STEFAN HUNZIKER
PATRICK BALMER
MARCEL FALLEGGER

ENTERPRISE RISK MANAGEMENT BEI SCHWEIZER UNTERNEHMEN

Fünf zentrale Herausforderungen und Handlungsempfehlungen basierend auf einer aktuellen Studie

Obwohl viele Schweizer Unternehmen ein modernes Risikomanagement fördern, besteht in verschiedenen Bereichen Nachholbedarf. Der Beitrag zeigt fünf relevante Herausforderungen auf und liefert Handlungsempfehlungen für die Praxis. Die Erkenntnisse basieren auf dem neusten COSO-ERM-Rahmenkonzept und einer Risikomanagement-Studie in hiesigen Unternehmen.

1. EINLEITUNG

Risikomanagement befindet sich im Wandel und wird neu interpretiert. Die relativ unabhängige und oft historisch gewachsene Risikosteuerung, die Risiken separat in verschiedenen Unternehmensbereichen oder Kategorien betrachtet (sog. Silo-Risikomanagement), ist nicht mehr zeitgemäss. Trotzdem ist diese Form von nicht unternehmensweit implementiertem Risikomanagement in der Praxis immer noch zu beobachten [1].

Dieser traditionelle Ansatz wird heute immer mehr von einem modernen Risikomanagement *(Enterprise Risk Management [ERM])* abgelöst. Das Verständnis von modernem Risikomanagement nimmt eine ganzheitliche, strategiebezogene Sichtweise ein. Die verstärkte Berücksichtigung strategischer Risiken, die systematische Analyse von Abhängigkeiten zwischen Risiken sowie das unternehmensweite Balancieren von Rendite und Risiko bietet Unternehmen Chancen, stellt diese aber auch vor methodische Herausforderungen. ERM stellt Instrumente und Techniken zur Verfügung, die eine ausgewogene Betrachtung aller Risikokategorien zulassen und somit ein realitätsnahes Abbild der Chancen- und Risikolage im Unternehmen ermöglichen. Dadurch soll Unternehmen aufgezeigt werden, ob es sich in Anbetracht der Risiken lohnt, Chancen auszunutzen, und ob Unternehmenswerte geschaffen werden können. ERM bereitet Informationen auf, um strategische Entscheidungen fundierter treffen zu können.

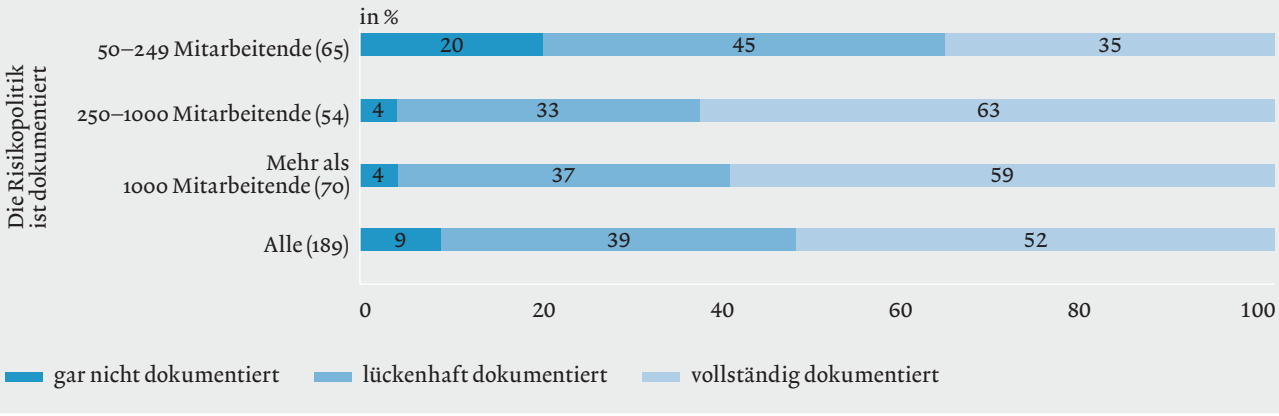
Diesem modernen Gedanken von Risikomanagement wird auch der Ansatz von COSO «Enterprise Risk Management – Aligning Risk with Strategy and Performance» gerecht [2], da er den Unternehmenswert hervorhebt und Anspruchsgruppen in den Mittelpunkt setzt. Dabei wird Risiko als ein mögliches Ereignis definiert, das sich positiv oder negativ auf ein Unternehmen auswirken und die Erreichung der Strategie und der Ziele beeinflussen kann. Des Weiteren wird unter ERM die unternehmensweite Identifikation, Bewertung, Steuerung, Berichterstattung und Überwachung von Risiken verstanden, um Werte für alle Anspruchsgruppen zu generieren.

Im September 2016 wurden 189 Unternehmen aus der Deutschschweiz mit mindestens 50 Vollzeitäquivalenten auf ihre ERM-Aktivitäten hin befragt [3]. Die Resultate wurden basierend auf den fünf eng miteinander verknüpften ERM-Komponenten aus dem COSO-Rahmenwerk-Entwurf analysiert. Im Folgenden werden fünf relevante Herausforderungen und entsprechende Handlungsempfehlungen basierend auf den Resultaten der Studie beschrieben. Diese stellen im Unterschied zu einem traditionellen Risikomanagement wesentliche Aspekte eines ERM dar. Dennoch zeigte die Studie auch, dass die befragten Unternehmen in einigen ERM-Bereichen bereits fortgeschritten sind. So misst die Mehrheit der Unternehmen der Verpflichtung zu Integrität und Ethik eine hohe Relevanz bei. Zudem weisen die Auswertungen auf einen angemessenen Einbezug von Chancen

STEFAN HUNZIKER,
PROF. DR. OEC. HSG,
INSTITUT FÜR
FINANZDIENSTLEISTUNGEN
ZUG (IFZ), HOCHSCHULE
LUZERN – WIRTSCHAFT,
ZUG

PATRICK BALMER,
M.A. HSG, DOKTORAND
UNIVERSITÄT ST. GALLEN,
WISSENSCHAFTLICHER
MITARBEITER, INSTITUT FÜR
FINANZDIENSTLEISTUNGEN
ZUG (IFZ), HOCHSCHULE
LUZERN – WIRTSCHAFT,
ZUG

Abbildung 1: **DOKUMENTATION DER RISIKOPOLITIK**



und Risiken beim Festsetzen von Zielen hin. Auch der Risikoinformationsfluss ist bei den meisten Unternehmen gut verankert.

2. FEHLENDE RISIKOPOLITIK UND MANGELHAFTE RISIKOKULTUR

In Abstimmung mit der Unternehmenspolitik bildet die Risikopolitik die Basis für den Aufbau des Risikomanagements. Es handelt sich dabei um die unternehmensinterne Festlegung, wie mit dem Thema Risiko umgegangen werden soll. Im Kontext der Risikopolitik wird unter den Mitarbeitenden das Risikobewusstsein gestärkt und vorgegeben, wie die Auseinandersetzung mit Risiken zu handhaben ist. Daraus kann das erwünschte Verhalten der Mitarbeitenden hergeleitet werden. Grundlage dazu bildet die interne Ausbildung und Kommunikation.

Risikomanagement-Kultur ist die beobachtete Umsetzung der Risikopolitik. Um diese zu fördern und dadurch das Risikobewusstsein in einem Unternehmen zu erhöhen, stellen vom Unternehmen vorgegebene, erwünschte Verhaltensweisen ein probates Mittel dar. Akzeptierte und nicht akzeptierte Verhaltensweisen werden in einem Verhaltenskodex festgelegt. Das erwartete Verhalten in Bezug auf den Umgang mit Risiken schafft Leitlinien zur Orientierung für die Mitarbeitenden.

Den Ergebnissen der Studie zufolge lässt sich bei den Unternehmen ein Aufholbedarf bei der Dokumentation der Risikopolitik identifizieren *(Abbildung 1)*. Nur rund die Hälfte kann eine formelle, schriftlich festgehaltene Risikopolitik vorweisen. Die andere Hälfte dokumentiert das gewünschte Verhalten nicht oder lediglich lückenhaft. Es muss festgehalten werden, dass auch 30% bis 40% der grösseren Unternehmen (250 oder mehr Mitarbeitende) die entsprechenden Vorgaben gar nicht oder lückenhaft dokumentiert haben.

Durch das Fehlen einer dokumentierten Risikopolitik haben die Unternehmen keine Grundauslegung für die Handhabung von Risiken im Unternehmen, womit sie einen zentralen Pfeiler für die Grundausrichtung des Risikomanagements vernachlässigen.

Ein Verhaltens- und Ethikkodex dient neben der Risikopolitik als wichtige Leitlinie für Mitarbeitende im Umgang mit Risiken. Ein entsprechender Kodex sollte genutzt werden, um das erwartete Verhalten und gleichzeitig die Verpflichtung des Managements zu Ethik und Integrität zu kommunizieren. Ebenso können ethische Unternehmenswerte vermehrt geschult werden, um Interpretationsspielraum zu vermeiden und ein gemeinsames Risikoverständnis zu etablieren. In der Praxis verspricht die Verwendung von guten Vorlagen oder Online-Tests sowie -Lerncentern mit attraktiven Inhalten, die von Mitarbeitenden individuell und zeitunabhängig genutzten werden können, einen Fortschritt.

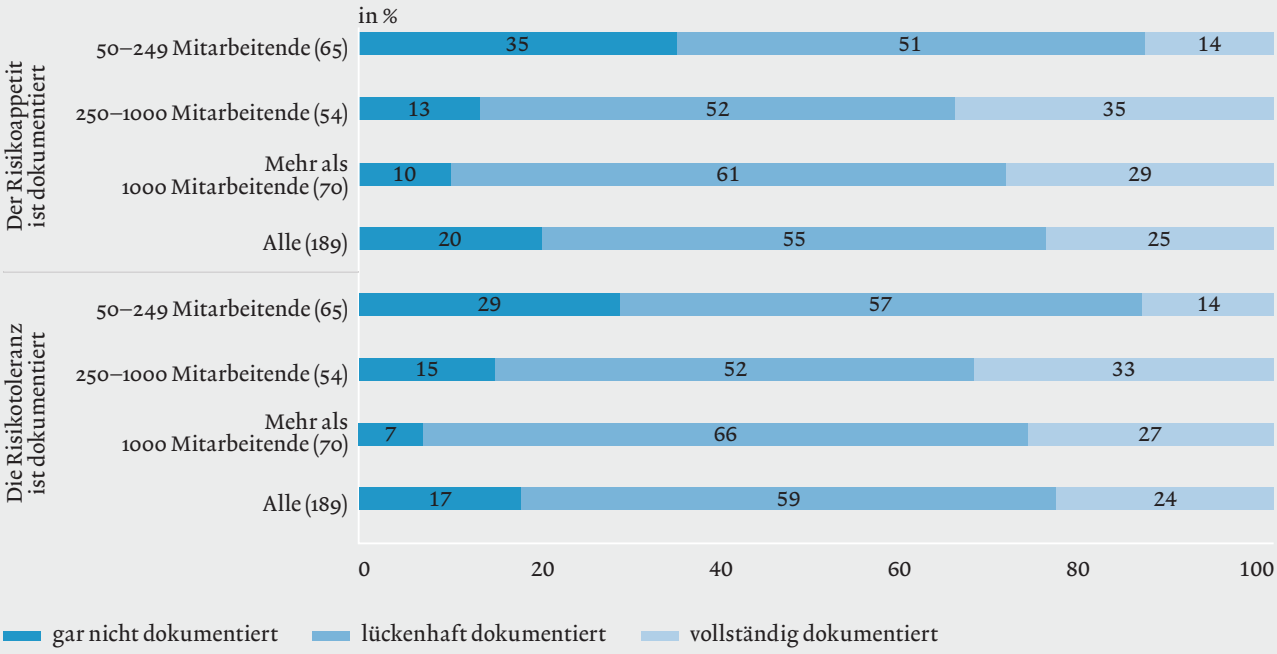
3. LÜCKENHAFTE DEFINITION DES RISIKOAPPETITS UND DER RISIKOTOLERANZ

Die Definition des Risikoappetits stellt die erste und wichtigste Aufgabe beim Aufbau eines Risikomanagements dar. Mit der Festlegung des akzeptierten gesamtunternehmerischen Risikoumfangs bestimmt das Unternehmen, wieviel Risiko es bereit ist einzugehen, um die damit verbundenen Chancen zu nutzen. Der Risikoappetit stellt diesbezüglich eine unerlässliche Zielgrösse für das Unternehmen dar. Er kann nicht berechnet werden, sondern ist eine bewusste Entscheidung der Unternehmensführung in Abstimmung mit den Anforderungen der Anspruchsgruppen.

Nicht zu verwechseln ist der Risikoappetit mit der Risikotoleranz. Letztere beschreibt das Maximum an Risiko, das ein Unternehmen tragen kann, ohne illiquide oder insolvent zu werden. Beispiele hierfür sind, wenn die gesetzlichen Auflagen nicht mehr erfüllt werden oder den Kunden- und Lieferantenverpflichtungen nicht mehr nachgekommen werden kann [4].

MARCEL FALLEGGER, MSC BANKING & FINANCE, CMA, WISSENSCHAFTLICHER MITARBEITER, INSTITUT FÜR FINANZDIENSTLEISTUNGEN ZUG (IFZ), HOCHSCHULE LUZERN – WIRTSCHAFT, ZUG

Abbildung 2: **DOKUMENTATION RISIKOAPPETIT UND -TOLERANZ**



Aus den Studienergebnissen geht hervor, dass bei einem Grossteil der Unternehmen der Risikoappetit nicht ausreichend dokumentiert ist *(Abbildung 2)*. Lediglich ein Viertel der Unternehmen weist den Risikoappetit vollständig aus. Das Festlegen der Risikobereitschaft scheint für Unternehmen aller Grössen eine komplizierte Aufgabe zu sein. Vor allem bei kleineren Unternehmen mit 50–249 Mitarbeitenden ist zu erkennen, dass lediglich ein geringer Teil den Risikoappetit dokumentiert hat. Dies ist problematisch, weil das Management das Eingehen von Risiken nicht an der maximal möglichen Risikokapazität reflektieren kann. Zudem fehlt die nötige Transparenz gegenüber den Anspruchsgruppen und dem entsprechenden Erwartungsmanagement.

Ähnlich sehen die Resultate bei der Dokumentation der Risikotoleranz aus. Drei Viertel der befragten Unternehmen belegen diese gar nicht oder nur lückenhaft. Obschon grössere Unternehmen leicht besser abschneiden als kleinere, ist auch bei ihnen die Erfassung der Risikotoleranz mangelhaft.

Der Risikoappetit soll als wichtiger Grundbaustein für das Eingehen von Risiken verständlich formuliert und festgehalten werden, um dem Management beim täglichen Umgang mit Entscheidungen eine klare Handlungsvorgabe zu geben. Der Appetit wird im Optimalfall als Kombination von Worten (z. B. als «gering» oder «mittel») und quantitativen Messgrössen formuliert. Dabei können maximal akzeptierbare Grenzen in Bezug auf den Unternehmenswert, das Umsatzwachstum, die Cashflow-Stabilität, den Gewinn pro Aktie oder die Reputation definiert werden. Der Risikoappetit ist abhängig von äusseren Veränderungen wie beispielsweise dem Marktumfeld und dem Wechselkurs und daher mindestens einmal jährlich zu überprüfen.

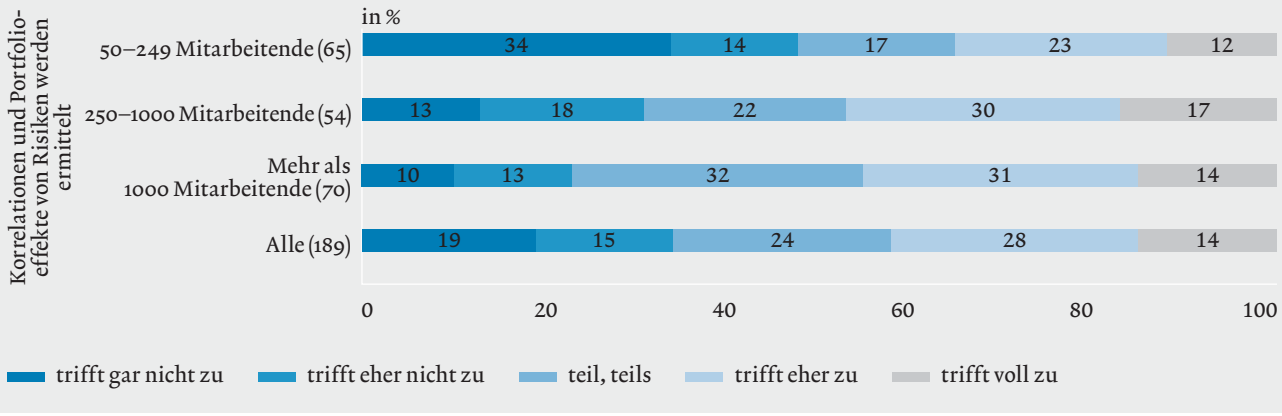
Die Risikoaggregation lässt die Bestimmung des Gesamtrisikoumfangs der Unternehmung zu – dieser muss unterhalb der Risikotoleranz einer Unternehmung liegen, um nicht in die Gefahr einer Illiquidität oder Insolvenz zu laufen. Der Gesamtrisikoumfang muss zudem regelmässig mit dem Risikoappetit abgeglichen werden und sollte diesen nicht übersteigen. Ansonsten müssten Massnahmen zur Reduzierung des Gesamtrisikoumfangs ergriffen werden.

4. FEHLENDE ERMITTLUNG VON ABHÄNGIGKEITEN UND PORTFOLIOEFFEKTEN

Eine der Hauptherausforderungen im Risikomanagement ist es, die «richtigen» risikogerechten Entscheidungen zu treffen, um die definierten Unternehmensziele zu erreichen. Dabei sind Unternehmen auf die Identifikation und Bewertung von Risiken angewiesen, wobei in der Praxis häufig die Eintrittswahrscheinlichkeit und das Schadensausmass herangezogen werden. Eine umfassende Risikoidentifikation und -bewertung beinhaltet auch die Betrachtung des Einflusses von Risiken auf gesamtunternehmerischer Ebene (Portfolioperspektive) respektive die Überprüfung von potenziellen Auswirkungen auf das Risikoprofil. Dadurch wird dem Management ermöglicht, die Auswirkungen und Abhängigkeiten der einzelnen Risiken im Gesamtkontext zu beurteilen. Dies ist dann von Bedeutung, wenn einzelne Risiken aufgrund eines Ereignisses gleichzeitig eintreten und nicht mehr als unabhängige Events beurteilt werden können.

In der Schweiz ermitteln lediglich 14% der befragten Unternehmen die Abhängigkeiten und Portfolioeffekte von Risiken *(Abbildung 3)*. Ungefähr die Hälfte bezieht die Wechselwirkung der Risiken teilweise oder mehrheitlich in ihre Risikobeurteilung ein. Bei einem Drittel entfällt die Ermittlung der gesamtunternehmerischen Risikoabhängigkeiten sogar komplett. Erstaunlicherweise schneiden Grossunterneh-

Abbildung 3: **ABHÄNGIGKEITEN UND PORTFOLIOEFFEKTE VON RISIKEN**



men (mehr als 1000 Mitarbeitende) unwesentlich besser ab als kleinere.

Der Grund hierfür könnte in der Schwierigkeit der Ermittlung der gegenseitigen Risikoeffekte in der Praxis liegen. Um die komplexe Analyse der Ursache-Wirkungs-Zusammenhänge nutzen zu können, muss der Risikomanagement-Verantwortliche über die entsprechenden Methodenkenntnisse verfügen. Unterstützung bieten können z. B. Szenarioanalysen, indem Ursache-Wirkungs-Ketten durchgedacht und diskutiert werden. Vorab muss sich ein Unternehmen aber gedanklich mit den potenziellen Effekten von Risiken auseinandersetzen, da sich der Effekt einzelner Risiken durch Wechselwirkungen verstärken bzw. vermindern kann.

«Im Zuge dieser Weiterentwicklung gilt es vermehrt, die Anschaffung einer softwaregestützten Risikomanagement-Lösung zu prüfen.»

5. SCHWACHE NUTZUNG VON INFORMATIONSSYSTEMEN

Damit ein Unternehmen Informationen für das Risikomanagement gezielt nutzen kann, müssen risikorelevante Daten aus internen und externen Quellen identifiziert, gesammelt und aggregiert dem Management in Form von Chancen und Risiken zur Verfügung gestellt werden. Auf diese Weise wird es möglich, transparente und klare Entscheidungen unter Berücksichtigung der Chancen- und Risikolage zu treffen. In Anbetracht der grossen Datenmengen ist es heutzutage zentral, mithilfe von Datenauswertungsmethoden die wesentlichen Informationen zu erkennen und diese zur richtigen Zeit den richtigen Personen zugänglich zu machen (so haben z. B. Prozessverantwortliche andere Risiko-Informationsbedürfnisse als Verwaltungsräte).

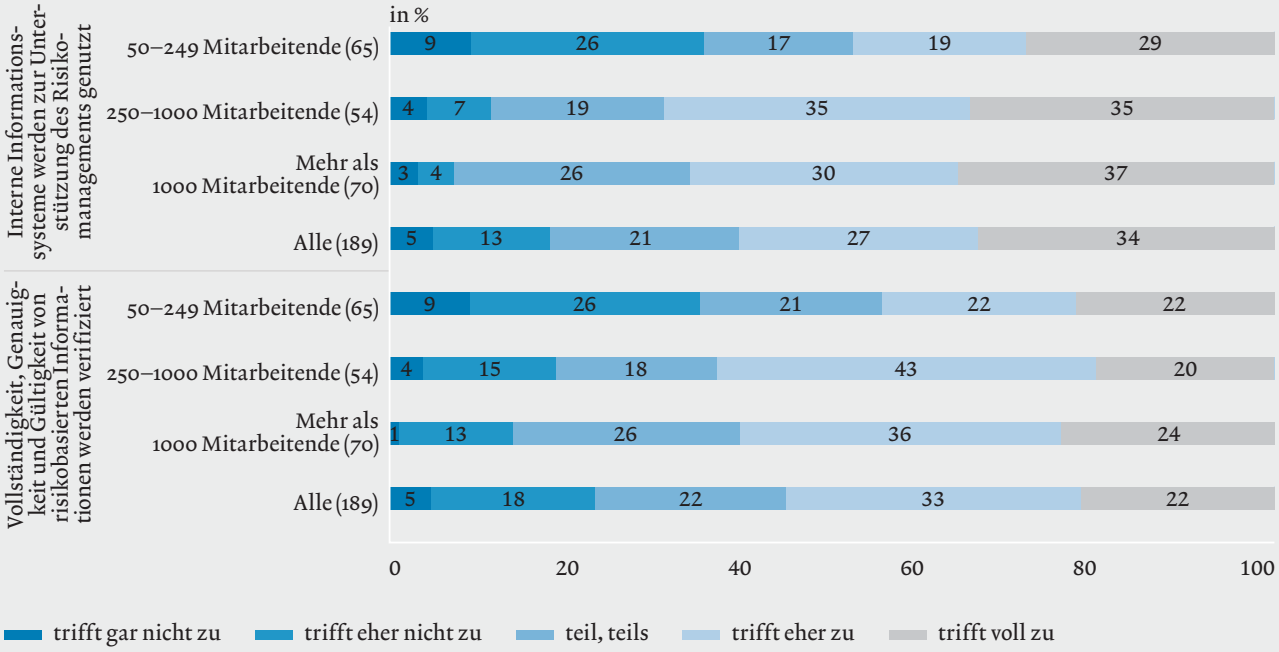
In dieser Hinsicht gewinnt das Informationsmanagement zunehmend an Bedeutung. Zur Unterstützung des Risikomanagements drängt sich hierfür die Nutzung von integrierten Informationssystemen auf. Letztere können den Risikomanager und weitere Funktionsträger im Risikomanagement beispielsweise durch die systematische und prozessorientierte Vorgehensweise bei der Sammlung von relevanten Daten (Identifikation) und der Verarbeitung zu aussagekräftigen Informationen (Analyse) unterstützen. Die Integration der Systeme erlaubt, zu einem späteren Zeitpunkt auch die Auswirkungen von relevanten Chancen und Risiken auf die Planzahlen des Unternehmens abzuleiten.

Da sich die Entscheidungsträger auf die entsprechende Risikoinformation verlassen müssen, spielen auch die angemessene Datenquantität und -qualität eine wichtige Rolle. Diese lassen sich danach beurteilen, ob die daraus generierten Informationen verfügbar, genau, angemessen, aktuell, verlässlich und vor Manipulation geschützt sind.

Die Studienergebnisse illustrieren, dass Informationssysteme mit der Fähigkeit, das Risikomanagement umfassend unterstützen zu können, noch zurückhaltend eingesetzt werden *(Abbildung 4)*. Nur 34% der befragten Unternehmen verlassen sich vollständig und 28% in einigen Teilbereichen auf interne Informationssysteme. Ferner besteht auch in Bezug auf das Informationsmanagement erhebliches Optimierungspotenzial. So prüft lediglich etwas mehr als ein Fünftel der Unternehmen die Qualität der risikorelevanten Informationen bzw. der entsprechenden Daten umfassend. Zumindest geben drei von vier Unternehmen an, die Vollständigkeit, Genauigkeit und Gültigkeit der Risikoinformationen wenigstens teilweise zu verifizieren.

Die Resultate lassen den Schluss zu, dass der systemgestützten Informationsversorgung und -verifizierung in der Praxis derzeit noch eine geringe Relevanz zukommt. In diesem Zusammenhang sind die erheblich schlechteren Werte von kleinen Unternehmen (weniger als 250 Mitarbeitende) auffallend. Mitunter könnte dies auf weniger umfangreiche und integrierte ERP-Lösungen zurückgeführt werden. Es ist davon auszugehen, dass mit zunehmender Unternehmensgrösse dem Ausbau und der Optimierung des Risikomanagements sowie den Informationssystemen ein grösserer Stellenwert zukommt.

Abbildung 4: **NUTZUNG VON INFORMATIONSSYSTEMEN**

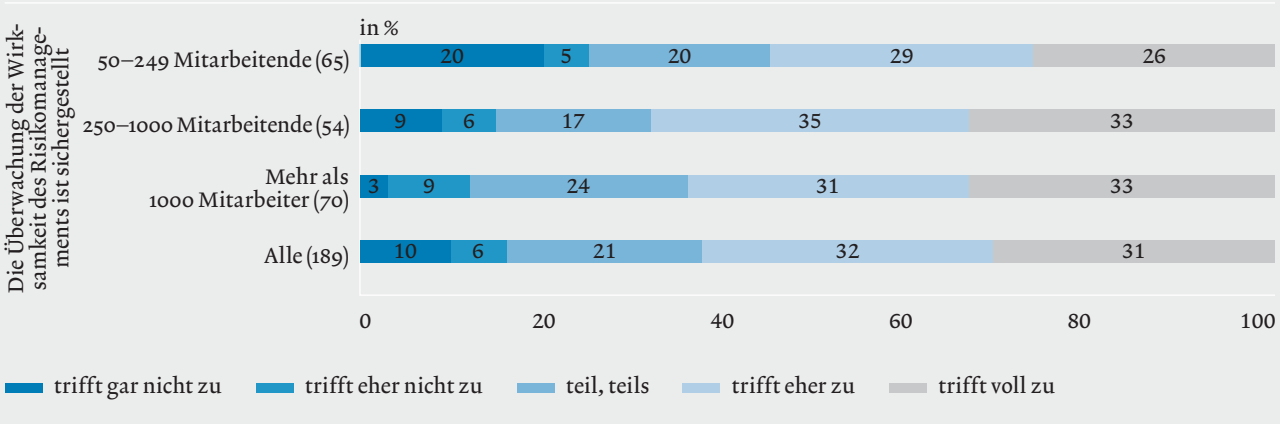


Im Zuge dieser Weiterentwicklung gilt es vermehrt, die Anschaffung einer softwaregestützten Risikomanagement-Lösung (oft unter RMIS bekannt) zu prüfen. Dadurch können Unternehmen einfacher detaillierte Analysen, realistische Simulationen sowie intelligente Prognoseverfahren umsetzen. Hierbei scheint es wesentlich, die Schnittstellen zu vorhandenen Systemen sorgfältig zu analysieren, um Beziehungen, beispielsweise mit den Finanzzahlen des Unternehmens, abbilden zu können.

6. FUNKTIONSFÄHIGKEIT (ZU) WENIG HINTERFRAGT

Das Bestreben der Überwachung liegt in erster Linie darin, zu beurteilen, ob die einzelnen Bestandteile des Risikomanagements ordnungsgemäss funktionieren. In diesem Zusammenhang soll auch überprüft werden, inwiefern das Risikomanagement die in der Risikopolitik definierten oder implizit verfolgten Risikoziele zu erfüllen vermag. Mit der regelmässigen Überprüfung eröffnet sich die Chance, die Wirksamkeit des Risikomanagements kontinuierlich zu verbessern. So sollen z. B. regelmässig der erwähnte Risikoappetit mit dem Risikoumfang abgeglichen oder die Methoden der Risikobewertung hinterfragt werden. Diese Überwachungstätigkeiten können durch das Management selbst, durch Unternehmensexterne oder durch beide erfolgen. Die Funktionsfähigkeit lässt sich schliesslich anhand des Ausmasses von unerklärbaren Abweichungen zwischen Plan- und Istwerten beurteilen (Schnittstelle zum Controlling). Je

Abbildung 5: **ÜBERWACHUNG DER WIRKSAMKEIT DES RISIKOMANAGEMENTS**



mehr solcher unerwarteten Abweichungen am Ende einer Berichtsperiode vorliegen, umso lückenhafter war die Risikoidentifikation. Weitere Indikatoren stellen die Qualität der Berichterstattung an den Verwaltungsrat sowie der Grad an Dokumentation dar.

Die Ergebnisse aus der Praxisstudie zeigen, dass bei ungefähr einem Drittel der Unternehmen die Überwachung der Funktionsfähigkeit des Risikomanagements vollständig sichergestellt ist *(Abbildung 5)*. Ein weiteres Drittel der Befragten behält die Wirksamkeit nur in Ansätzen im Auge. Bei den restlichen Unternehmen geben rund 17% an, dass die Überwachung gar keine oder lediglich eine geringe Aufmerksamkeit geniesst. Die Form und die Ausgestaltung der Überwachungsaktivitäten hängen mit grosser Wahrscheinlichkeit mit dem Reifegrad des Risikomanagements zusammen. Wenn formale Vorgaben für das Risikomanagement definiert und implementiert sind, werden die entsprechenden Tätigkeiten in Anbetracht von Kosten-Nutzen-Überlegungen eher überwacht.

Grössere Unternehmen (ab 250 Mitarbeitende) scheinen das Risikomanagement stärker zu überwachen als kleinere. Die Erfahrungen aus der Praxis bestätigen, dass kleinere Unternehmen aufgrund von Ressourcenengpässen einen geringeren Reifegrad aufweisen und daher die vereinzelten Risikomanagement-Komponenten nicht systematisch überprüfen. Zusammenfassend haben etwa 40% der Unternehmen noch (grossen) Aufholbedarf in Bezug auf die Überwachung der Wirksamkeit. Die Ausgestaltung des Risikomanagements sollte folglich noch stärker hinterfragt bzw. systematischer überprüft werden.

Damit die Überwachung zielführend erfolgen kann, werden Methoden- und Prozesskenntnisse vorausgesetzt. Eine erste Möglichkeit zur Verbesserung besteht darin, die Ergebnisse der Überwachung in die Berichterstattung zu integrieren (z. B. mit Informationen zur letzten Durchführung, Mängel, Massnahmenliste). Weiter kann das situative Beiziehen von externen Fachexperten helfen, Lücken in der Überwachung aufzudecken. Zuletzt kann auch die Etablierung eines Frühwarnsystems das Unternehmen dabei unterstützen, unerwünschte Entwicklungstendenzen zu erkennen. Massnahmenpläne lassen sich dann gemäss den Ergebnissen anpassen.

7. FAZIT

Risikomanagement befasst sich mit der Zukunft, d. h. mit möglichen Ereignissen, die heute noch keine Realität darstellen. Gleichzeitig gilt es zu beachten, dass auch ein fortschrittliches und umfassendes Risikomanagement künftige Ereignisse weder zu beeinflussen noch vorauszusagen vermag. Es kann Unternehmen aber dabei unterstützen, potenziell erfolgskritische Szenarien frühzeitig zu antizipieren. Folglich lassen sich Entscheidungen verbessern, indem deren Konsequenzen sichtbar gemacht werden.

Erfreulicherweise zeigen die Ergebnisse der vorgestellten Studie, dass die meisten befragten Unternehmen der Abwägung von Chancen und Risiken bei der Prüfung von alternativen Strategien genügend Beachtung schenken. Trotzdem veranschaulichen die genannten Herausforderungen, dass noch erhebliches Potenzial besteht. Besonders die vermehrte Definition von risikopolitischen Grundsätzen kann dabei helfen, die Verantwortlichkeiten und das Risikobewusstsein zusätzlich zu verbessern. In Bezug auf die Risikoanalyse müssen Abhängigkeiten noch gezielter in die Risikobeurteilung einfliessen. Zur Verbesserung der Information und Dokumentation drängt sich die verstärkte Nutzung von Risikomanagement-Informationssystemen auf. Dadurch würde im Rahmen der Überwachung auch der Abgleich zwischen dem Risikoappetit und dem Risikoumfang begünstigt.

Anmerkungen: 1) Vgl. Hunziker, S. & Meissner, J. O. (2017). Risikomanagement in 10 Schritten. Wiesbaden: Springer Fachmedien. **2)** Vgl. Committee of Sponsoring Organizations of the Treadway Commission, COSO (Hrsg.); (2016). Enterprise Risk Management – Aligning Risk with Strategy and Performance. Public Exposure. June 2016 Edition. Online (17. Oktober 2016): erm.coso.org/Documents/COSO-ERM-Public-Exposure.pdf. **3)** Vgl. Hunziker, S., Balmer, P., Schellenberg C. (2016). Enterprise Risk Management 2016. Studie zum Risikomanagement in Schweizer Unternehmen. Zug: Swiss ERM und IFZ – Hochschule Luzern. **4)** Vgl. Hunziker, S., Meissner, J. O. (2017). Risikomanagement in 10 Schritten. Wiesbaden: Springer Fachmedien.