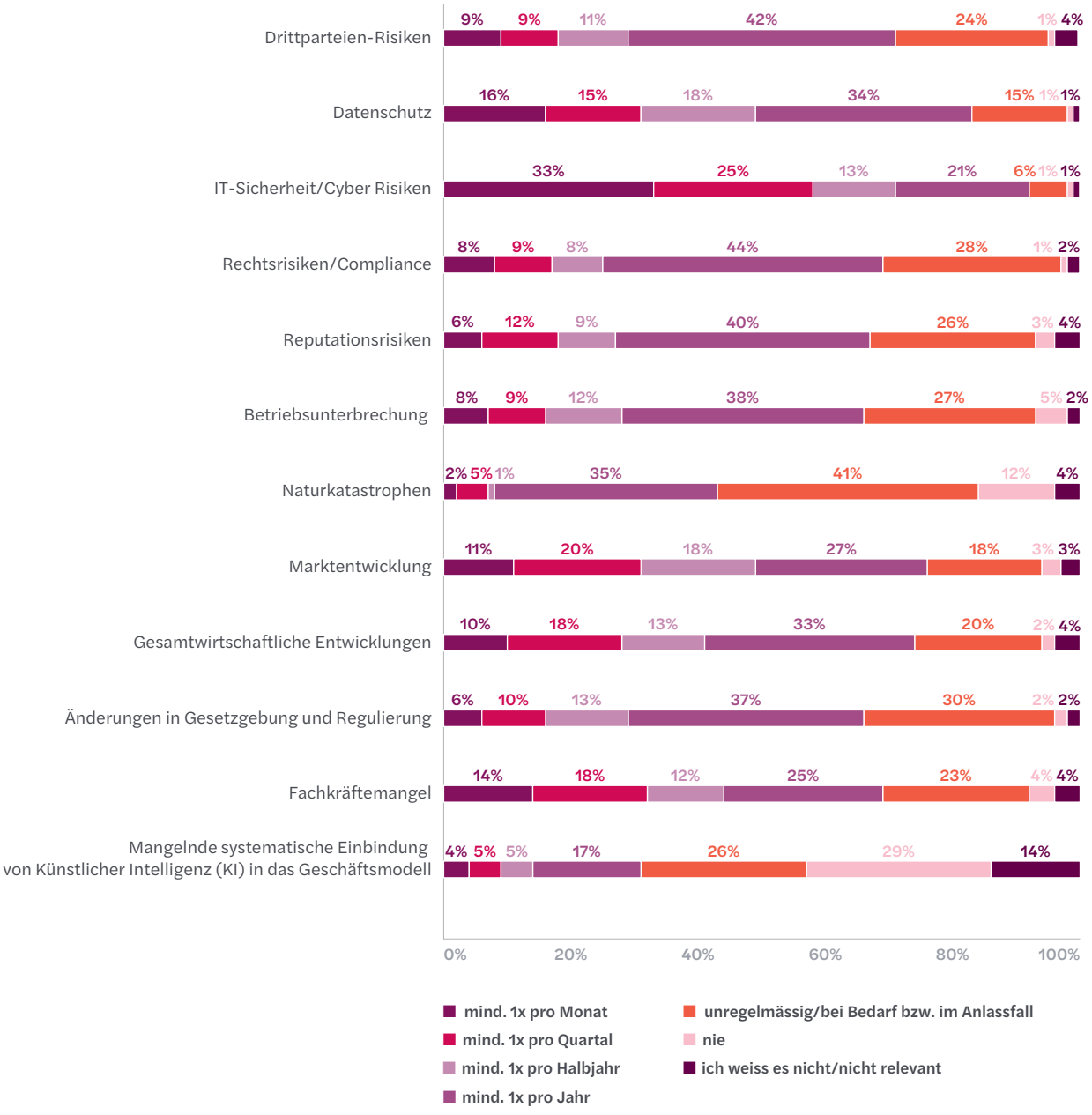


Abbildung 15: In welcher Regelmässigkeit befassen sich die Verantwortlichen in ihrem Unternehmen mit den folgenden Risiken? (n=278)



Internes Kontrollsystem

Die Ergebnisse der Umfrage bestätigen die Annahme, dass grössere Unternehmen tendenziell über ein aktuelles, formalisiertes und standardisiertes internes Kontrollsystem (IKS) verfügen. Während der Hauptnutzen eines IKS in erster Linie im Schutz des Geschäftsvermögens gesehen wird, werden Zeitdruck und Personalmangel als Hauptursache für Schwachstellen gesehen. Als grösste Herausforderungen werden die laufende Pflege des IKS sowie die Digitalisierung und Automatisierung genannt.

Mit 54% hat eine knappe Mehrheit der befragten Unternehmen angegeben, dass sie über ein **aktuelles formalisiertes und standardisiertes internes Kontrollsystem (IKS)** verfügt. Bei weiteren 18% existiert ein formalisiertes und standardisiertes IKS, welches nicht (mehr) aktuell ist und dessen Überarbeitung (z.B. Anpassungen, Automatisierungen) geplant ist. 8% geben an, dass zwar zur Zeit kein formalisiertes und standardisiertes IKS vorliegt, aber die Einführung geplant ist. Bei 19% ist kein IKS vorhanden und eine Einführung ist auch nicht geplant (siehe Abbildung 16).

Wird die Beantwortung dieser Frage nach Unternehmensgrösse (gemessen an der Anzahl der Mitarbeitenden) aufgeschlüsselt, zeigt sich, dass grössere Unternehmen tendenziell eher über ein aktuelles, formalisiertes und standardisiertes internes Kontrollsystem (IKS) verfügen (siehe Abbildung 17). Dieses Muster deutet darauf hin, dass die Implementierung eines formalisierten und standardisierten IKS mit der Unternehmensgrösse korreliert.

Als **Hauptnutzen oder Mehrwert eines internen Kontrollsystems** werden von den befragten Unternehmen mehrheitlich der Schutz des Geschäftsvermögens vor Verlust, Missbrauch und Schaden (45%), die Sicherung der ordnungsgemässen und effizienten Geschäftsführung (43%) und die Identifikation von finanziellen Risiken und deren Überwachung (41%) genannt (siehe Abbildung 18). Weniger oder kaum im Fokus stehen die zeitgerechte Erstellung verlässlicher Finanzinformationen (12%), die Erfüllung von Rechenschaftspflichten (10%) und die Durchsetzung von Honorarkürzungen für die Prüfung der Jahresrechnung (1%).

Als **Hauptgründe für Schwachstellen in den internen Kontrollen** sehen die befragten Unternehmen insbesondere den Zeitdruck und den Personalmangel (in 69% der Antworten genannt) und, etwas weniger ausgeprägt, mangelndes Kontrollbewusstsein (42%) sowie die mangelnde organisatorische Verankerung der internen Kontrollen (40%) (siehe Abbildung 19).

Abbildung 16: Verfügt Ihr Unternehmen über ein formalisiertes und standardisiertes internes Kontrollsystem (IKS)? (n=278)

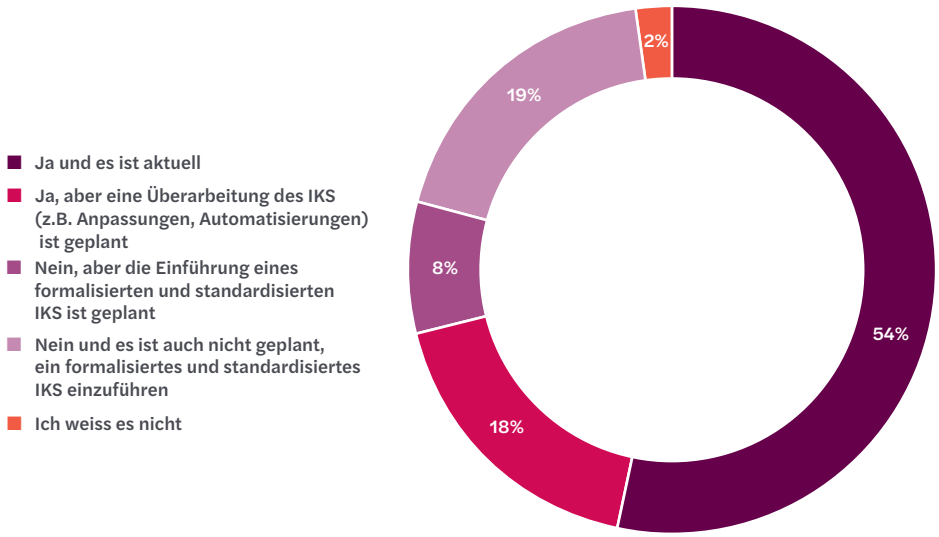


Abbildung 17: Verfügt Ihr Unternehmen über ein formalisiertes und standardisiertes internes Kontrollsystem (IKS) (nach Anzahl Mitarbeitende)? (n=278)

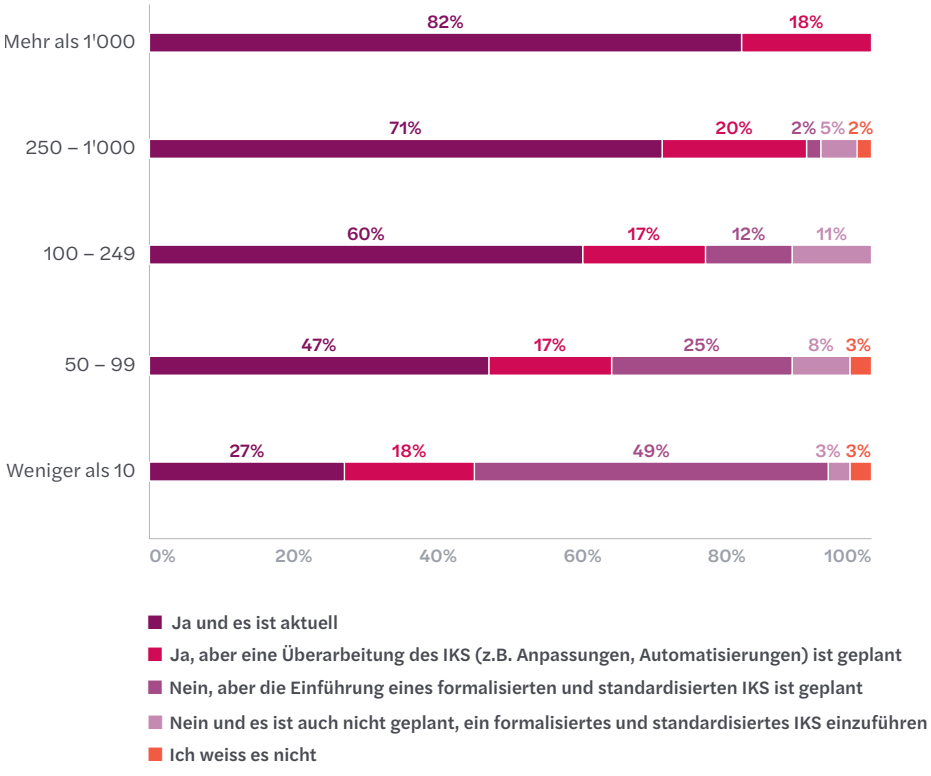


Abbildung 18: Welches sind aus Ihrer Sicht die wichtigsten Ziele eines internen Kontrollsystems bzw. worin liegt der Hauptnutzen/Mehrwert eines internen Kontrollsystems? (n=278)

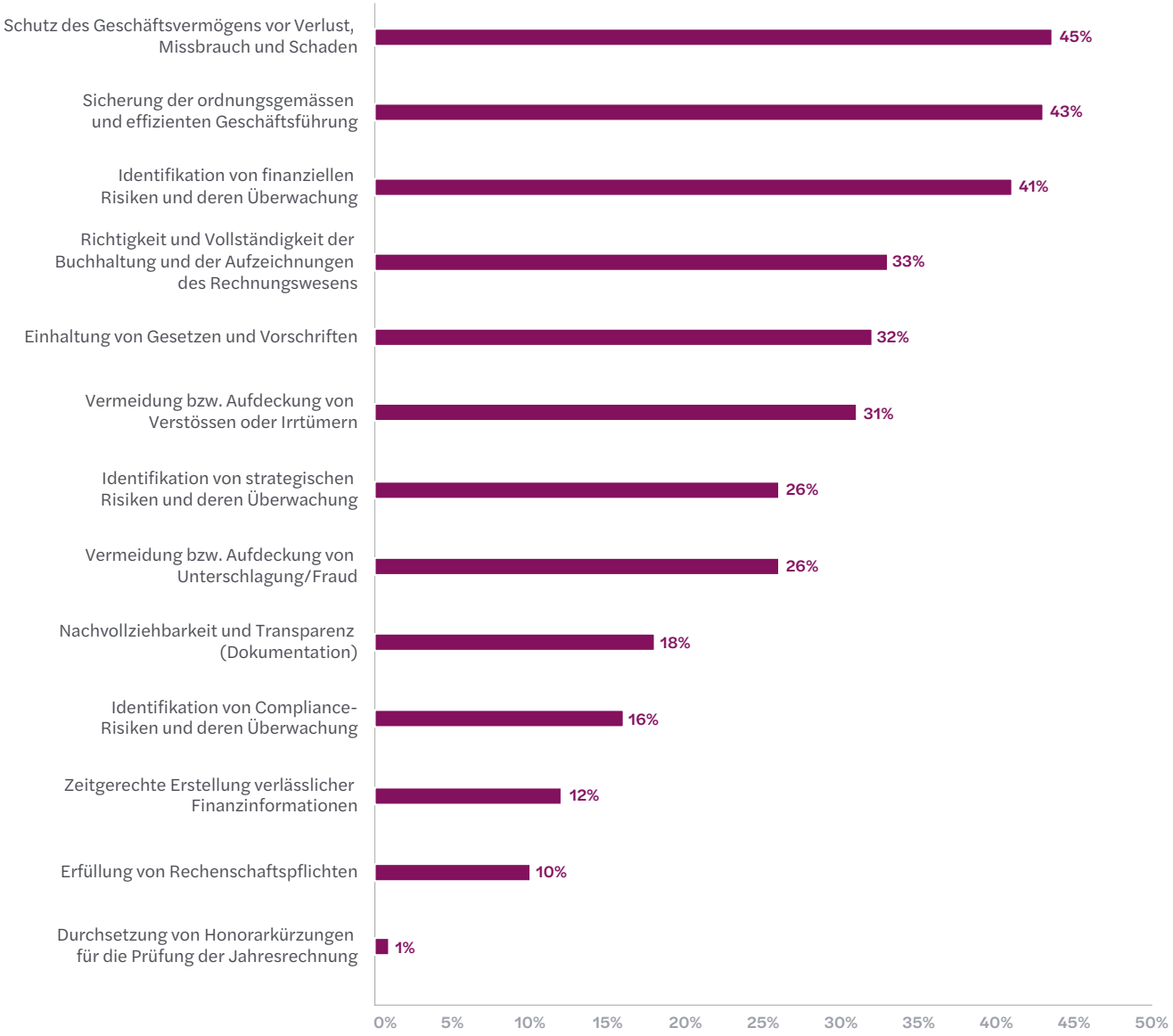
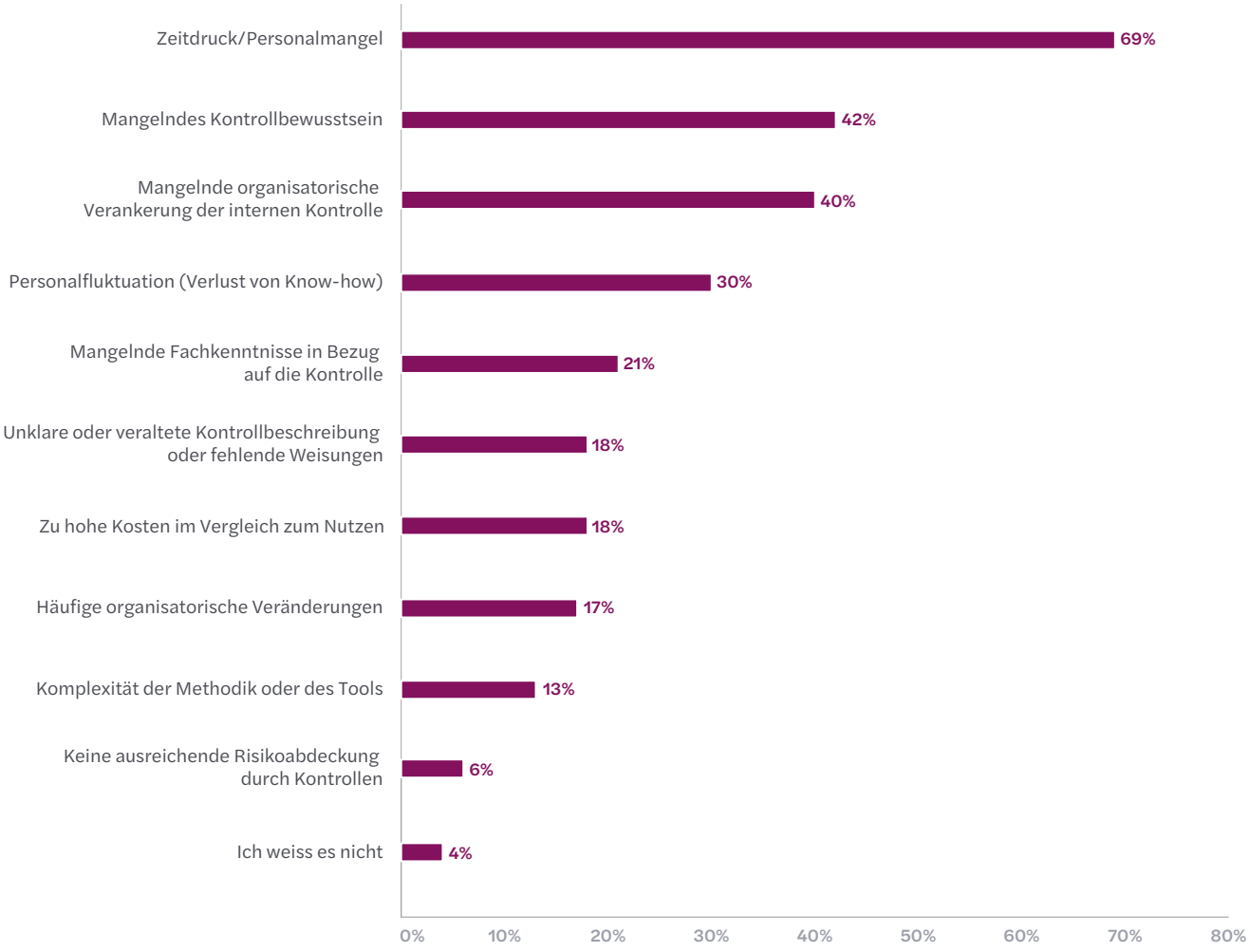


Abbildung 19: Welches sind aus Ihrer Sicht die Hauptgründe für Schwachstellen in den internen Kontrollen? (n=278)



Bezüglich **Kontrollarten** hat die Funktionstrennung für die Mehrheit der befragten Unternehmen, die über ein formalisiertes und standardisiertes Kontrollsystem verfügen, die grösste Bedeutung – der organisatorischen Trennung unvereinbarer Tätigkeiten (Vermeidung von Selbstkontrollen, z.B. durch das «Vier-Augen-Prinzip») wird in 86% der Antworten eine hohe oder eher hohe Bedeutung zugemessen und der systemseitigen Trennung (z.B. über das Berechtigungskonzept) 70% (siehe Abbildung 20). Als ebenfalls bedeutend werden unternehmensweite Kontrollen eingeschätzt (67% hohe oder eher hohe Bedeutung). Manuellen Kontrollen wird eine höhere Bedeutung zugemessen als den automatischen Kontrollen (79% gegenüber 52% hohe oder eher hohe Bedeutung). Eine etwas tiefere Bedeutung hat die systematische Datenanalyse – lediglich in 38% der Antworten wurde dieser Kontrollart eine hohe oder eher hohe Bedeutung attestiert.

Wird bei der Frage zu den Kontrollarten die Unternehmensgrösse (gemessen an der Anzahl Mitarbeitenden) herangezogen, so zeigt sich, dass mit zunehmender Unternehmensgrösse vor allem die Bedeutung von automatischen Kontrollen und – noch ausgeprägter – von der systemseitigen Funktionstrennung zunimmt (siehe Abbildungen 21 und 22). Deutlich weniger ausgeprägt zeigt sich diese Tendenz bezüglich der organisatorischen Trennung, der systematischen Datenanalyse und der unternehmensweiten Kontrollen. Umgekehrt lässt sich bezüglich der Bedeutung der manuellen Kontrollen feststellen, dass diese bei Unternehmen mit mehr als 1'000 Mitarbeitenden eine im Vergleich zu kleineren Unternehmen tiefere Bedeutung haben – aber selbst bei 64% dieser Unternehmen haben manuelle Kontrollen eine hohe oder eher hohe Bedeutung (siehe Abbildung 23).

Abbildung 20: Auf welchen Kontrollarten basiert das in Ihrem Unternehmen aktuell angewandte interne Kontrollsystem (IKS) und welche Bedeutung hat die jeweilige Kontrollart in Bezug auf Schlüsselrisiken sowie Anteil an der Gesamtheit der Kontrollen? (n=200)

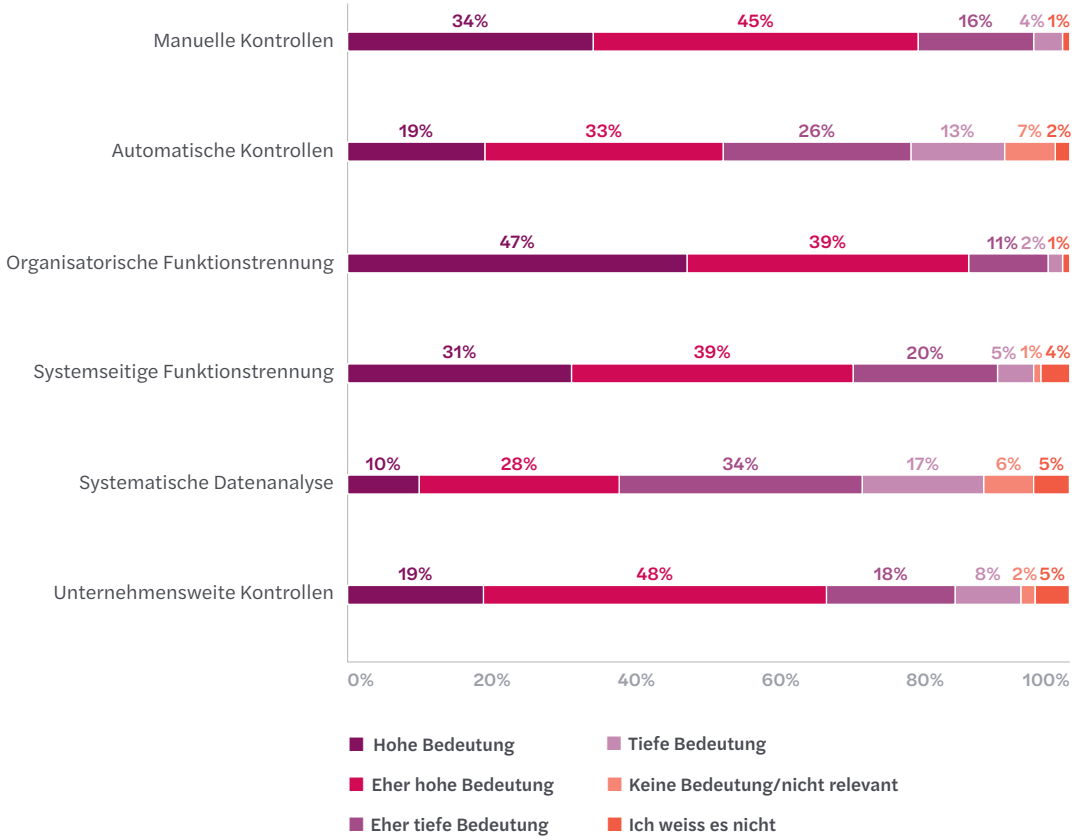


Abbildung 21: Bedeutung der automatischen Kontrollen nach Anzahl Mitarbeitende (n=200)

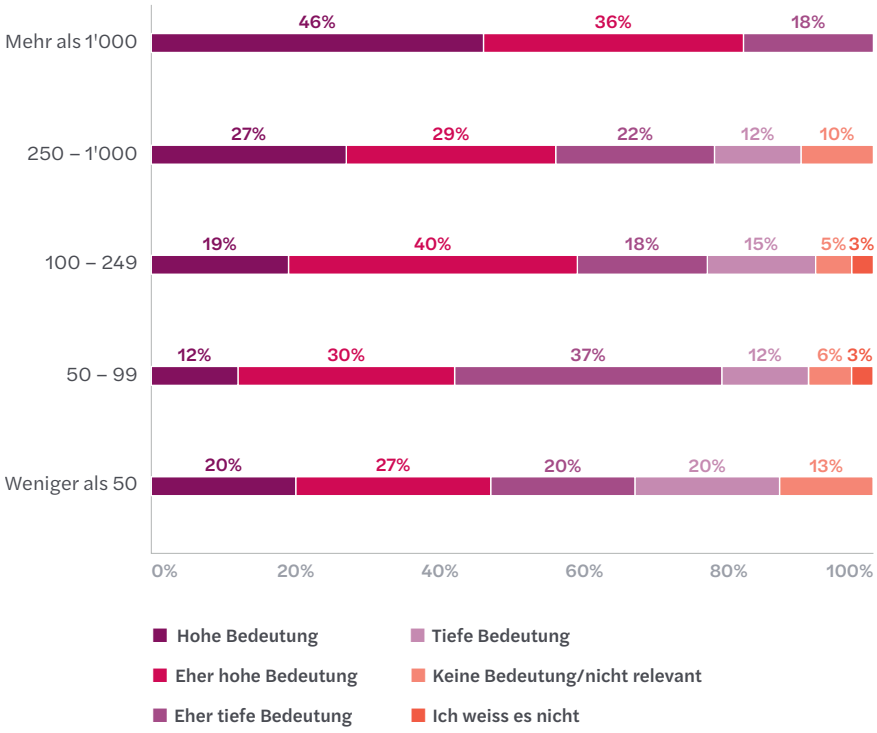
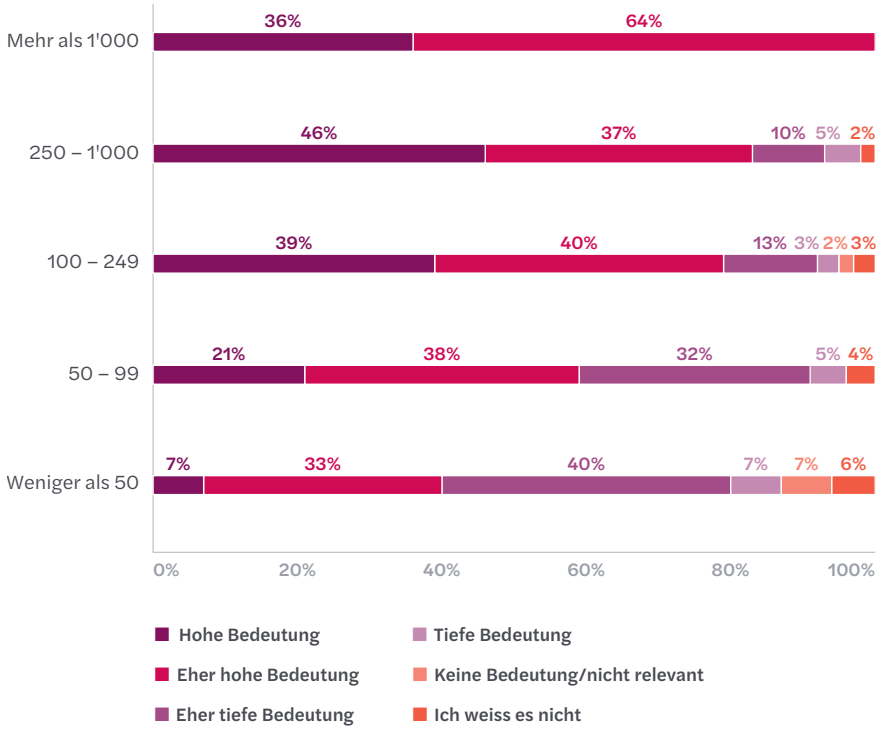


Abbildung 22: Bedeutung der systemseitigen Funktionstrennung nach Anzahl Mitarbeitende (n=200)



Wenn es um den Reifegrad der **Implementierung automatischer Kontrollen** geht, lässt sich aufgrund der Umfrageergebnisse Folgendes feststellen (siehe Abbildung 24):

- Rund ein Drittel der befragten Unternehmen hat eine weitgehende Implementierung der automatischen Kontrollen umgesetzt und alle automatischen Kontrollen entlang der relevanten Prozessen evaluiert, implementiert, dokumentiert und nachvollziehbar in ihr internes Kontrollsystem integriert.
- Etwas mehr als die Hälfte (53%) sieht eine Möglichkeit, manuelle detektive Kontrollen durch automatische präventive Kontrollen zu ersetzen.
- Rund 70% haben vereinzelte Kontrollen mittels ERP-Funktionalitäten automatisiert (z.B. Toleranzgrenzen für Wareneingänge, Rechnungsprüfung).
- 24% der befragten Unternehmen geben an, keine automatischen Kontrollen implementiert zu haben.

Auch diesbezüglich zeigt sich, dass die grösseren Unternehmen die Automatisierung der Kontrollen stärker vorangetrieben haben als die kleineren Unternehmen:

- Während fast Dreiviertel der Unternehmen mit mehr als 1'000 und gegen die Hälfte der Unternehmen mit mehr als 250 Mitarbeitenden alle automatischen Kontrollen entlang der relevanten Prozesse in das IKS integriert hat, sind es bei Unternehmen mit weniger als 250 Mitarbeitenden lediglich rund ein Viertel.
- Eine Automatisierung von Kontrollen mittels ERP-Funktionalität erfolgt bei 86% der Unternehmen mit mehr als 250 Mitarbeitenden, jedoch nur bei 57% der Unternehmen mit weniger als 100 Mitarbeitenden.
- Mehr als 30% der Unternehmen mit weniger als 100 Mitarbeitenden geben an, keine automatischen Kontrollen implementiert zu haben. Bei Unternehmen mit mehr als 250 Mitarbeitenden liegt dieser Anteil bei 14%. Betrachtet man nur Unternehmen mit mehr als 1'000 Mitarbeitenden, so hat keines von ihnen angegeben, keine automatischen Kontrollen implementiert zu haben.

Abbildung 23: Bedeutung der manuellen Kontrollen nach Anzahl Mitarbeitende (n=200)

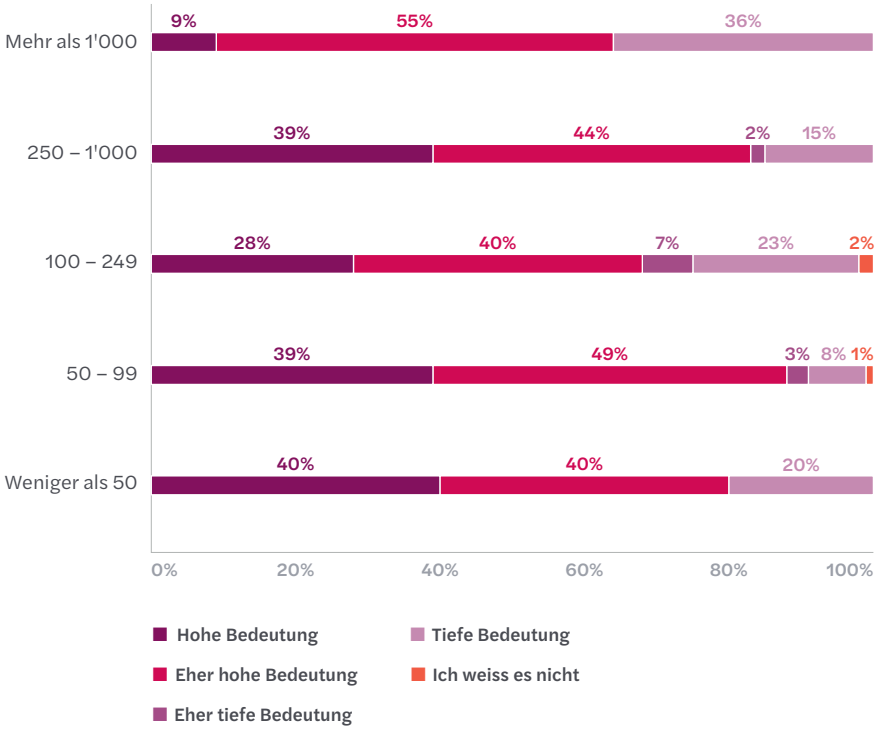
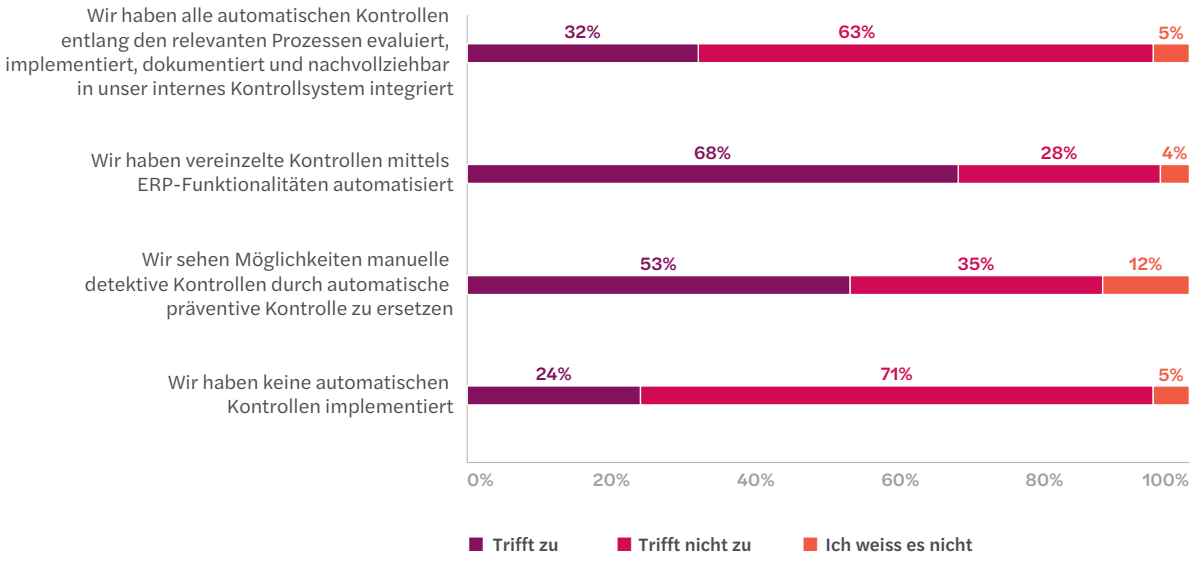


Abbildung 24: Inwieweit sind in Ihrem Unternehmen automatische Kontrollen implementiert? (n=278)



Insgesamt 74% der befragten Unternehmen geben an, dass **kritische organisatorische Funktionstrennungen auch im IT-/ERP-System** abgebildet sind (siehe Abbildung 25):

- Bei 35% sind kritische Funktionstrennungen für die Endanwender (z.B. Trennung von Einkaufsbestellung und Wareneingang) im IT/ERP-System umgesetzt, in einem Berechtigungskonzept dokumentiert und werden regelmässig mit Hilfe von Analyse-Tools ausgewertet.
- 24% geben an, dass mit Einführung des IT/ERP-Systems auf kritische Funktionstrennungen geachtet wurde, aber seither keine Auswertung mit Hilfe von Analyse-Tools erfolgt ist.
- Bei 15% liegt der Fokus auf «kritischen Benutzern» innerhalb der IT-Abteilung (wie z.B. Administratorenkonten).

Wird bei dieser Frage die Unternehmensgrösse herangezogen, so zeigt sich, dass die Abbildung kritischer organisatorischer Funktionstrennungen im IT-/ERP-System bei grösseren Unternehmen klar stärker umgesetzt ist als bei kleineren – so geben 64% der Unternehmen mit mehr als 1'000 Mitarbeitenden an, dass kritische Funktionstrennungen für die Endanwender (z.B. Trennung von Bestellung und Wareneingang) im IT/ERP-System umgesetzt und in einem Berechtigungskonzept dokumentiert sind sowie regelmässig mit Hilfe von Analyse-Tools ausgewertet werden. Bei 43% der Unternehmen mit weniger als 50 Mitarbeitenden erfolgt im Gegensatz dazu keine Abbildung im IT-/ERP-System (siehe Abbildung 26).

Bezüglich der Frage nach den **zukünftig grössten Herausforderungen im Bereich des internen Kontrollsystems** wird von den befragen Unternehmen hauptsächlich die laufende Pflege des internen Kontrollsystems bzw. die laufende Anpassung an veränderte Rahmenbedingungen und an das Risikoumfeld gesehen (in 66% der Antworten genannt). Häufig angegeben werden auch die Digitalisierung/Automatisierung des internen Kontrollsystems (47%) und die konsequente Umsetzung bzw. Einhaltung der Vorgaben im operativen Geschäft (44%) (siehe Abbildung 27).

Abbildung 25: Sind kritische organisatorische Funktionstrennungen auch im IT-/ERP-System Ihres Unternehmens abgebildet? (n=278)

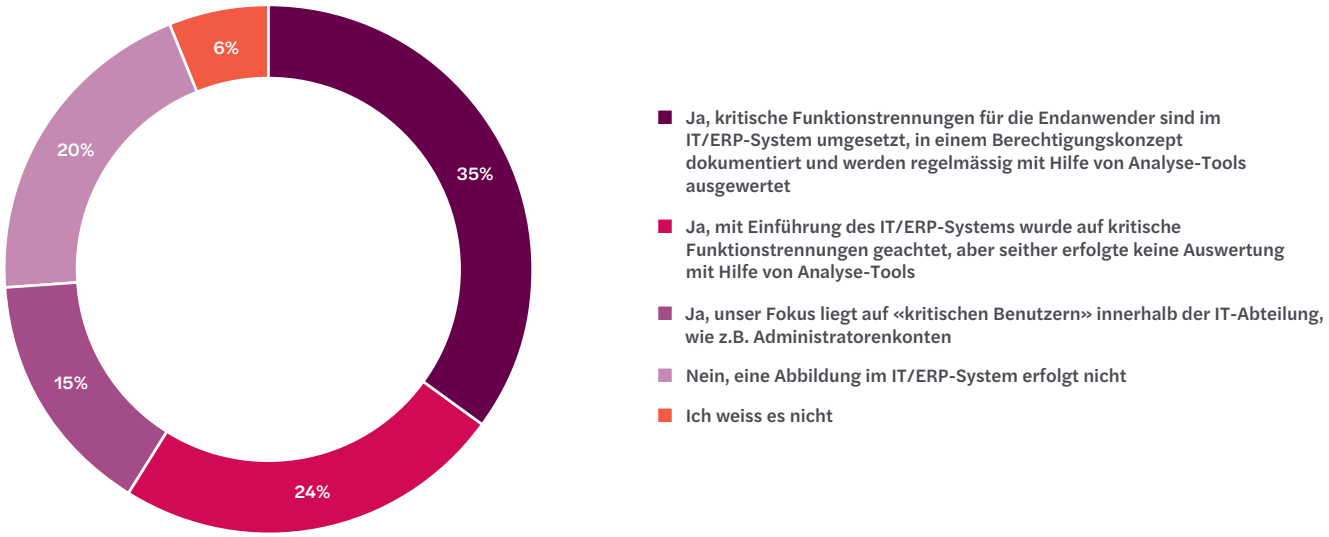
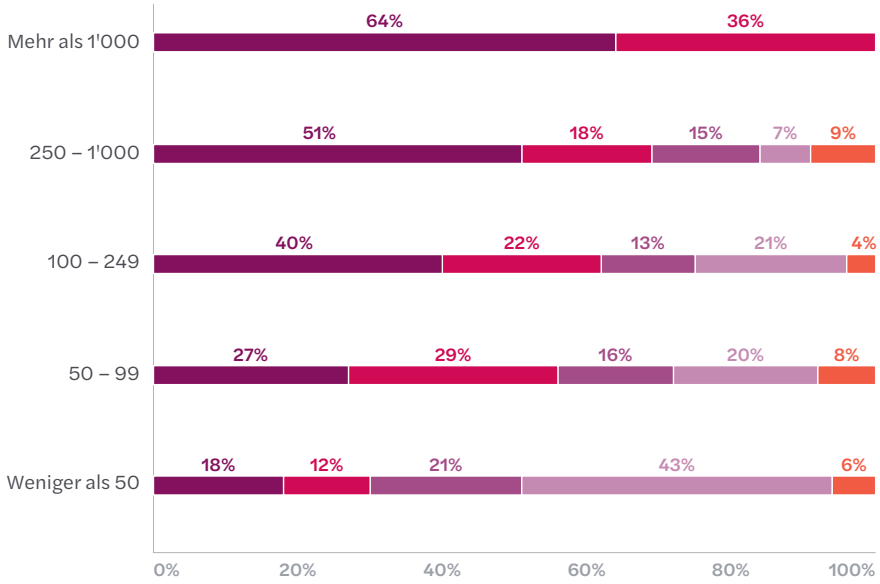
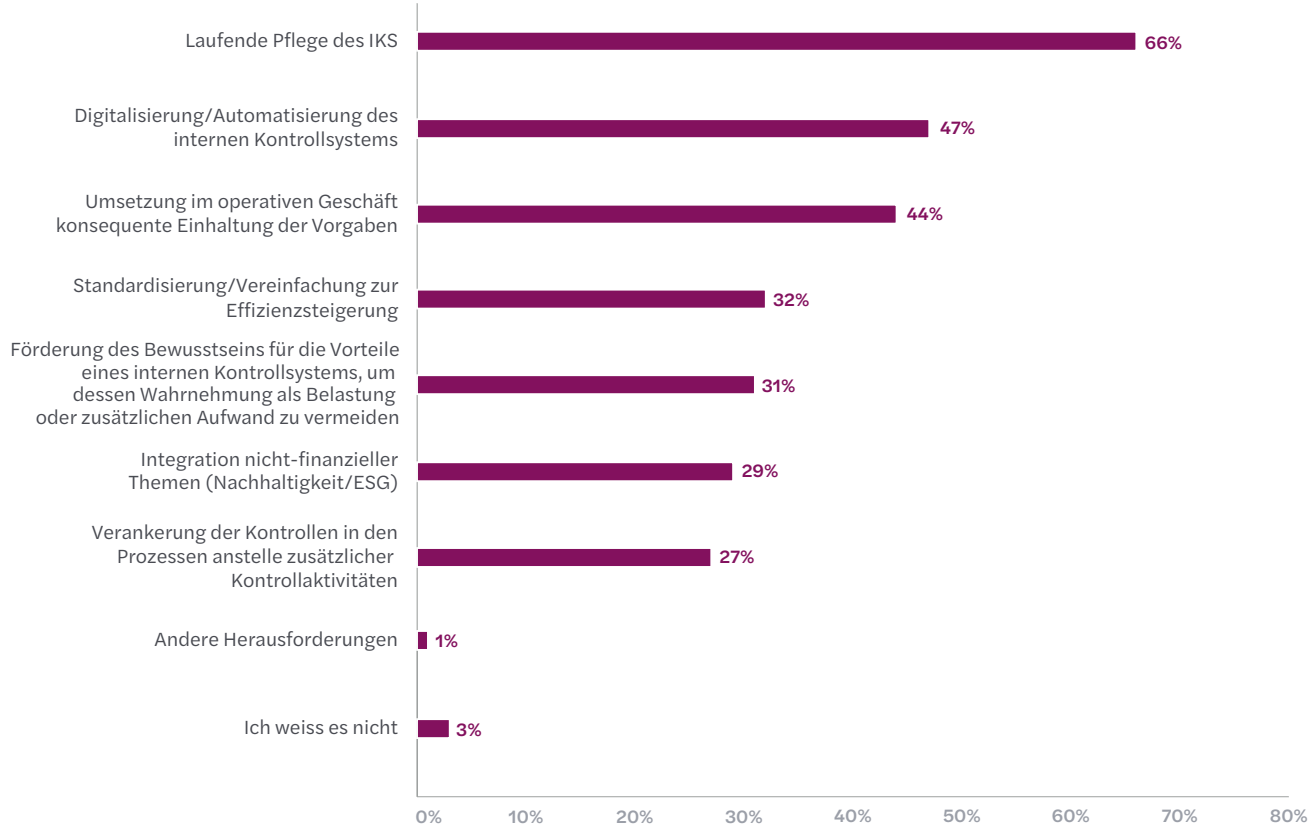


Abbildung 26: Sind kritische organisatorische Funktionstrennungen auch im IT-/ERP-System Ihres Unternehmens abgebildet (nach Anzahl Mitarbeitende)? (n=278)



- Ja, kritische Funktionstrennungen für die Endanwender sind im IT/ERP-System umgesetzt, in einem Berechtigungskonzept dokumentiert und werdenregelmässig mit Hilfe von Analyse-Tools ausgewertet
- Ja, mit Einführung des IT/ERP-Systems wurde auf kritische Funktionstrennungen geachtet, aber seither erfolgte keine Auswertung mit Hilfe von Analyse-Tools
- Ja, unser Fokus liegt auf «kritischen Benutzern» innerhalb der IT-Abteilung, wie z.B. Administratorenkonten
- Nein, eine Abbildung im IT/ERP-System erfolgt nicht
- Ich weiss es nicht

Abbildung 27: Worin bestehen Ihrer Meinung nach die in Zukunft grössten Herausforderungen im Bereich des internen Kontrollsystems? (n=278)



Digitalisierung, Automatisierung und Datenanalyse

Über 80% der befragten Unternehmen sind gegenüber Digitalisierungs- und Automatisierungsvorhaben offen bis sehr offen. Gleichzeitig liegt bei fast der Hälfte der Unternehmen keine klar definierte und kommunizierte Digitalisierungsstrategie vor. Als wichtigster Treiber für die Digitalisierung im IKS wird die Steigerung der Effizienz in der Kontrolldurchführung und -überwachung gesehen, während die fehlenden personellen Ressourcen als die klar grösste Herausforderung beim Vorantreiben der Digitalisierung gelten. Bei der Automatisierung sind die befragten Unternehmen noch zurückhaltend, insbesondere was Advanced Analytics und Künstliche Intelligenz/Maschinelles Lernen betrifft.

Die grosse Mehrheit der befragten Unternehmen zeigt sich gegenüber **Digitalisierungs- und Automatisierungsvorhaben** offen (58%) oder sogar sehr offen (25%), während nur eine verschwindend kleine Anzahl diesem Thema ablehnend gegenüber steht (siehe Abbildung 28). Dabei zeigt sich die positive Einstellung gegenüber der Digitalisierung und Automatisierung über alle Unternehmensgrössen hinweg, auch wenn Unternehmen mit mehr als 1'000 Mitarbeitenden besonders offen sind und die ablehnende Haltung ausschliesslich bei Unternehmen mit weniger als 100 Mitarbeitenden zu finden ist (siehe Abbildung 29).

Eine klar definierte und kommunizierte **Digitalisierungsstrategie** liegt bei rund 25% der befragten Unternehmen vor – insbesondere bei solchen mit mehr als 250 Mitarbeitenden – und bei ähnlich vielen ist eine solche Strategie in Ausarbeitung (siehe Abbildung 30). Andererseits verfügt fast die Hälfte der Unternehmen aktuell über keine konkrete Digitalisierungsstrategie, wobei es sich vor allem um Unternehmen mit weniger als 50 Mitarbeitenden (64%) handelt. Aber selbst 20% der Unternehmen mit mehr als 1'000 Mitarbeitenden haben angegeben, über keine Digitalisierungsstrategie zu verfügen.

Als wichtigste **Treiber bzw. Gründe für die Digitalisierung im internen Kontrollsystem** werden mit 50% mehrheitlich die Steigerung der Effizienz in der Kontrolldurchführung und -überwachung (und damit einhergehend die Senkung des Ressourcenaufwandes für das IKS) genannt, gefolgt von der Möglichkeit von datenbasierten Analysen und der Automatisierung von Kontrollen (35%) und Steigerung der Wirksamkeit in der Kontrolldurchführung und -überwachung mit 32% (siehe Abbildung 31). Nur in Ausnahmefällen (3%) wird angegeben, dass kein Bedarf für die Digitalisierung des internen Kontrollsystems besteht.

Die grössten **Herausforderungen beim Vorantreiben der Digitalisierung des internen Kontrollsystems** sehen die befragten Unternehmen klar bei den fehlenden personellen Ressourcen (48%), während finanzielle Aspekte mit 29% weniger oft genannt werden (siehe Abbildung 32). Häufig erwähnt werden auch die Komplexität der Umstellung von Systemen und Prozessen (29%) und das fehlende Knowhow (26%). Erwähnenswert ist zudem, dass Sicherheitsrisiken (Cyber Risks/Datenschutz) von lediglich 14% der Befragten genannt werden.

Abbildung 28: Wie schätzen Sie generell die Offenheit gegenüber Digitalisierungs- und Automatisierungsvorhaben in Ihrem Unternehmen ein? (n=278)

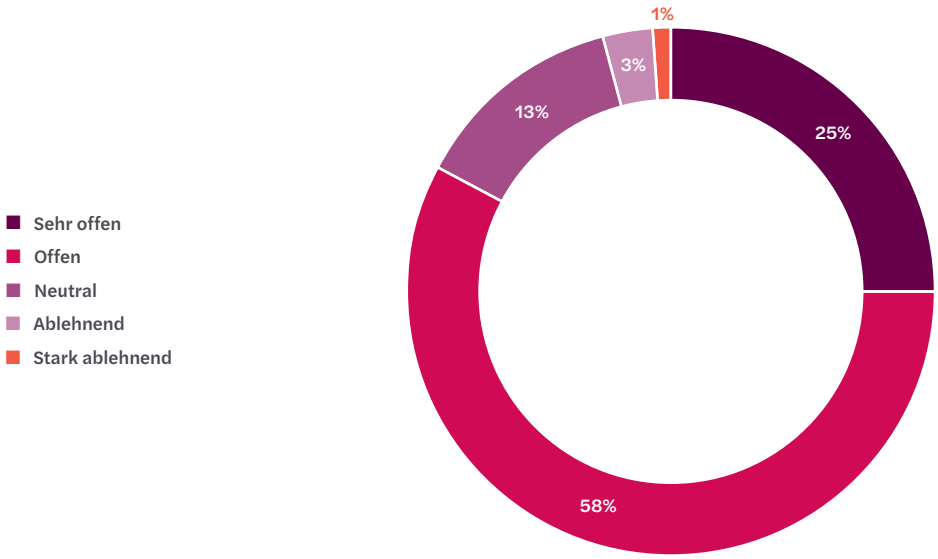


Abbildung 29: Wie schätzen Sie generell die Offenheit gegenüber Digitalisierungs- und Automatisierungsvorhaben in Ihrem Unternehmen ein (nach Anzahl Mitarbeitende)? (n=278)

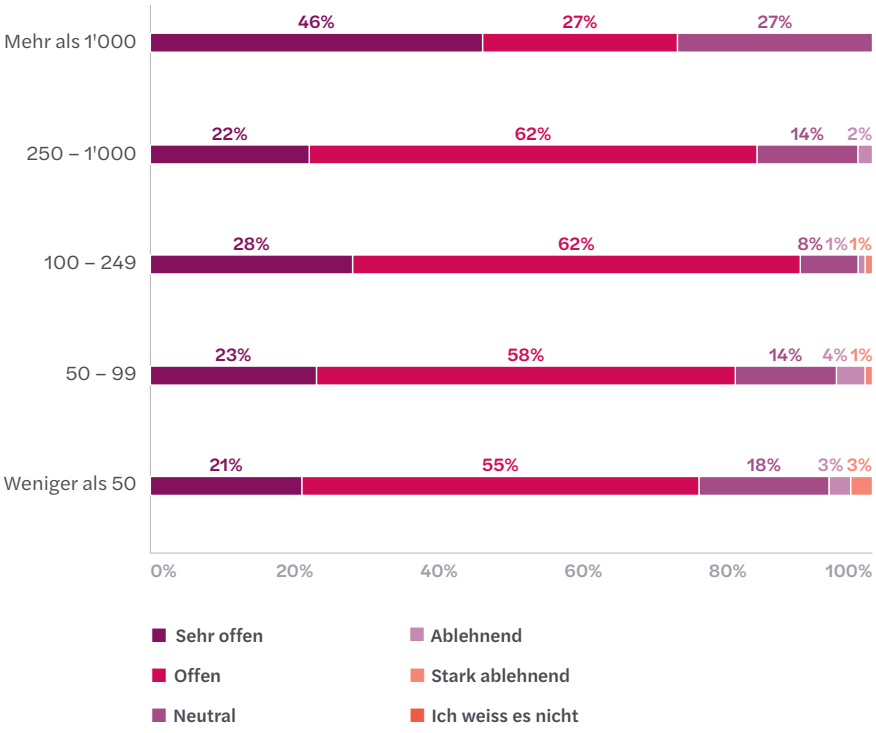


Abbildung 30: Liegt in Ihrem Unternehmen eine klar definierte und kommunizierte Digitalisierungsstrategie vor? (n=278)

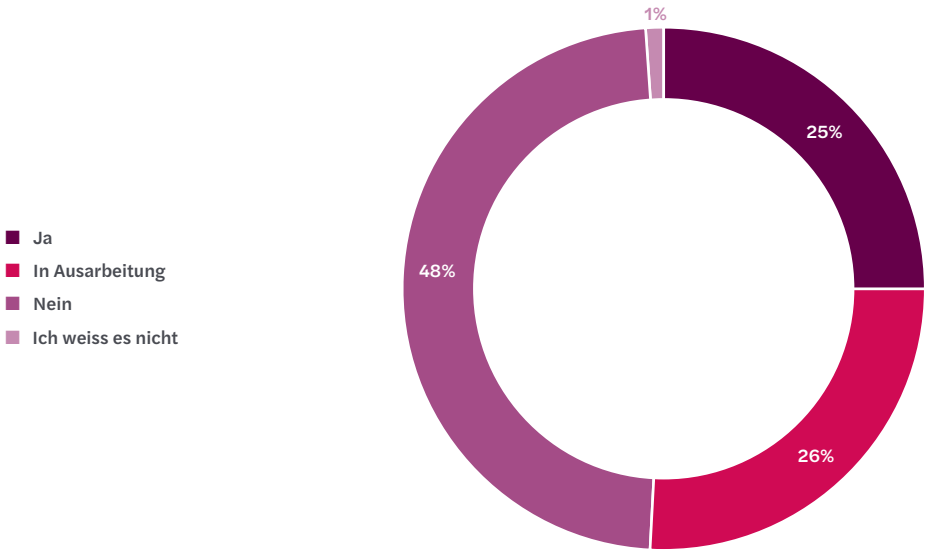
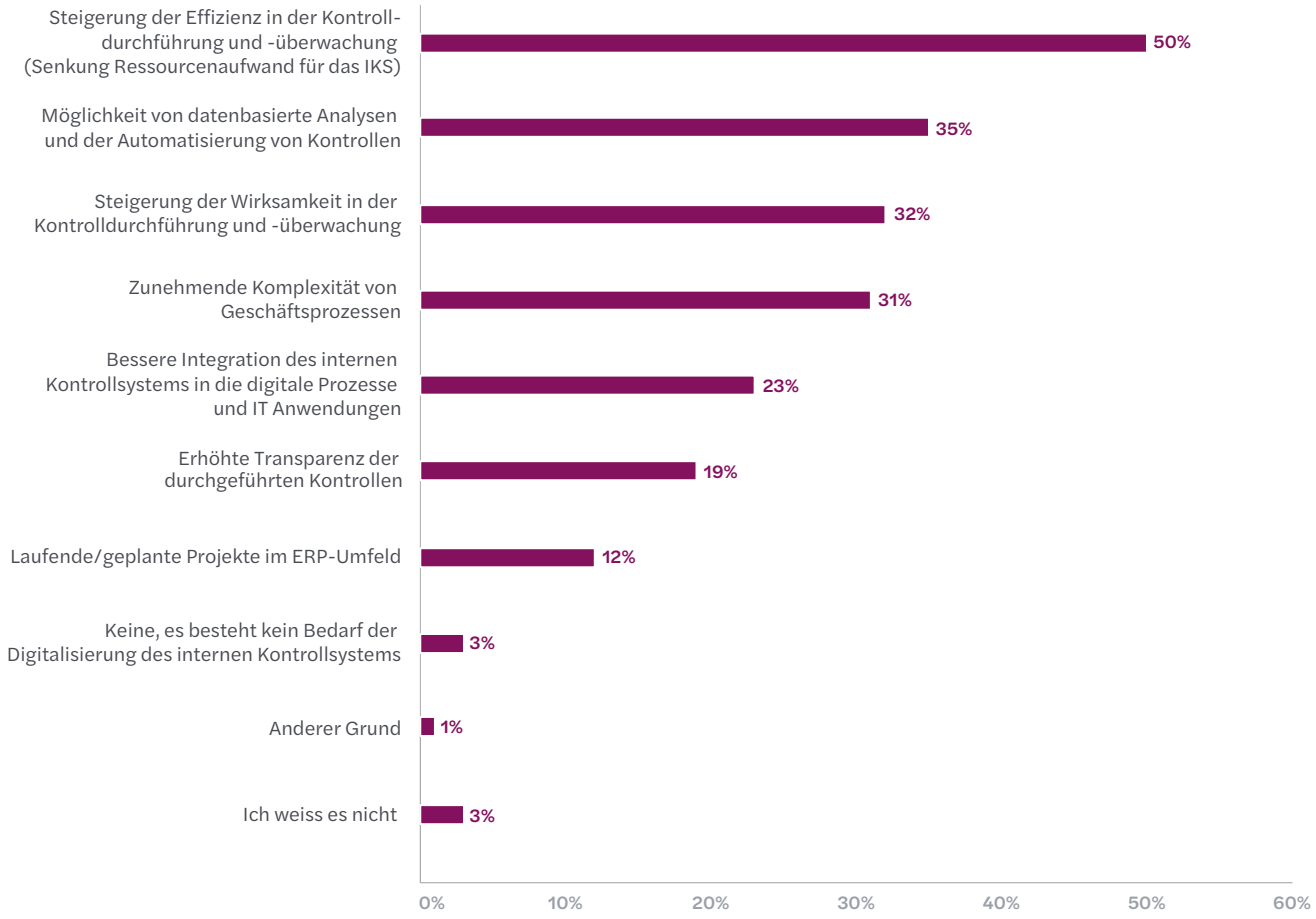


Abbildung 31: Wo sehen Sie die wichtigsten Treiber bzw. Gründe für die Digitalisierung im internen Kontrollsystem? (n=278)



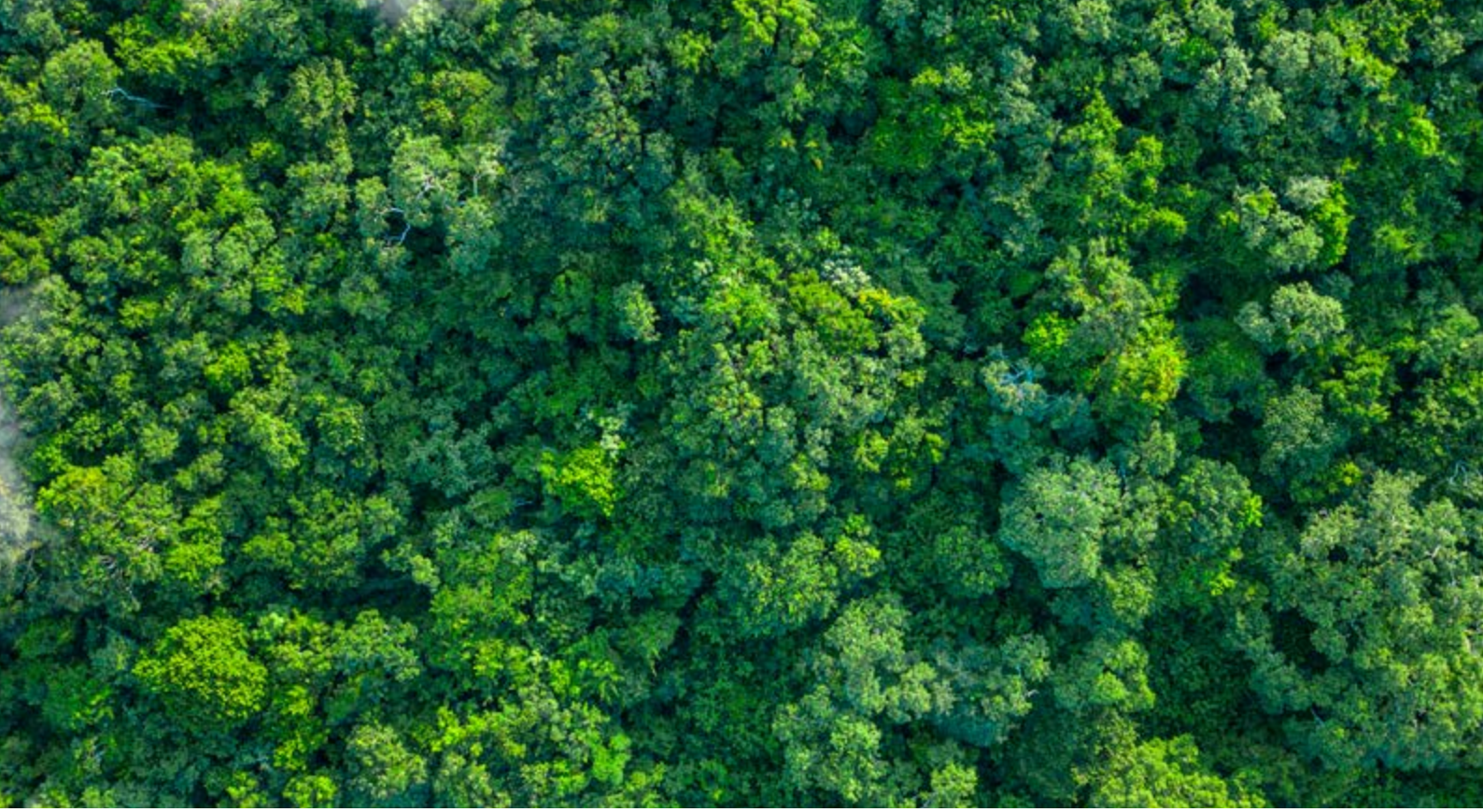
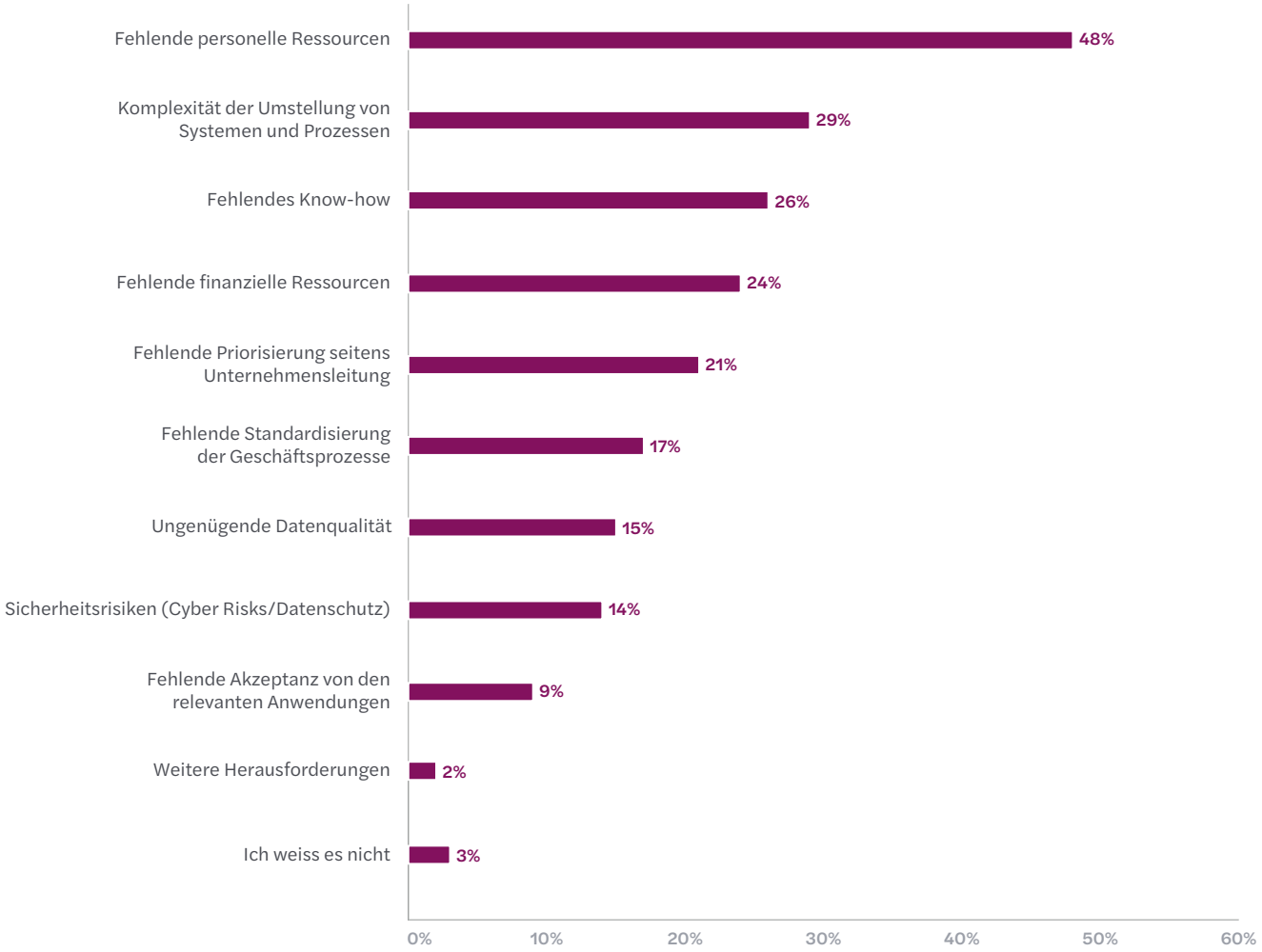


Abbildung 32: Welches sind aus Ihrer Sicht die grössten Herausforderungen beim Vorantreiben der Digitalisierung des internen Kontrollsystems? (n=278)



Bezüglich der Frage, welche **Formen der digitalen Unterstützung im Rahmen der Dokumentation** von Prozessen und Kontrollen zum Einsatz kommen, werden die digitalen Ablage von Kontrollnachweisen (47%) und die Analyse und Inventarisierung von Risiken (37%) am häufigsten genannt (Abbildung 33). Auch Workflowsysteme zur Bestätigung der Kontrolldurchführung sind ein Thema – 33% nutzen ein solches System bereits und weitere 25% planen eine Nutzung. Demgegenüber werden Formen wie die Prozessvisualisierungen und -beschreibungen (z.B. mit Hilfe von Process Mining Tools) und Softwarelösungen zur Dokumentation von Kontrollen und dem Massnahmen-Monitoring bei gegen der Hälfte der befragten Unternehmen nicht genutzt bzw. es ist keine Nutzung geplant.

Wenn es um die **Automatisierung im Rahmen des internen Kontrollsystems** geht, scheinen die befragten Unternehmen (noch) eher zurückhaltend zu sein. Am ehesten genutzt werden Datenanalysen bei der Kontrolldurchführung (27%) und für das datenbasierte Risikomanagement (25%), während nur je rund 4% Künstliche Intelligenz bzw. Maschinelles Lernen (z.B. zur Datenanalyse, Durchführung von Kontrollen sowie Erstellung und Optimierung von Kontrollberichten) und Advanced Analytics-Methoden (z.B. zur Erkennung von Trends oder Durchführung von Simulationen) nutzen (siehe Abbildung 34). Während die Nutzung von Künstlicher Intelligenz und Maschinellem Lernen bei 22% der Unternehmen zumindest angedacht wird, ist dies bei den Advanced Analytics-Methoden nur bei 8% der Fall. Wie zu erwarten handelt es sich bei den aktuellen Nutzern von Künstlicher Intelligenz (KI) und Maschinellem Lernen (ML) sowie Advanced Analytics-Methoden beinahe ausschliesslich um solche mit mehr als 1'000 Mitarbeitenden. Unter den Unternehmen, die den Einsatz von KI und ML in Erwägung ziehen, sind jedoch alle Kategorien relativ gleichmässig vertreten: jeweils rund 25% der Unternehmen mit 250 bis 1'000 und 100 bis 249 Mitarbeitenden sowie jeweils rund 20% der Unternehmen mit 50 bis 99 und weniger 50 Mitarbeitenden.

Bei der **Datenanalyse im Rahmen von Risikomanagement und internen Kontrollen** kommt bei 82% der Unternehmen Excel zur Anwendung und 34% nutzen Datenanalyse Tools wie PowerBI, Qlik oder Tableau (siehe Abbildung 35). Kaum eingesetzt werden Datenanalyse-Tools in Verbindung mit Large Language Models (LLM) wie ChatGPT und Co-Pilot. Als weitere Tools werden nebst Eigenentwicklungen auch Werkzeuge innerhalb des ERP-Systems oder die Swiss GRC Toolbox genannt.

Abbildung 33: Welche Formen der digitalen Unterstützung kommen in Ihrem Unternehmen im Rahmen der Dokumentation von Prozessen und Kontrollen zum Einsatz? (n=278)

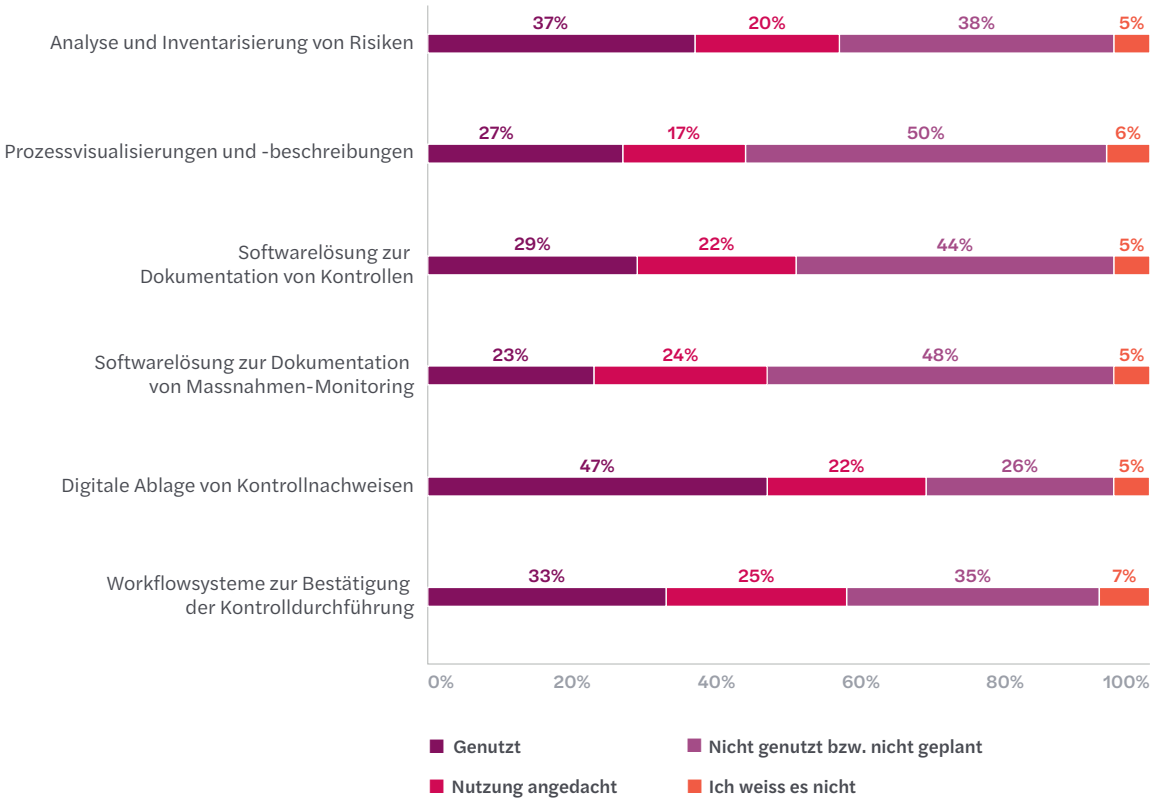


Abbildung 34: Welche Formen der Automatisierung kommen in Ihrem Unternehmen im Rahmen des internen Kontrollsystems generell zum Einsatz? (n=278)

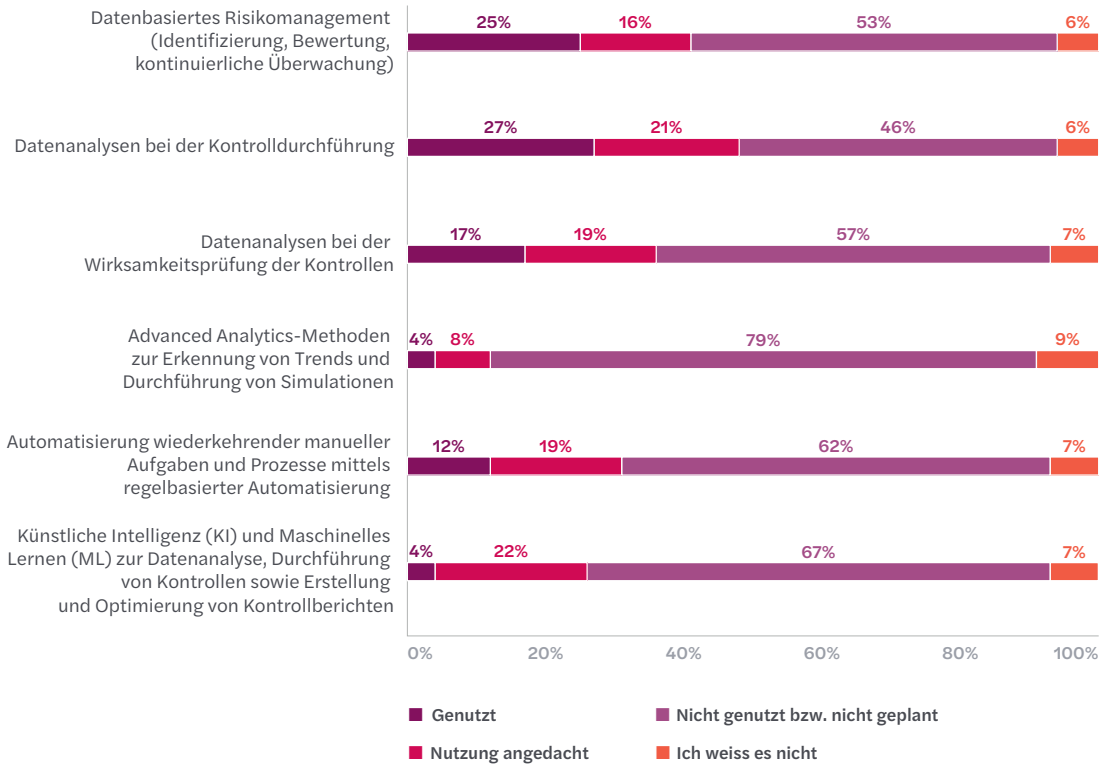
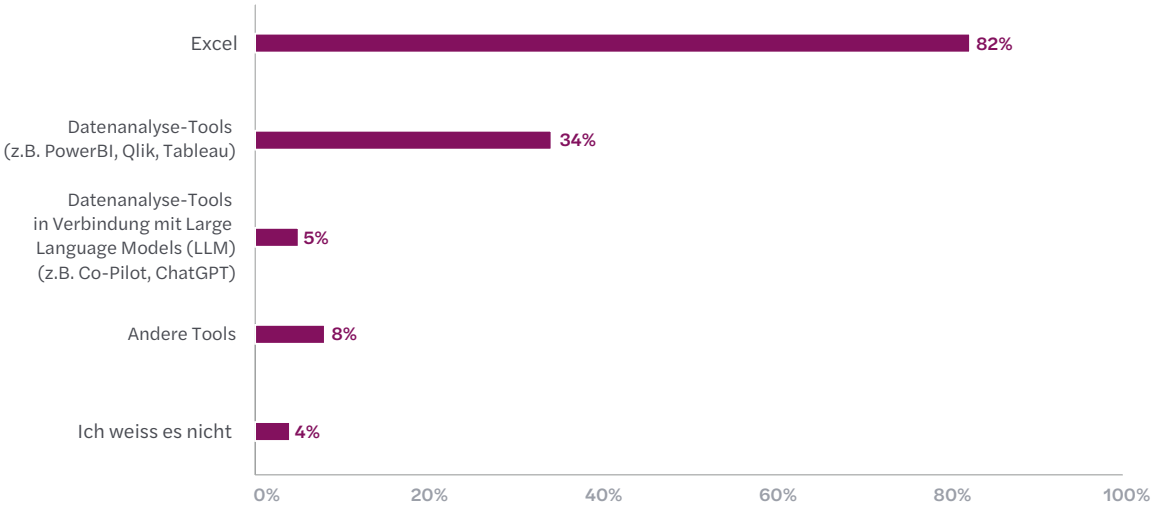


Abbildung 35: Welche Form von Datenanalysen im Rahmen von Risikomanagement und internen Kontrollsystemen nutzen Sie in ihrem Unternehmen? (n=278)



Ergebnisse der Interviews

In den Interviews wurde betont, dass Risikomanagement und interne Kontrollen essenziell für eine effektive Unternehmensführung sind. Ein systematisches Vorgehen ist zentral, wobei die Ausgestaltung von der Unternehmensgrösse und der Komplexität des Geschäftsmodells abhängt und kleinere Organisationen pragmatische Ansätze verfolgen können. Die grössten Herausforderungen sehen die Befragten in der Digitalisierung und Automatisierung des internen Kontrollsystems, wobei Schweizer KMU oft noch nicht weit fortgeschritten sind. Dennoch sind die Befragten überzeugt, dass sich die Digitalisierung und Automatisierung zukünftig stärker durchsetzen werden.

Insgesamt wurden sechs Interviews mit Fachexpertinnen und -experten geführt, die sich in ihrer täglichen Arbeit aus unterschiedlichen Gründen mit den Themen aus dem Risikomanagement und dem internen Kontrollsystem beschäftigen. Dies waren nebst Anwendern auch Beraterinnen und Berater im Bereich des Risikomanagements und der internen Kontrollen sowie Expertinnen und Experten aus der Forschung (Interviewpartnerinnen und -partner Seite 58).

Organisatorische Ausgestaltung

Die Mehrheit der befragten Expertinnen und Experten ist sich einig, dass die Gesamtverantwortung für die Koordination und Überwachung des Risikomanagements und des internen Kontrollsystems (IKS) idealerweise beim Verwaltungsrat liegen sollte, während die Geschäftsleitung die operative Verantwortung trägt. In der Praxis zeigt sich aus ihrer Erfahrung jedoch, dass das interne Kontrollsystem häufig in der Finanzabteilung angesiedelt ist, was auch die Umfrageergebnisse bestätigen. Dies liegt vermutlich daran, dass gesetzliche Anforderungen an ein IKS hauptsächlich finanzielle Aspekte betreffen, weshalb sich betroffene Unternehmen auf interne Kontrollen in finanziellen Prozessen konzentrieren. Bei dieser Konstellation ist es zentral, dass der Finanzleiter/CFO den Verwaltungsrat, dem die Gesamtverantwortung für das interne Kontrollsystem obliegt, regelmässig über die Belange des internen Kontrollsystems informiert. In mehreren Interviews kommt auch klar zum Ausdruck, dass ein effektives internes Kontrollsystem über die gesetzlichen Mindestanforderungen hinaus auch operative Risiken abdecken muss – dabei wäre die Ansiedlung des IKS-Prozesses beim CFO zu «finanzlastig» und die Zuständigkeit sollte konsequenterweise bei der operativen Leitung liegen. Zudem wird betont, dass bei der Ausgestaltung von Risikomanagement und IKS vor allem die Komplexität des Geschäftsmodells und nicht allein die Unternehmensgrösse entscheidend ist. Es ist auch wichtig zu berücksichtigen, in welchem Umfeld die Kunden tätig sind – sind wichtige Kunden zum Beispiel börsenkotiert und/oder in einem regulierten Bereich wie dem Finanzsektor tätig, müssen die Unternehmen unabhängig ihrer Grösse als Lieferanten teilweise auch Vorgaben bezüglich Risikomanagement und interne Kontrollen erfüllen. Allgemein ist zu beobachten, dass die Anforderungen auch an kleine und mittlere Unternehmen, die entweder direkt in regulierten Branchen tätig sind oder Abnehmer aus diesen Branchen haben, aufgrund gestiegener regulatorischer Anforderungen immer weiter zunehmen.

In Bezug auf die Frage, ob es für Risikomanagement und interne Kontrollen eine dedizierte Stelle braucht, herrscht unter den befragten Personen weitgehend Einigkeit, dass eine solche Position vor allem für klei-

nere KMUs nicht zwingend erforderlich ist. Wichtig ist jedoch, dass diese Aufgaben klar zugewiesen und in die Stellenbeschreibungen anderer geeigneter Positionen integriert werden. Ein Experte schlägt zum Beispiel vor, strategische Themen beim CEO anzusiedeln, während das Team zum Qualitätsmanagement die Prozesssicht einnimmt und die IT-Sicherheit in der IT-Abteilung (z.B. beim «Chief Information Security Officer») zu verorten ist. Ein anderer Experte spricht sich hingegen grundsätzlich gegen die Schaffung dedizierter Stellen in diesem Bereich aus und argumentiert, dass die Mitarbeitenden im operativen Bereich die Geschäftsrisiken am besten einschätzen können, da sie direkt am «Puls» des Geschehens sind. Einige Experten haben die Erfahrung gemacht, dass bei KMUs die Themen Risikomanagement und interne Kontrollen oft als «Nebenschauplatz» betrachtet und eher «stiefmütterlich» behandelt werden. Die Aufgaben werden häufig auf verschiedene Personen verteilt, die sich primär mit anderen Aufgaben beschäftigen und diesen Themen keine hohe Priorität einräumen. In solchen Fällen fehlt dann oft eine Gesamtsicht, was ein grösseres Risiko darstellen kann.

Die befragten Expertinnen und Experten stimmen überein, dass das interne Kontrollsystem ein integraler Bestandteil des unternehmensweiten Risikomanagements sein sollte. Alternativ sollte zumindest eine regelmässige Abstimmung zwischen beiden Bereichen erfolgen. Eine isolierte Betrachtung der beiden Bereiche ist weder sinnvoll noch effizient. Ohne Abstimmung besteht die Gefahr, dass Kontrollen nicht risikobasiert implementiert werden und somit nicht gewährleistet ist, dass das IKS die relevanten Risiken abdeckt. Aus Erfahrung werden bei fehlender Abstimmung häufig zu viele Kontrollen eingeführt, wodurch das interne Kontrollsystem weder effizient noch zielgerichtet ausgestaltet wird. Eine regelmässige Abstimmung der beiden Bereiche stellt zudem sicher, dass Änderungen in der Risikostruktur (z.B. aufgrund neuer Geschäftsfelder oder neuer Prozesse) im internen Kontrollsystem entsprechend berücksichtigt werden. Es wird auch verschiedentlich darauf hingewiesen, dass Risikomanagement und interne Kontrollen insbesondere in kleineren, eigentümergeführten Unternehmen häufig von derselben Person betreut werden, wodurch eine Abstimmung zwischen beiden Bereichen automatisch sichergestellt wird.

In Bezug auf die Frage, ob die vollständige Umsetzung des «Three-Lines-of-Defense»-Modells auch für mittlere und kleinere Unternehmen sinnvoll ist, plädiert ein Teil der befragten Personen für eine pragmatische Herangehensweise. Sie sind der Ansicht, dass es hilfreich ist, wenn Unternehmen das Grundprinzip mit den drei Verteidigungslinien kennen und dann überlegen, wie sie daraus eine sinnvolle Organisation auf KMU-Ebene entwickeln können. Andere Experten sind der Meinung, dass jedes Unternehmen, unabhängig von seiner Grösse, eine interne Revision benötigt. Sie empfehlen die Einrichtung einer dritten Verteidigungslinie, die je nach Risiken des Geschäftsmodells sogar zwingend erforderlich sein kann. In einfacheren Verhältnissen kann diese Verteidigungslinie schlank gehalten werden. Es ist zudem prüfenswert, diese Position extern zu besetzen oder ausführen zu lassen. Falls auf eine interne Revision oder eine vergleichbare Stelle verzichtet wird, sollte zumindest eine unabhängige zweite Verteidigungslinie (Risikomanagement/Compliance) vorhanden sein. Letztendlich hängt der Umfang der Ausgestaltung davon ab, als wie wichtig das Thema Risikomanagement und internes Kontrollsystem von der Unternehmensführung bzw. der Eigentümerschaft betrachtet wird. Dabei ist es von entscheidender Bedeutung, dass insbesondere bei kleineren KMU eine gründliche Kosten-Nutzen-Analyse durchgeführt wird. Ein Experte beobachtet zudem, dass ein Verwaltungsratsgremium umso mehr auf die drei Verteidigungslinien bestehen wird, je professioneller dieses ist.

Risikomanagement

Die befragten Expertinnen und Experten sind der Ansicht, dass ein strukturierter Ansatz zur Risikoerkennung zentral ist. Wichtig dabei ist, dass sich die Unternehmensleitung konsistent und in regelmässigen Abständen – jedoch mindestens einmal im Jahr – bewusst mit dem Risikomanagement auseinandersetzt und sei dies «nur» mittels eines Traktandums an einer Unternehmensleitungssitzung. Dies zwingt die Unternehmensleitung, sich regelmässig objektiv und systematisch mit den Risiken zu befassen und diese auf den Tisch zu bringen. Für spezifische Risiken wie Cyberrisiken kann es sinnvoll sein, punktuell externe Personen beizuziehen.

Das immer wieder vorgebrachte Argument der «überformalisierten Bürokratisierung» wird von einigen der interviewten Personen damit entkräftet, dass ein formalisierter und strukturierter Ansatz im Risikomanagement nicht zwangsläufig zu mehr Bürokratie führt. Besonders für KMU geht es nicht darum, internationale Rahmenwerke wie COSO oder ISO 31000 eins zu eins umzusetzen. Diese theoretischen Rahmenwerke können zwar als Ausgangspunkt dienen, doch letztlich geht es nicht um die «beste Methodik» – vielmehr steht im Vordergrund, Risiken zu identifizieren, deren Wahrscheinlichkeit einzuschätzen und deren Auswirkungen zu bewerten. Dies kann einfach mittels einer Risiko-

matrix in einer Excel-Tabelle erfolgen. Letztlich ist es viel wichtiger, dass das Risikomanagement etabliert und gelebt wird, als dass es formalisiert ist. Bürokratie wäre in diesem Fall eher hausgemacht und entsprechend unnötig.

Laut der Umfrage beschäftigen sich die Verantwortlichen der befragten Unternehmen am häufigsten mit IT-Sicherheit und Cyberrisiken. Dieses Ergebnis überrascht die Befragten nicht und deckt sich weitgehend mit ihren eigenen Erfahrungen. Es wird vermutet, dass Cyberrisiken besonders viel Aufmerksamkeit erhalten, weil das Thema relativ neu und aktuell in aller Munde ist, während andere Risiken bereits etablierter sind. Zudem wird auf die Vor- und Nachteile der Digitalisierung hingewiesen – sie führt oft zu mehr Effizienz, macht die digitalisierten Prozesse jedoch auch anfälliger. Besonders durch die Fortschritte im Bereich der Künstlichen Intelligenz ist es für Cyberkriminelle heute leichter, eine grosse Anzahl auch kleinerer Unternehmen anzugreifen. Ein befragter Experte meint, dass Schweizer KMU schlecht auf diese IT-Risiken vorbereitet sind. Umso wichtiger ist es, dass sich KMU dieser Risiken bewusst sind und bei Bedarf mit erfahrenen IT-Spezialisten zusammenarbeiten, falls qualifiziertes Personal mit dem entsprechenden Know-how nicht vorhanden ist. Aus Sicht einer der befragten Personen wäre es wünschenswert, dass Lösungen auf übergeordneter Ebene (z.B. auf Verbandsebene) entwickelt werden und dass der Bund oder die öffentliche Hand vermehrt Förderprogramme anbietet, um den Cyberrisiken besser zu begegnen.

Zusätzlich nennen die befragten Expertinnen und Experten Themen wie die geopolitische Lage, Lieferkettenrisiken, Lieferantenabhängigkeit und Fachkräftemangel als aktuelle wesentliche Risiken. Eine der befragten Personen vertritt demgegenüber die Meinung, dass Geopolitik und Lieferkettenprobleme für viele Unternehmen nicht mehr im Vordergrund stehen, da sie sich inzwischen an die aussergewöhnliche Situation gewöhnt haben. Stattdessen rücken Risiken im Bereich Umwelt, Soziales und Unternehmensführung (ESG: Environmental, Social, Governance) stärker in den Fokus. Ein Experte betont, dass viele Unternehmen Risikothemen opportunistisch angehen und sich vor allem aufgrund von externem Druck, etwa durch Gesetzgeber oder Regulatoren, damit auseinandersetzen.

Internes Kontrollsystem

Die Mehrheit der Befragten ist der Ansicht, dass ein internes Kontrollsystem (IKS) generell – auch bei kleineren Unternehmen – unabdingbar ist. Ein funktionierendes und effektives IKS ist ein wesentlicher Bestandteil verantwortungsvoller Unternehmensführung («Good Governance»). Es trägt massgeblich zur Vermeidung und Minderung von Risiken bei und wirkt präventiv gegen Betrug. Zudem unterstützt ein IKS die Standardisierung von Prozessen und kann den Aufwand für die externe Revision sowie potenziell auch die Revisionskosten senken. Dabei ist es wichtig sicherzustellen, dass die Prozesse zur Risikoidentifikation geeignet sind und die Kontrollpunkte an den richtigen Stellen gesetzt werden. Ähnlich wie beim Risikomanagement sind die meisten der Befragten der Meinung, dass ein systematisches Vorgehen bei der Gestaltung eines internen Kontrollsystems von zentraler Bedeutung ist. Insbesondere in kleineren und weniger komplexen Organisationen kann ein pragmatischer und weniger anspruchsvoller Ansatz sinnvoll sein.

Die befragten Expertinnen und Experten identifizieren mehrere Hauptgründe für Schwachstellen im internen Kontrollsystem. An erster Stelle stehen die mangelnde Führung und eine unzureichende organisatorische Verankerung, was zu einem geringen Kontrollbewusstsein innerhalb der Organisation führt. Weitere genannte Faktoren sind fehlendes Know-how, mangelndes Verständnis für Compliance-Themen und allgemeiner Zeitdruck. Eine generelle Herausforderung besteht darin, dass Sekundärprozesse wie die internen Kontrollen in erster Linie oft als Kostenfaktor betrachtet werden. Daher ist es umso wichtiger, den Mitarbeitenden den Mehrwert eines funktionierenden IKS zu verdeutlichen. Dies gelingt besonders gut, wenn die internen Kontrollen in die bestehenden operativen Prozesse integriert sind und nicht als separates, paralleles System wahrgenommen werden. Mehrfach wird auch betont, dass die Wahrscheinlichkeit für Schwachstellen erheblich reduziert werden kann, wenn Kontrollen möglichst automatisiert und somit von menschlichen Fehlern und Unterlassungen entkoppelt werden.

Die Befragten sehen die grössten Herausforderungen im Bereich des internen Kontrollsystems mehrheitlich in der Digitalisierung und Automatisierung, insbesondere der Automatisierung von Kontrollen. Damit einhergehend nehmen die Abhängigkeit von Technologie und die Komplexität der IT-Sicherheitsthemen zu.

Digitalisierung und Automatisierung

Die Mehrheit der befragten Personen sieht den Haupttreiber für die Digitalisierung im internen Kontrollsystem in der höheren Effizienz. Durch die Digitalisierung werden Fehler reduziert, die Transparenz erhöht, das Reporting und Monitoring vereinfacht, Zeit gespart, die Unabhängigkeit von menschlichen Eingriffen gesteigert und die Standardisierung der Prozesse verbessert.

Bezüglich der grössten Herausforderungen werden nebst der Standardisierung der Prozesse und noch stärker in den Fokus kommenden Cyberrisiken vor allem die fehlenden personellen aber auch finanziellen Ressourcen genannt. Als Sekundärprozess hat das interne Kontrollsystem bei der internen Ressourcenallokation nicht immer die besten Karten, insbesondere wenn diese Ressourcen knapp sind, was bei KMU eher die Regel als die Ausnahme ist.

In einem der Interviews wird darauf hingewiesen, dass die digitale Unterstützung zur Dokumentation von Prozessen und Kontrollen im KMU-Bereich noch nicht weit verbreitet ist, insbesondere wenn man excelbasierte Lösungen ausser Acht lässt. Eine Ausnahme bilden Unternehmen in Branchen mit strengen Standards, wie beispielsweise die Pharmaindustrie. Viele Unternehmen zögern offenbar, solche Systeme einzuführen, wahrscheinlich aufgrund der erforderlichen Ressourcen und des nicht sofort erkennbaren Mehrwerts. Auch im Bereich der Automatisierung innerhalb des internen Kontrollsystems gibt es bei Schweizer KMUs derzeit oft nur geringe Fortschritte. Obwohl das Thema in aller Munde und den meisten Unternehmen bekannt ist, hat es insbesondere in der KMU-Welt noch keinen festen Platz im Alltag gefunden. Es wird weiterhin mehr darüber diskutiert als tatsächlich gehandelt, und viele Unternehmen zögern noch, konkrete Automatisierungsinitiativen umzusetzen. Oft beschränken sich die Datenanalysen auf Excel oder excelbasierte Lösungen, was jedoch besonders bei überschaubaren Verhältnissen ausreichend ist. Aus Kosten-Nutzen-Überlegungen sollte die Anschaffung spezieller Tools immer sorgfältig geprüft werden.

Im Rahmen eines der Interviews wird auch die Feststellung gemacht, dass KMU im Bereich der Digitalisierung zwar oft nicht sehr versiert sind, gleichzeitig aber die Möglichkeiten unterschätzen, die ihnen bereits durch bestehende Tools und Systeme, insbesondere die aktuellen Versionen der ERP-Systeme, zur Verfügung stehen.

Trotz dieser Herausforderungen sind die Befragten aufgrund der offensichtlichen Vorteile der Digitalisierung und Automatisierung überzeugt, dass sich diese Themen auch in der KMU-Welt zukünftig immer stärker durchsetzen werden. Dies gilt insbesondere vor dem Hintergrund, dass die den internen Kontrollen zugrunde liegenden Prozesse nach und nach digitalisiert und automatisiert werden.

Fazit und Ausblick

Als Haupterkenntnis aus der vorliegenden Studie lässt sich einerseits ableiten, dass Risikomanagement und interne Kontrollen bei den meisten der befragten Unternehmen einen hohen Stellenwert geniessen. Andererseits zeigt die Studie, dass eine klare Mehrheit der befragten Unternehmen offen für Digitalisierungs- und Automatisierungsvorhaben ist, die Umsetzung dieser Vorhaben aber noch zögerlich erfolgt. Die befragten Expertinnen und Experten sind jedoch überzeugt, dass sich die Digitalisierung und Automatisierung im Bereich des Risikomanagements und der internen Kontrollen auch in der Welt der Schweizer KMU zukünftig immer stärker durchsetzen wird.

Risikomanagement und interne Kontrollen gelten gemeinhin als essenziell für eine effiziente und effektive Unternehmensführung. Die Umfrageergebnisse zeigen, dass diese Themen auch für die Mehrheit der befragten Unternehmen einen hohen Stellenwert haben. Während die Koordination und Überwachung des Risikomanagements bei den befragten Unternehmen häufig auf Stufe der obersten Führungsebene erfolgt, sind diese Aufgaben beim internen Kontrollsystem mehrheitlich bei der finanziellen Führung angesiedelt. Dies wird von einem Teil der interviewten Personen bedauert – für sie sollte ein wirksames internes Kontrollsytem nicht nur wie gesetzlich für gewisse Unternehmen in der Schweiz vorgegeben die finanziellen Prozesse, sondern auch die operativen Prozesse abbilden und müsste konsequenterweise bei der operativen Unternehmensleitung angesiedelt sein. Dabei ist ein systematisches Vorgehen bei der Ausgestaltung des Risikomanagements und des internen Kontrollsystems zentral, wobei kleinere Unternehmen auch einfachere und pragmatische Ansätze verfolgen können – wichtiger als die Umsetzung einer formalisierten Methodik ist, dass diese Themen in einer Organisation etabliert sind und effektiv gelebt werden. Dies gelingt besonders gut, wenn Risikomanagement und internes Kontrollsystem in die bestehenden operativen Prozesse integriert sind und nicht als separate, parallele Systeme wahrgenommen werden. Wichtig ist auch zu erkennen, dass die Ausgestaltung des Risikomanagements und des internen Kontrollsystems nicht allein von der Unternehmensgrösse, sondern auch von der Komplexität des Geschäftsmodells abhängt. Gerade kleine und mittlere Unternehmen in regulierten Branchen oder mit Kunden aus diesen Branchen sehen sich steigenden regulatorischen Anforderungen gegenüber, welchen sie zwingend nachzukommen haben.

Die Umfrageergebnisse zeigen auch, dass sich die befragten Unternehmen aktuell vor allem mit der IT-Sicherheit und Cyberrisiken auseinandersetzen. Hinweise aus den Interviews zeigen jedoch, dass Schweizer KMU eher schlecht auf diese IT-Risiken vorbereitet zu sein scheinen. Umso wichtiger ist es, dass sich die Unternehmen dieser Risiken bewusst sind und bei Bedarf mit erfahrenen IT-Spezialisten zusammenarbeiten. In einer globalisierten Welt können Cyberrisiken nicht von Einzelunternehmen alleine mitigiert werden. Es wäre daher wünschenswert, vermehrt Lösungen auf übergeordneter Ebene (z.B. auf Verbandsebene) zu entwickeln und dass der Bund oder die öffentliche Hand entsprechende Förderprogramme anbietet, um diesen Risiken besser begegnen zu können.

Die Umfrageergebisse bestätigen schliesslich, dass eine grosse Mehrheit der befragten Unternehmen Digitalisierungs- und Automatisierungsvorhaben offen bis sehr offen gegenüberstehen. Gleichzeitig zeigt sich aber, dass die Unternehmen bei der Automatisierung des internen Kontrollsystems, insbesondere bei Advanced Analytics und Künstlicher

Intelligenz/Maschinellem Lernen, noch zurückhaltend sind, was sich auch mit den Feststellungen der befragten Personen deckt. Diese sind jedoch überzeugt, dass sich die Digitalisierung und Automatisierung im Bereich des Risikomanagements und der internen Kontrollen auch in der Welt der Schweizer KMU zukünftig immer stärker durchsetzen wird. Dies gilt insbesondere vor dem Hintergrund, dass die dem internen Kontrollsystem zugrunde liegenden Prozesse nach und nach digitalisiert und automatisiert werden. Zudem sind die ERP-Systeme immer mehr auf die Digitalisierung und Automatisierung der Prozesse ausgerichtet. Schliesslich sind Digitalisierung und Automatisierung auch geeignete Mittel, um den in der Umfrage genannten Herausforderungen bezüglich Mangel an personellen Ressourcen (z.B. im Zusammenhang mit Schwachstellen im IKS) zu begegnen. Der fortschreitenden Digitalisierung und Automatisierung werden sich auch die diesbezüglich aktuell noch eher zurückhaltenden Schweizer KMU nicht entziehen können.

Interviewpartnerinnen und -partner

Folgende Personen haben sich freundlicherweise für die Interviews zur Verfügung gestellt (in alphabetischer Reihenfolge):

Daniel Binggeli
Chief Technology Officer und Mitglied der Geschäftsleitung
Puzzle ITC, Bern

Markus Blanka-Graff
Chief Financial Officer und Mitglied der Geschäftsleitung der Kühne + Nagel Gruppe
Kühne + Nagel International AG, Schindellegi

Claudia Dill
Group Chief Operating Officer und Mitglied der Geschäftsleitung SCOR
Verwaltungsrätin UBS Schweiz AG und Intix

Dirk Heinrichs
Head Internal Audit der Autoneum Gruppe
Autoneum Management AG, Winterthur

Mario Köpfli
Partner
iRisk GmbH, Zürich

Dr. Christian Russ
Dozent am Institut für Wirtschaftsinformatik
ZHAW School of Management and Law, Winterthur

Verweise

COSO – Commitee of Sponsoring Organizations of the Treadway Commission (2013). Internal Control – Integrated Framework: Framework and Appendices.

Economiesuisse (2023). Swiss Code of Best Practice for Corporate Governance.

EXPERTsuisse (2022), Schweizer Standards zur Abschlussprüfung (SA-CH).

EXPERTsuisse (2023). Schweizer Handbuch der Wirtschaftsprüfung, Band «Buchführung und Rechnungslegung» (Ausgabe 2023).

Pfaff, D., Ruud, F. (2020). Schweizer Leitfaden zum Internen Kontrollsystem (IKS) (8. Auflage). Orell Füssli Verlag.

Romeike, F. (2018). Risikomanagement. Springer Gabler.

Ruud, F., Friebe, P. (2013). Leitlinie zum Internen Audit (3. Auflage).

Vanini, U., Rieg, R. (2021). Risikomanagement (2. Auflage). Schäffer-Poeschel Verlag.

Autorenschaft

Prof. Dr. Gabriela Nagel-Jungo
Dr. oec. publ.
Leiterin des Instituts für Financial Management
ZHAW School of Management and Law, Winterthur

Jean-Marc Huber
Lic. rer. pol./eidg. dipl. Wirtschaftsprüfer
Dozent am Institut für Financial Management
ZHAW School of Management and Law, Winterthur

Roger Leu
Eidg. dipl. Wirtschaftsprüfer
Partner/Leiter Audit & Assurance Industrie Deutschschweiz
Forvis Mazars AG, Zürich

Marc Michely
Executive Director Audit & Assurance
Forvis Mazars AG, Zürich

Das Institut für Financial Management (IFI) der ZHAW School of Management and Law beschäftigt sich mit praxisrelevanten Fragen rund um die Rechnungslegung, Controlling, Auditing sowie Corporate Finance und Corporate Banking. Das Institut deckt in der Ausbildung (Bachelor- und Masterprogramme) und Weiterbildung sämtliche Themen aus dem Financial Management ab und forscht zu verschiedenen Aspekten der Themenschwerpunkte Accounting and Corporate Reporting, Corporate Performance and Sustainable Financing und Corporate Finance and Capital Markets. Zudem stellen die Expertinnen und Experten des Instituts ihr Wissen und ihre Erfahrungen im Rahmen von Beratungsmandaten in den Dienst der Auftraggeber.

Forvis Mazars Group SC ist ein unabhängiges Mitglied von Forvis Mazars Global, einem führenden Professional Services-Netzwerk. Als international integrierte Partnerschaft ist die Forvis Mazars Group in über 100 Ländern und Regionen der Welt tätig und auf die Bereiche Audit, Tax sowie Advisory spezialisiert. Die Partnerschaft greift auf die Expertise und das kulturelle Know-how von mehr als 35'000 Mitarbeitenden weltweit zurück, um Kundinnen und Kunden jeder Grösse in jeder Phase ihrer Entwicklung zu unterstützen. In der Schweiz arbeiten mehr als 400 Expertinnen und Experten an zehn verschiedenen Standorten.

Herausgeber

Forvis Mazars AG
Herostrasse 12
8048 Zürich

ZHAW School of Management and Law
Institut für Financial Management
Gertrudstrasse 8
Postfach
8401 Winterthur

Kontakt

Roger Leu
roger.leu@mazars.ch

Jean-Marc Huber
jean-marc.huber@zhaw.ch

Digitale Exemplare der Studie
www.forvismazars.com/ch
www.zhaw.ch/ifi


forvis
mazars
x
Zürcher Hochschule
für Angewandte Wissenschaften
zh
aw
School of
Management and Law