

## Business Intelligence

# Risikomanagement in die Führungsprozesse integrieren

Unsere Welt wird immer digitaler und Prozesse werden mehr und mehr durch IT Systeme unterstützt und automatisiert. Mit Business Intelligence wird durch Datensammlung, Auswertung und geeigneter Aufbereitung (beispielsweise durch ein Management Cockpit oder ein Managemet Informations System) ein Mehrwert hinsichtlich eines schnellen Überblicks zur Lage des Unternehmens, geboten.

**Sieglinde Schenk**

Die Komplexität nimmt zu; sei es durch die interne Prozesslandschaft oder sei es durch die Anforderungen, die an Unternehmen von aussen gestellt werden (wie beispielsweise durch Regularien und Vorschriften).

Es ist schwierig sich in dieser Datenflut zurechtzufinden bzw. aus der daraus resultierenden Fülle an Informationen die richtigen Schlüsse zu ziehen und Strategien zu erarbeiten. Somit kommt den Systemen zur Wissensaufbereitung eine immer grössere Bedeutung zu. Auch Risikomanagement soll in diese Prozesse integriert werden. Daraus ergeben sich aber auch einige Fragestellungen.

In diesem Artikel soll ermittelt werden, inwieweit Business Intelligence (BI) das Risikomanagement (RM) auf Führungsebene unterstützen kann. Welche Risiken sind für das oberste Management relevant? Braucht es überhaupt eine eigene Risikoabteilung?

Kann man allein mit automatisierten Verfahren Risikomanagement betreiben? Wäre dies nicht objektiver, als auf die Bewertung von Experten zuzugreifen? Wo lassen sich Softwareprodukte gut einsetzen und wo

ergeben sich die Grenzen solcher Anwendungen? Welche Einsatzbereiche des Risikomanagements lassen sich damit abbilden?

## Wer betreibt Risikomanagement?

RM ist in aller Munde. Der Eindruck entsteht, dass wirklich fast jeder im Unternehmen RM betreibt. Jede Abteilung: Controlling, Security, Legal, Compliance, Business Development, IT, die Projektleiter bis hin zum CFO, CEO und dem Verwaltungsrat. Wozu braucht es dann noch ein eigenes RM und Risikomanager? Alle Risiken scheinen doch schon mehrfach bewirtschaftet. Oder doch nicht?

Bei so viel Risikoabsicherung kann man verstehen, wenn auf Führungsebene die Meinung entsteht, dass man auch gut ohne ein eigenes RM auskommen kann.

Trotzdem sollte genau differenziert werden zwischen dem Risikobewusstsein einzelner Abteilungen und der Aufgabe eines eigenständigen neutralen RM.

Ein Managementprozess gehört zu den Führungsprozessen und beeinflusst und definiert die Kernprozesse. Dazu gehört auch das Risikomanagement.

## Automatisiertes RM – eine Alternative?

Schlagworte wie Artificial Intelligence (AI) oder «Large Scale Cyber Risk Management», Robotic Processes, etc. suggerieren, dass bei entsprechender Softwareinstallation die Risiken im Griff behalten werden können.

Manche Softwarelösungen geben vor, dass das Management per Mausklick die relevanten KPIs bzw. Risikoexpositionen in einem «Risk Cockpit» sofort sehen kann. Das klingt verlockend; erfordert jedoch grossen Aufwand und Vorbereitung.

Und es funktioniert nichts von selbst. Der laufende Betrieb erfordert Wartung, Anpassung, Weiterentwicklung und Plausibilisierung. Schliesslich können Daten nicht einfach so übernommen werden, sondern müssen in einem sinnvollen Kontext gebracht werden. Sonst wird das verwendete System selbst zum Risiko, das Scheingenaugigkeit suggeriert.

«Every tool needs it's fool»; heisst es in Softwarkreisen so lapidar. Es ist also wichtig, dass jemand für die Betreuung der Tools verantwortlich ist und diese Aufgabe auch entsprechend ernst nimmt. Ohne die Berücksichtigung der Datenpflege und Plausibilisierung kann unter Umständen auch sehr viel Datenmüll erzeugt werden. Dieses Phänomen wird in der sogenannten GIGO Phrase in der Informatik aufgegriffen – «Garbage in – garbage out». Und schliesslich sollten die Ergebnisse auch richtig interpretiert werden können: «a fool with a tool is still a fool».

Wer selbst einmal programmiert hat, der weiss um das Prinzip Bescheid, dass es eine Anleitung in Form eines Maschinencodes braucht, um ein Ergebnis aus Programmen zu bekommen. Eine Fehlerquelle liegt schon in der Erfassung der Problemstellung. Was ist das gewünschte Ziel? Die Interpretation der Daten beinhaltet schon die nächste Fragestel-



Abb. 1:  
Grobe Unterteilung  
der Prozesse

Quelle: Sieglinde Schenk

**Sieglinde Schenk** hat eine breite universitäre Ausbildung (naturwissenschaftlich/technische und betriebswirtschaftlich) absolviert. Sie ist seit mehr als 10 Jahren im Corporate Risk Management tätig und war davor lange in der IT Entwicklung und im Projektmanagement beschäftigt.

lung: Welche Aussagekraft liegt den Ergebnissen zugrunde?

Wie gut sind die Schnittstellen an die bestehenden IT Landschaft angepasst oder zu externen Quellen (wie etwa Börsenkurse, Preiskurven) und wie gut erkennt das System Eingabefehler? Es gibt viel zu analysieren; auch bei Standard Softwarelösungen.

Trivial ist das nicht. Es wird deutlich, dass Informationen lückenhaft oder falsch sein können, dass Änderungen und Erweiterungen nicht immer einfach möglich sind und unter Umständen zu hohen Kosten führen.

Fehler in den Systemen können aus unterschiedlichen Bereichen kommen: von der Erfassung der Aufgabenstellung, der Programmlogik, der Syntax, den Schnittstellen zu anderen Systemen, durch Eingabefehler der Anwender bis hin zu Hardwareproblemen.

Auch die leistungsstärksten Computersysteme sind davor nicht gefeit.

Digitale Transformationsprozesse sind teuer, können aber bei sinnvoller Integration ins Unternehmen auch einen hohen Mehrwert bringen.

### Wann macht Automatisierung Sinn? Und wann nicht?

Automatisierung im RM ist für die Bewältigung grosser Datenmengen, wie beispielsweise im Finanzbereich («price forward curves», «ratings», Plausibilitätschecks etc.) oder für interne Kontrollmechanismen unerlässlich. Die angewendeten Mechanismen sind für Bereiche wie «Liquidity Management», «FX Management» und «Financial Monitoring» äusserst wichtig.

Die eingesetzten Tools können Auffälligkeiten entdecken (beispielsweise im Zahlungsverkehr), «Stopp loss» Mechanismen in Gang setzen und Warnungen verschicken.

Doch es gibt sicherlich auch Grenzen der Automatisierung.

Wie sieht das nun für den Bereich Corporate Risk Management (CRM) aus? Die Aufgabe des Corporate Risk Managers ist es, der obersten Leitung die existenzbedrohenden Risiken zur Kenntnis zu bringen und Massnahmen zur Bewirtschaftung abzubilden. Diese Aufgabe beinhaltet die Betrachtung aller Risiken; sowohl operativer Risiken als auch strategischer Risiken. Zur Erfassung der Gesamtrisikosituation haben sich Experteninterviews als äusserst wertvoll und effektiv erwiesen.

Obwohl die Daten durchaus auch in RM Tools erfasst werden können, um Simulationen und analytische Berechnungen durchzu-

führen, ist der Automatisierungsgrad gering. Das Erfassen und Beschreiben der Risiken obliegt meist dem Risikomanager oder ausgewählten Risikoexperten. Es geht vielmehr darum, die relevanten Risiken revisionssicher zu verspeichern, zu analysieren, aufzubereiten und einen Risikobericht zu generieren.

### Anforderungen ans RM

Die Kompetenz im RM ist natürlich auch massgeblich am Gelingen des Risikoprozesses beteiligt. Die Anforderungen (regulatorischer und wirtschaftlicher Art) können je nach Unternehmen stark differieren. Rigoroses Abarbeiten nach Schema F genügt vielleicht gerade regulatorischen Verpflichtungen, bringt aber, ausser Mehrbelastung und Frust, den operativen Einheiten und der Firmenleitung nicht viel.

Es ist eben die Kunst des Risikomanagers auf der einen Seite mit Akribie, Scharfsinn, Analytik und Systematik zu operieren und auf der anderen Seite dennoch Menschenverstand und Diplomatie walten zu lassen. Profundes Sachwissen, Flexibilität, Ausdauer und eine grosse Frustrationstoleranz komplettieren das Anforderungsprofil. Selbstverständlich sollte der Risikomanager ebenfalls über Integrität und Loyalität verfügen und kein willfähriger Befehlsempfänger sein. Schlussendlich ist es auch wichtig, die Fähigkeit zu besitzen aus der Fülle von Informationen die wichtigen existenzbedrohenden Gefahren in plausibler Weise herauszufiltern und zu dokumentieren.

### Fazit

Business Intelligence bedeutet nicht, dass alles in Standardprozessen abgebildet werden kann. Besonders im Risikobereich können fir-

menspezifische Gefahren entstehen, die nicht in ein Schema passen und plötzlich durch ein geändertes Umfeld an Bedeutung gewinnen können. Als Beispiel kann hier natürlich die Finanzkrise mit ihren verheerenden Auswirkungen herangezogen werden. Aber meist sind die Auswirkungen nicht so allumfassend, sondern betreffen dann nur eine Firma oder eine Branche. BI umfasst nicht nur die Installation von einer Softwarelösung, sondern auch die Fähigkeit von Mitarbeitern bzgl. Kollaboration, Analyse und ständigen kritischen Hinterfragen, aber auch lösungsorientierten zielgerichteten Vorgehen. Im RM bedeuten die Systeme eine grosse und teilweise unverzichtbare Unterstützung, wenn man sich der Grenzen und Gefahren bewusst ist.

Die Leistung der Computersysteme nimmt immer mehr zu; in diesem Zusammenhang steht beispielsweise die Entwicklung der Quantencomputer, die mit ihrer Rechenstärke heutige Kryptoverfahren bereits in ein paar Jahren obsolet machen können, da Sie Rechenoperationen millionenfach schneller ausführen können als herkömmliche Computer.

Die Herausforderung aus einer solchen Fülle von Informationen die richtigen Schlüsse zu ziehen nimmt allerdings ebenfalls zu. Scheinsicherheiten können grossen Schaden anrichten. Die Verantwortung für strategische Entscheidungen und Massnahmen liegt immer noch beim Topmanagement und die wird auch von keinem Supercomputer übernommen werden können. ■

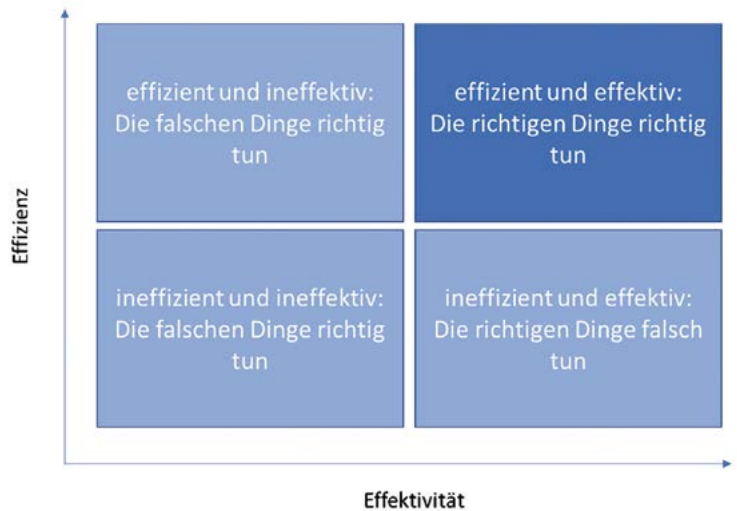


Abb 2:  
Der Unterschied  
zwischen Effizienz  
und Effektivität

### Hinweis

Dieser Fachartikel erscheint in einer MQ-Serie, die von Experten und Expertinnen des «Netzwerk Risikomanagement» beigeleitet wird:

[www.netzwerk-risikomanagement.ch](http://www.netzwerk-risikomanagement.ch)