

# Enterprise Risk Management

## Paradigmenwechsel im Risikomanagement

Das Enterprise Risk Management (ERM) ist ein wesentlicher Bestandteil der unternehmensinternen Corporate Governance. Es unterstützt die Organisation bei der Identifikation, objektiven Beurteilung und aktiven Steuerung der wesentlichen Unternehmensrisiken und schafft damit Sicherheit und Planbarkeit unter anderem für die Geschäftsleitung und den Verwaltungsrat.

Aufgrund der Pandemie-Situation der letzten 18 Monate nahmen jedoch die strategischen, operativen, finanziellen und organisatorischen Unsicherheiten für die Geschäftsleitungen und die Verwaltungsräte überproportional zu. Das bestehende und in der Organisation meist fest institutionalisierte, aber teilweise etwas restaurative ERM-Rahmenwerk konnte hierzu kurzfristig nur begrenzt Antworten oder Orientierung bieten, z.B. bezüglich der Ausrichtung oder zeitlichen Materialisierung von Risiken.

In diesem Artikel zeigen wir auf, dass diese fehlende, zeitnahe Ausrichtung nur wenig mit der Frage zu tun hat, ob pandemierelevante Risiken Bestandteil des zentralen Risikokatalogs waren oder nicht. Vielmehr diskutieren wir Ansätze eines generellen Paradigmenwechsels, der sich stärker auf Ursache-Wirkung konzentriert und weniger auf die detailgetriebene Genauigkeit bei der Bewertung von Risiken.

### Aktuelle Erhebung zur Risikosituation und Pandemiebereitschaft bei Schweizer Unternehmen

Eine aktuelle Umfrage des Instituts für Finanzdienstleistungen (IFZ) hat aufgezeigt, dass lediglich 46 Prozent der befragten Risikoverantwortlichen das Pandemierisiko teilweise oder vollumfänglich im Risikokatalog integriert bzw. auf dem Risikoradar überwacht hatten.<sup>1</sup> Erfahrungen aus unseren Kundengesprächen bezüglich der Ableitung von geeigneten, zeitnahen Massnahmen auf die kurzfristigen Pandemieherausforderungen bestätigten diesen Eindruck zusätzlich.<sup>2</sup>

Die IFZ-Studie ergab zudem, dass Organisationen, die sich des Risikos einer Pandemie bewusst waren und diese entsprechend in ihrem Risikokatalog aufführten, in erster Linie operative Gegenmassnahmen auf folgenden Gebieten festgelegt hatten: Sicherstellung einer zeitnahen Verfügbarkeit von Desinfektionsmitteln, dokumentierter und erprobter/getesteter Pandemieplan, regelmässige Krisenübungen und dokumentiertes Notfallkonzept für mögliche Grippewellen, welche die Belegschaft des Unternehmens betreffen.

<sup>1</sup> ERM Report 2020 «Die Rolle der Risk Manager in der COVID-19-Krise»; Hunziker et al. (2020:34); <https://hub.hslu.ch/financialmanagement/2020/11/05/erm-report-2020/>

<sup>2</sup> «Perception of key and emerging risks»; Zupan (2020); (<https://home.kpmg/ch/de/blogs/home/posts/2020/12/ia-after-covid-emerging-risks.html>)





Die Mehrheit der Unternehmen hatte hingegen in ihrer Risk-Map keine spezifischen Risiken im Zusammenhang mit potenziellen Pandemien dargestellt. Ebenso fehlte es an spezifischen Massnahmen zu deren allfälligen Eindämmung bzw. an der Definition und Zuordnung von Rollen und Verantwortlichkeiten innerhalb der Organisation im Falle eines Ausbruchs. Die Überlegung und Argumentation hinter diesem Vorgehen waren hauptsächlich auf folgenden Prämissen aufgebaut:

1. Das Eintreten einer derart folgenschweren Lage ist äusserst unwahrscheinlich.
2. Selbst wenn eine solche Lage eintreten sollte, bleibt noch genügend Zeit für die Einleitung von Vorbereitungsmaßnahmen.
3. Das Pandemierisiko ist ein «schwarzer Schwan», dessen Kosten-Nutzen-Aufwand nicht in Relation zur Eintrittswahrscheinlichkeit steht.

### **Unternehmerische Reaktionen und Antworten auf die Pandemiemassnahmen**

Die vergangenen 12 bis 18 Monate haben einerseits gezeigt, dass die meisten Regierungen von der Geschwindigkeit und den Auswirkungen der Pandemie auf die Gesellschaft, die Wirtschaft und die Infrastruktur überrollt wurden.

Andererseits reagierten die Unternehmen im Allgemeinen zeitnah, proaktiv und konzentrierten sich auf die umgehende Adaption ihrer unternehmerischen Prozesse an die aktuelle Lage (nicht zuletzt auch dank der staatlichen Massnahmen zur Abfederung der allgemeinen wirtschaftlichen Belastung durch die Pandemie in Form von Kurzarbeitsentschädigung, Hilfskrediten, Subventionen etc.).

Es zeigte sich, dass die Unternehmen rasch und flexibel auf die neuen Arbeitsbedingungen reagieren konnten.

Ein paar Beispiele dazu sind:

- Lockdown: Während des Büro-Lockdowns ermöglichten bzw. entwickelten die internen IT-Funktionen schnell und effektiv Instrumente für die Arbeit im Homeoffice.
- Als die internationalen Handels- und Versorgungswege geschlossen wurden, erschlossen sie alternative Beschaffungswege (wenn auch teilweise zu wesentlich höheren Logistik- bzw. Beschaffungskosten).
- Um temporär geschlossene Fabriken und Betriebsstätten wieder zu öffnen, adaptierten Produktionsunternehmen ihre Beschaffungs-, Produktions- und Belieferungsplanung (z.B. in Form von Schichtarbeit).<sup>3</sup>
- Den Mitarbeitenden wurden die notwendigen Instrumente und Ressourcen (z.B. Computer) für das Homeoffice zur Verfügung gestellt.

Zusammenfassend lässt sich sagen, dass die übergreifenden Infrastrukturen der Schweiz grosse Herausforderungen mit massiven Folgen auf staatlicher, unternehmerischer und privater/persönlicher Ebene zu meistern hatten. Gleichzeitig agierten die Schweizer Unternehmen überraschend flexibel und passten sich rasch an die neue Situation an.

Der beste Beleg für diese Anpassung ist die Tatsache, dass die Schweizer Wirtschaft im zweiten Quartal 2020 zwar spürbar einbrach, diesen Rückstand im dritten Quartal jedoch in einem gewissen Ausmass aufzuholen vermochte. Wirtschaftswissenschaftlern zufolge dürfte die Schweizer Wirtschaft Ende 2021 gar erneut ihr Vorkrisenniveau erreicht haben.

### **Wahrnehmung der Aufsichtsfunktion bezüglich der Tragweite der Pandemie**

Wie oben ausgeführt, konnten die kurzfristigen Anpassungen des Arbeitsumfelds (d.h. Standort, Präsenz am Arbeitsplatz, Einsatz von digitalen Kommunikations-Tools, um vernetzt zu bleiben) äusserst effizient und wirksam umgesetzt werden.

Offen blieben aber insbesondere Fragen hinsichtlich der nachhaltigen Aufrechterhaltung der Corporate Governance, der Kontrollrahmenwerke und der wesentlichen Geschäftsprozesse sowie der möglichen Auswirkungen aufgrund kurzfristiger Anpassungen und Veränderungen.

<sup>3</sup> März 2020 bis Juni 2020; Dezember 2020 bis Mai 2021

Die Grundprämisse der Unternehmen bestand darin, ihren Betrieb nach Möglichkeit nicht zu unterbrechen und die Geschäftstätigkeit so effizient wie möglich fortzuführen. Die Auswirkungen auf die Kontroll- und Überwachungssituation (Stichwort: interne Kontroll- und Überwachungssysteme) sollten dabei vorerst nicht bzw. nur als sehr niedrige Priorität berücksichtigt werden.

Rückblickend lässt sich dieses Vorgehen hauptsächlich dadurch erklären, dass die Unternehmen zwar über leicht umzusetzende Notfallpläne für kurzfristige, aussergewöhnliche Umstände verfügten, potenziell länger andauernde Anomalien in den Geschäftsprozessen in diesen Plänen jedoch nicht berücksichtigt wurden. Man ging davon aus, dass sich die Lage in ein bis zwei Wochen «normalisieren» würde.

Dies war eindeutig nicht der Fall – in gewissen Unternehmen dauert die auf wenige Wochen ausgelegte Ausnahmesituation bis heute an. Die direkte Konsequenz aus dieser neuen «Abnormalität» war, dass die internen Corporate Governance- und Kontroll-Regelwerke der meisten Unternehmen die effektiven Abläufe zu einem wesentlichen Teil risikotechnisch nicht mehr überwachen bzw. kontrollieren konnten.

Die Beurteilung von Ursache und Wirkung gestaltete sich nicht ausreichend transparent und die Interdependenzen der einzelnen Risiken waren für die Verantwortungsträger (z.B. VR, AC, GL) nur sehr bedingt nachvollziehbar. Beispiele dazu sind:

1. Aufgabentrennung und -effektivität: Manuelle Kontrollen im Rahmen der Prüfung und Genehmigung von Transaktionen, erfolgen neu virtuell. Die Arbeit im Homeoffice bringt es unter Umständen mit sich, dass diese Kontrollen und Prozesse mehr Zeit in Anspruch nehmen bzw. nicht mehr ausreichend aufgeteilt werden können (Stichwort: Segregation of duties).
2. Wichtige Dokumente (z.B. Verträge oder Bestellungen), die einer qualifizierten Unterschrift bedürfen, können nicht mehr persönlich an die zuständigen, internen Funktionen übergeben werden. Stattdessen muss entweder ein zeit- aufwändiger Kurierdienst in Anspruch genommen oder auf elektronische Unterschriftskopien zurückgegriffen werden, die in den meisten Fällen nicht ordnungsgemäss zertifiziert/ beglaubigt sind.<sup>4</sup>



3. Budgetierungs- und Prognoseverfahren für die kommenden Perioden müssen unter völlig anderen Gesichtspunkten (alternative Treiber und Annahmen) durchgeführt werden, während Nachfrage-, Angebots- und Konjunkturprognosen hochgradig unsicher sind.
4. Neu eingerichtete, staatliche Zuschüsse und Unterstützungen bei Kurzarbeit, die den Unternehmen auf Antrag zur Verfügung gestellt werden, unterliegen klar festgelegten Vorschriften und Regulierungen, die für die Unternehmen zum Teil nicht vollständig nachvollziehbar sind oder deren langfristige Auswirkungen und Folgen nicht absehbar erscheinen (z.B. Einschränkung der Flexibilität aufgrund von Anpassungen des Personalbestands an die neue Nachfragesituation).

**Kurz:** Die Ursachen und Wirkungen der mittel- und langfristigen Einflüsse der Pandemie auf das Risiko- und Corporate Governance-Profil der einzelnen Unternehmen waren gezwungenermassen unklar bzw. liessen sich kaum realistisch abschätzen. Der Verwaltungsrat, als oberstes Aufsichtsgremium eines Unternehmens, sah sich gezwungen, die Organisation und deren Prozesse risikobezogen zu beaufsichtigen und zu steuern, ohne über ausreichend transparente Angaben zu Ursachen und Wirkungen zu verfügen.

### **Welche ERM-Lektionen lassen sich auf Verwaltungsrats- und Geschäftsleitungsebene lernen?**

Als Fazit und Empfehlung sollten der Verwaltungsrat und die Geschäftsleitung verlangen, dass das ERM ganzheitlicher und zukunftsorientierter ausgerichtet wird. Die Risiken sind in Bezug auf gegenseitige Abhängigkeiten, die Zeitvariable (d.h. die Zeitspanne zwischen der Identifikation und dem Eintreten eines Risikos) sowie im Kontext von potenziellen Abwehrstrategien (d.h. Strategie zur Risikovermeidung) transparenter und holistischer zu betrachten.

Letztendlich sollte das ERM zudem nicht den Ist-Zustand des betreffenden Unternehmens, sondern dessen möglichen Zustand in der nahen, mittelfristigen und langfristigen Zukunft einschätzen bzw. beurteilen und daraus die Auswirkungen auf die Risikosituation des Unternehmens ableiten (im Sinne von Ursache und Wirkung von strategischen Entscheidungen und deren Umsetzung).

<sup>4</sup> Die Erfahrung hat gezeigt, dass die meisten Unternehmen noch nicht über ein elektronisches/digitales Unterschriftenverfahren verfügten, bzw. die elektronische Unterschrift noch keine offizielle Beglaubigung besitzt.





Weiter sind die ERM-Verantwortlichen besser in Bezug auf die Erkennung von «schwarzen Schwänen» zu schulen. Der Begriff von «schwarzen Schwänen» bezeichnet dabei potenziell auftretende Risiken, welche die Organisation nicht auf ihrem Radar hat und für deren Behebung oder Minderung auch keine Strategien oder Notfallpläne ausgearbeitet wurden. Derartige Risiken, die als nicht prognostizierbar und unwahrscheinlich gelten, haben jedoch eine wesentliche Wirkung auf das Unternehmen.

Die zuständigen Aufsichtsorgane des Unternehmens (VR, AC), sollten hierzu klar die Erwartung äussern, dass das ERM mindestens einmal jährlich seinen Horizont um potenzielle Bedrohungen und Chancen erweitert, die heute aufgrund ihrer Distanz (noch) nicht relevant für das Unternehmen sind, morgen aber massive Folgen nach sich ziehen könnten.

Ferner sollte sich das ERM nicht ausschliesslich auf die Beurteilung/Validierung von potenziellen Ereignissen konzentrieren, die sich möglicherweise auf das Unternehmen auswirken, sondern diese Auswirkungen im Rahmen einer grundlegenden Ursachenanalyse weitergehend analysieren.

Konkret bedeutet dies, dass der Verwaltungsrat mittels ERM einen Einblick in potenziell neu auftretende Risiken erhält und diese nicht nur im individuellen, singulären Kontext betrachtet, sondern auch Überlegungen dazu anstellt, wie derartige Ereignisse sich allenfalls auf andere Unternehmensrisiken auswirken können (Stichwort: Schneeballeffekt) bzw. welche Strategien eine effektive und effiziente Option für die Risikobewirtschaftung bieten.

Beispielsweise hatte eine singuläre Betrachtung des Pandemie-risikos kaum dazu beigetragen, den Aufsichtsorganen des Unternehmens die nötige Sicherheit über den Zustand des Unternehmens zu geben, da die Fragen nach den potenziellen Auswirkungen auf den Geschäftsgang, die Organisation, die Prozesse sowie die mittelfristigen Governance- und Kontroll-Regelwerke vorwiegend vage oder ganz offen blieben.

Für die Zukunft empfiehlt es sich, dass der Verwaltungsrat/ das Audit Committee die klassischen Risikolandkarten, welche die Risiken in Form von Auswirkungen und Wahrscheinlichkeiten sehr rudimentär darstellen, nachdrücklich in Frage stellt.

Anstelle derartiger Kartierungen sind gegenseitige Abhängigkeiten, Zeitfaktoren und Reaktionsstrategien für Schlüsselrisiken in die Betrachtungen aufzunehmen, sodass der Verwaltungsrat in der Lage ist, die Tragweite der Auswirkungen besser nachzuvollziehen und zu hinterfragen, ob in der verbleibenden Vorbereitungszeit die Geschäftsleitung angemessene Massnahmen ins Auge gefasst hat.

### **Suche nach neuen ERM-Kompetenzen**

Diese Entwicklungen werden sich auch auf das Anstellungsprofil des Risikomanagers auswirken. Bis anhin lag der Fokus hauptsächlich auf der Beurteilung von internen, finanziellen, betrieblichen und Compliance-bezogenen Risiken bezüglich Eintrittswahrscheinlichkeit und Auswirkung. Diese wurden identifiziert und in die Beurteilung der bestehenden Unternehmensstrukturen und -prozesse sowie der Governance einbezogen.

Neu muss ein Risikomanager die langfristigen, strategischen und operativen Entwicklungen des Unternehmens genau verstehen, um daraus jene möglichen Ereignisse abzuleiten, die sich grundlegend auf die Organisation auswirken können. Der ERM-Verantwortliche muss in der Lage sein, die Komplexität, Vielschichtigkeit und Interdependenz von Ereignissen erfolgreich in einer Risikomanagement-Perspektive miteinander zu verknüpfen.

In dieser Rolle müssen Risikomanager nachvollziehen können, wie sich der Strategieprozess des Unternehmens gestaltet und wie mittelfristige Ziele im Rahmen des Planungsprozesses festgesetzt und operationalisiert werden. Zugleich müssen sie die Auswirkungen von neuen Geschäftsmodellen oder Änderungen der Organisation und ihrer Prozesse aus dem Blickwinkel von Risiken und Chancen erfassen können.

---

## Fazit

Die Pandemie der letzten 18 Monate hat gezeigt, dass Unternehmen mit der Materialisierung von Risiken rechnen müssen, die sie vorher nicht als wesentlich bzw. gar nicht wahrgenommen haben.

Die Risikomanager müssen dabei ihre Tätigkeit als Risikoüberwacher innerhalb des Unternehmens agiler und flexibler angehen. Bei der Methodologie sollte weniger Zeit für die Analyse bestehender Risiken aufgewendet und stattdessen die Suche nach neuen Eventualitäten «am Horizont» intensiviert werden.

**Wichtiger noch:** Die Definition und die Umsetzung von Massnahmen sollten verstärkt aus einer auf Ursachen und Wirkungen gerichteten Perspektive und einer anhaltenden holistischen Risikobetrachtung erfolgen. Sprich: Der Blickwinkel sollte sich nicht einzig und allein auf Wahrscheinlichkeiten und Auswirkungen beschränken, sondern ebenso auf Zeitfaktoren/ Reaktionszeit und Abhängigkeiten bzw. Wechselbeziehungen von möglichen Risiken fokussieren sowie die Beurteilung der geplanten Massnahmen zur Risikovermeidung inkludieren (Stichwort: Brutto- vs. Nettobetrachtung).

Themen wie die «Risikoidentifikation» und die «Risikominderung» sollten höher gewichtet werden als die Frage, wie ein bestimmtes Risiko bezüglich der Wahrscheinlichkeitsausprägung einzustufen ist (z.B. «äusserst wahrscheinlich» versus «sehr wahrscheinlich»).

Klar definierte strategische Massnahmen zum Umgang mit Risiken (d.h. Risikoübertragung, Risikovermeidung, Tragen von Risiken oder Risikominderung/Gegenmassnahmen) sollten die konsolidierte Risikoperspektive prägen und dem Risikomanager Möglichkeiten bieten herauszufinden, ob ein bestimmtes Risiko mehrdimensionale Abhängigkeiten haben kann. So wirkt sich z.B. das Pandemierisiko auf organisatorische Massnahmen aus, die wiederum Auswirkungen auf die Kontrolle und Governance haben, welche ihrerseits Auswirkungen auf die kurzfristige Planung haben, wobei Letztere sich auf die wirtschaftliche Wachstumsstrategie auswirkt, die Folgen hat für ... etc.

Ferner sollten Risikomanager auf die effektive Umsetzung der Massnahmen zum Umgang mit Risiken pochen, d.h. wiederkehrend nachfragen, ob die entsprechenden Pläne und Massnahmen konkretisiert und umgesetzt wurden.



### Luka Zupan

Partner, Head Internal Audit, Risk and Compliance Services (IARCS)  
KPMG Schweiz

+41 58 249 36 61  
lzupan@kpmg.com

---

Dieser Artikel ist Bestandteil der KPMG Board Leadership News. Um diesen Newsletter für Verwaltungsrätinnen und Verwaltungsräte dreimal pro Jahr zu erhalten, können Sie sich [hier registrieren](#).

## Über das KPMG Board Leadership Center

Das KPMG Board Leadership Center ist unser Kompetenzzentrum für Verwaltungsrätinnen und Verwaltungsräte. Mit vertieftem Fachwissen und neusten globalen Kenntnissen unterstützen wir Sie in Ihren aktuellen Herausforderungen, damit Sie Ihre Rolle höchst effektiv erfüllen können. Zusätzlich bieten wir Ihnen die Möglichkeit, mit Gleichgesinnten in Kontakt zu treten und sich auszutauschen.

Erfahren Sie mehr unter [kpmg.ch/blc](https://kpmg.ch/blc)

---

Die hierin enthaltenen Informationen sind allgemeiner Natur und beziehen sich daher nicht auf die Umstände einzelner Personen oder Rechtsträger. Obwohl wir uns bemühen, genaue und aktuelle Informationen zu liefern, besteht keine Gewähr dafür, dass diese die Situation zum Zeitpunkt der Herausgabe oder eine künftige Situation akkurat widerspiegeln. Die genannten Informationen sollten nicht ohne eingehende Abklärungen und professionelle Beratung als Entscheidungs- oder Handlungsgrundlage dienen. Bei Prüfkunden bestimmen regulatorische Vorgaben zur Unabhängigkeit des Prüfers den Umfang einer Zusammenarbeit. Sollten Sie mehr darüber erfahren wollen, wie KPMG AG personenbezogene Daten bearbeitet, lesen Sie bitte unsere Datenschutzerklärung, welche Sie auf unserer Homepage [www.kpmg.ch](https://www.kpmg.ch) finden.

© 2021 KPMG AG, eine Schweizer Aktiengesellschaft, ist eine Tochtergesellschaft der KPMG Holding AG. KPMG Holding AG ist Mitglied der globalen KPMG-Organisation unabhängiger Firmen, die mit KPMG International Limited, einer Gesellschaft mit beschränkter Haftung englischen Rechts, verbunden sind. Alle Rechte vorbehalten.