Struktur-Optimierungen

Synergien im Risikomanagement

Wenn mehrere Personen über den Inhalt von Risikomanagement in Organisationen diskutieren, entsteht schnell ein Konsens über die Anwendung des Risikomanagement-Prozesses (Rahmenbedingungen, Risikoidentifikation, Analyse, Bewertung, Bewältigung usw.). Schwieriger wird es, wenn es um die Zuordnung einzelner Anwendungen des Risikomanagements und die eigentliche organisationale Synergie geht.

Bruno Brühwiler

Unter dem Dachbegriff Risikomanagement werden gut und gerne auch ERM (Enterprise Risk Management), auch Teilbereiche wie IKS (Internes Kontrollsystem), BCM (Business Continuity Management), CMS (Compliance Management), QMS (Qualitätsmanagement), SMS (Sicherheitsmanagement) usw. untergeordnet. Leider bestehen unterschiedliche Wahrnehmungssilos.

Eine zu einfache, aber kaum realisierbare Lösung würde darin bestehen, dass man das Risikomanagement als Oberbegriff nutzt, um alle anderen Teilbereiche darin zu integrieren. Ein «Total-Risikomanagement» ist in der IT-Realität jedoch schwierig zu implementieren, weil jeder Teilbereich eine andere Zielsetzung verfolgt, spezifische Inhalte umfasst, fachlich ungleiche Anforderungen stellt, einen anderen Geltungsbereich aufweist oder eine andere Methodik zeigt.

Wie können aufwendige Überschneidungen und Ressourcen-Verschwendungen anstelle von Synergien und Vereinfachungen vermieden werden?

Die nachfolgenden Ausführungen verfolgen zwei Ziele: Erstens Geltungsbereiche und Schnittstellen der Anwendungsgebiete von Risikomanagement klären; zweitens konzeptionelle Lösungen aufzeigen, um Doppelspurigkeiten zu vermeiden und Vereinfachungen herbeizuführen.

Risikomanagement und Unterbereiche

Organisationen setzen Risikomanagement als Führungsinstrument ein. Dies tun nicht nur private Unternehmen, sondern zunehmend auch öffentliche Institutionen und Verwaltungen. Risikomanagement wird teilweise gesetzlich vorgeschrieben. Bei der Umsetzung gelangen Standards wie die internationale Norm «ISO 31000 Risk management – Guidelines» oder das amerikanische «COSO Enterprise Risk Management Framework» zur Anwendung. Risiko wird als «Auswirkung von Unsicherheit auf Ziele, Tätigkeiten und Anforderungen» definiert.

Die Risikomanagement-Standards sind auf alle Organisationen, alle Entscheidungssituationen und alle Unternehmensprozesse anwendbar. Oft spricht man von «Unternehmens-Risikomanagement» oder von «Enterprise Risk Management (ERM).

Risikomanagement im weiteren Sinn umfasst viele Unterbereiche, die ähnlich, aber doch anders sind. Hier finden Sie die wichtigsten Bereiche:

– *Im Compliancemanagement (CMS)* geht es darum, dass sich die Organisation an Gesetze, an regulatorische Vorschriften, an relevante Normen und Richtlinien hält. Gemäss der internationalen Norm ISO 19600 soll das Compliancemanagement «risikobasiert» gestaltet werden. Dies bedeutet, dass vor allem diejenigen Gesetze und Vorschriften von hoher Bedeutung sind, deren Nicht-Einhalten für die Organisation zum (negativen) Risiko wird.

– *Im Internen Kontrollsystem (IKS)* sollen Kontrollen (4-Augen-Prinzip, Stichproben, Systemkontrollen usw.) sicherstellen, dass die finanzrelevanten Prozesse korrekt ablaufen, was zu einer fehlerfreien finanziellen Berichterstattung führen soll.

Zusätzlich stehen die sorgfältige Verwendung von Finanzmitteln, die Verhinderung von Betrug und Schadenfällen im Fokus. Interne Kontrollsysteme befassen sich auch mit der Einhaltung von gesetzlichen Vorschriften und internen Weisungen, wobei darauf zu achten ist, dass es keine Überschneidungen bzw. Doppelspurigkeiten mit dem Compliancemanagement gibt.

– *Im Notfall-, Krisen- und Kontinuitätsmanagement* (das in der angelsächsischen Welt mit Business Continuity Management / BCM bezeichnet wird) geht es darum, dass die Organisation nach eingetretenen schweren Schadenfällen richtig reagiert und Massnahmen vorbereitet, um die unterbrochenen Betriebsfunktionen rasch wieder zurückzugewinnen.

Um die neuralgischen Stellen in der Organisation zu finden, die besonders kritisch für die Gewährleistungen der operationellen Prozesse sind, wird z.B. in der ISO 22301 empfohlen, eine Business-Impact-Analyse durchzuführen, was eine direkte Verbindung zum Risikomanagement-Prozess schafft.

– *Im Bereich der Informationssicherheit beim Umgang mit IT-Systemen* kommt es darauf an, dass die Verfügbarkeit, die Integrität und der Schutz der Daten gewährleistet sind. Die internationalen Normen ISO 27001 und ISO 27005 stellen das Informationssicherheits-Managementsystem zur Verfügung und geben besondere Hinweise auf die Notwendigkeit von Risikoanalyse.

– *Im Sicherheitsmanagement* treffen wir auf viele industriespezifische Einzelbereiche. Sie umfassen die Arbeitssicherheit (neue ISO 45001) und die Umweltsicherheit (ISO 14001) genauso wie die Produktsicherheit (z.B. ISO 14971) und die Patientensicherheit (EN 15224). In all diesen Gebieten sind Risikoanalysen vorgeschrieben.

Prof. Dr. Bruno Brühwiler, Technische Hochschule Deggendorf, Geschäftsführer Euro Risk AG, Zürich

Dennoch ist es erforderlich, dass die vielen Spezialisten zusammenarbeiten, um Doppelspurigkeiten zu vermeiden und Synergien zu schaffen.

Risikomanagement in komplexen Unternehmen

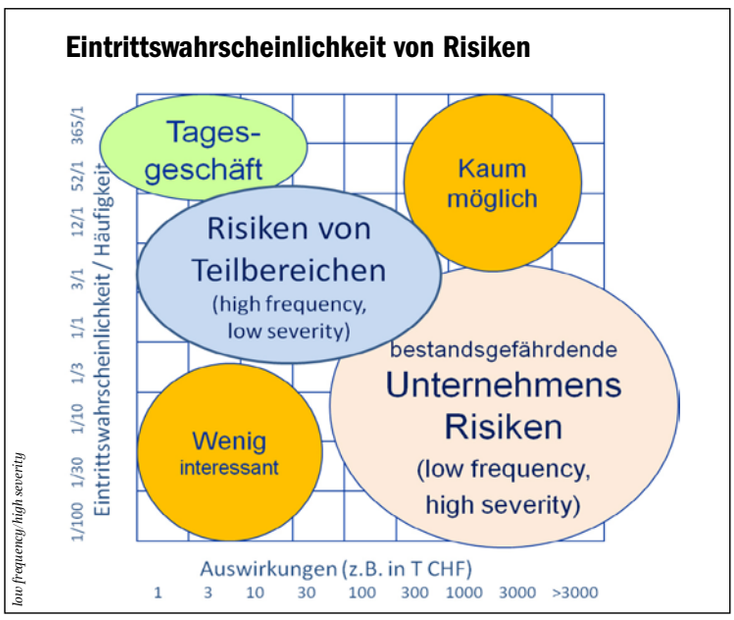
Das Ordnungs-System im Risikomanagement erfordert Systematik: Einerseits geht es darum, risikotechnische Gesichtspunkte zu berücksichtigen. Andererseits sind die fachspezifischen Inhalte und Methoden einzelner Teilbereiche aufrechtzuerhalten.

Wenn man in einer komplexen Organisation das Unternehmens-Risikomanagement ins Zentrum stellt und dieses mit den risikobasierten Teilsystemen vernetzt, kann man in der Konzeption des Top-down- und Bottom-up-Ansatzes die Lösungen finden. Das Unternehmens-Risikomanagement ist der Top-down-Ansatz, welcher das langfristige Überleben, die Existenzsicherung, den «Bestandserhalt» oder – in der französischen Sprache sehr schön gesagt – die «Pérennité» (ewige Dauer / Nachhaltigkeit) umfasst. Dieser Lösungsansatz ist im Deutschen Aktienrecht im KonTraG § 91 (2) AktG verankert («den Fortbestand des Unternehmens gefährdende Entwicklungen»).

Die oberste Leitung, d.h. der Verwaltungsrat / Aufsichtsrat und die Geschäftsleitung müssen sich mit diesen bestandsgefährdenden Risiken regelmässig befassen. Dabei ist sicherzustellen, dass die Risiken richtig identifiziert, mit Ursachen und Auswirkungen analysiert, verständlich beschrieben, korrekt bewertet und regelmässig gesteuert und überwacht werden.

Risikomanagement im Daily Business

Auch wenn ein Risiko nicht bestandsgefährdende Auswirkungen hat, sollte es eine bestimmte «Aussergewöhnlichkeit» aufweisen, um sich als Risiko vom Tagesgeschäft abzuheben. Im Tagesgeschäft gibt es viele Störungen, Unregelmässigkeiten und Abweichungen. Diese sollte man keinesfalls zum Thema des Risikomanagements oder eines risikobasierten Ansatzes machen, weil dadurch eine riesige Bürokratie entstehen würde, die keinen Nutzen stiftet. Hier muss das Instrument der kontinuierlichen Verbesserung dafür sorgen, dass die Leistungsprozesse laufend verbessert und optimiert werden.



Die vertikale Achse beschreibt die Häufigkeit: 1/100 = einmal in 100 Jahren, 365/1 = einmal pro Tag.

Bild: stevanovicigor depositphotos

Durch unterschiedliche Silowahrnehmungen kommen sich viele Organisationen wie in einem Labyrinth vor.

Davon zu unterscheiden ist das Fehlermanagement. Fehler können durch eine «Verkettung unglücklicher Umstände» zu einem grossen Sicherheitsrisiko führen. Hier ist die Auseinandersetzung mit den Fehlern eine Methode des Risikomanagements, die oft mit dem Begriff «Critical Incidents Reporting» oder Fehlermeldesystem bezeichnet wird.

Eine Organisation hat in der Regel nur wenige bestandsgefährdende Risiken, in der Anzahl sind dies vielleicht etwa 10 Risiken. Zu ihnen gehören nicht nur strategische Risiken einer Organisation, sondern auch operative Risiken.

Hilfreich für die Zuordnung von möglichen Abweichungen zum Risikomanagement, zu einem risikobasierten Teilbereich oder zum Tagesgeschäft ist die Analyse von Vorkommnissen in Bezug auf Häufigkeit des Auftretens und ihre Auswirkungen, im nachfolgenden Beispiel mit der finanziellen Dimension abgebildet.

In der Grafik (links) wird sichtbar, dass die bestandsgefährdenden Unternehmensrisiken aus risikotechnischer Sicht erhebliche Auswirkungen in qualitativer und quantitativer Art auf die Unternehmensziele haben können, sie treten allerdings nur mit geringen Eintrittswahrscheinlichkeit auf (low frequency / high severity).

Demgegenüber haben Risiken aus den entsprechenden Teilbereichen in der Regel eine hohe Frequenz, aber eine eher begrenzte Auswirkung auf die Unternehmensziele. Ausgenommen sind hier die bestandsgefährdenden Risiken. Die Behandlung der Risiken mit hoher Frequenz und begrenzter Auswirkung im Rahmen von Teilbereichen (z.B. im Internen Kontrollsystem) kann lohnend bzw. profitabel sein.

Risiko-Résumé

Die Gestaltung eines synergetischen Risikomanagement-Systems ist eine anspruchsvolle Aufgabe. Sie verlangt nicht nur ein tiefes Verständnis der vorangehend aufgeführten Teilbereiche des Managements, sondern auch ein hohes Mass an interner Kommunikation und Koordination. Normenwerke bieten dabei leider kaum Unterstützung, da sie in einer separierten Architektur oder nur partiell integrierten Struktur vorliegen.

Organisationen, die es verstanden haben, das Risikomanagement verständlich zu strukturieren, werden nicht nur über eine zweckmässige «Governance» verfügen, sondern insbesondere einen deutlichen Vorteil in effektiver und effizienter Nutzung ihrer Ressourcen sicherstellen. ■

Dieser Fachartikel erscheint in einer MQ-Serie, die von Experten und Expertinnen des «Netzwerk Risikomanagement» beigesteuert wird. www. netzwerk-risikomanagement.ch