G 59071

13·2006

- KREDITRISIKO
- MARKTRISIKO
- OP RISK
- ERM

RISIKO MANAGER

Mittwoch, 28.6.2006

WWW.RISIKO-MANAGER.COM

Inhalt

Erkennung von Trends und Frühen Signalen im Risikomanagement

Frühwarnindikatoren: Kritischer Faktor Spätwarnung

Ein Frühwarnsystem verfolgt das Ziel, aufkommende zukünftige Gefahren frühzeitig als solche zu erkennen und Gefährdete möglichst schnell darüber zu informieren. Frühwarnsysteme sollen ermöglichen, durch eine rechtzeitige Reaktion die Gefahr abzuwenden oder zu mildern.

In diesem Kontext sei etwa an das Tsunami-Frühwarnsystem im Indischen Ozean erinnert. Dort registrieren Messstationen im Meer Seebeben oder den erhöhten Wasserdruck, der durch die riesigen Tsunami-Wellen entsteht. Die Daten werden via Satellit an zentrale Frühwarnzentralen übertragen. Von dort können die Warnungen per Internet, E-Mail und SMS an alle angeschlossenen Nutzer gesandt werden. Dies geschieht im Idealfall nahezu in Echtzeit, denn die Reaktionszeit ist der entscheidende Faktor – Tsunamis breiten sich mit bis zu 1000 Kilometern pro Stunde aus. Je früher Alarm gegeben wird, desto mehr Zeit bleibt den Menschen zur Flucht. Auch im Bereich der Wirtschaft zielt ein Frühwarnsystem darauf ab, negative Tendenzen bzw. operationelle Risiken möglichst frühzeitig zu erkennen, so dass eine Umsatzminderung, ein Schaden, oder gar ein Konkurs verhindert werden können.

Fortsetzung auf Seite 4

CEBS veröffentlicht Konsultationspapier zum Stress Testing

■ Das Committee of European Banking Supervisors (CEBS) hat die öffentliche Konsultationsphase zum „Stress Testing“ gestartet: Mit dem neu veröffentlichten Konsulationspapier (CP12) werden die CEBS-Richtlinien im Hinblick auf den so genannten „Supervisory Review Process“ vom Januar 2006 ergänzt. In seiner aktuellen Form gibt das Konsultationspapier das abgestimmte Verständnis der Europäischen Aufsichtsbehörden im Hinblick auf das Thema „Stress Testing“ wieder. Das CEBS weist in diesem Zusammenhang darauf hin, dass die Richtlinien zum Stress Testing im Rahmen des Dialogs zwischen Aufsichtsbehörden und Finanzinstituten angewendet werden. Sie sollten also nicht dahingehend interpretiert werden, dass sie automatisch zu einer erhöhten Kapitalanforderung führten.

Der Begriff „Stress Testing“ wird in der Richtlinie verwendet, um die unterschiedlichen Techniken von Finanzinstituten zu beschreiben, mit deren Hilfe sie versuchen, ihre Anfälligkeit für außergewöhnliche, aber plausible Ereignisse abzuschätzen. Das CEBS hält es für wichtig, dass Stress Tests innerhalb des Risikomanagement-Rahmenwerks einer Bank berücksichtigt werden. Stress Testing wird dabei als Bestandteil der internen Prozesse gesehen. Dementsprechend sollten die Institute – im Rahmen des so genannten Internal Capital Adequacy Assessment

Fortsetzung auf Seite 2

Fortsetzung von Seite 1

Vom menschlichen Nervensystem zum Frühwarnsystem im Unternehmen

Risiko-Indikatoren sind mit dem menschlichen Nervensystem vergleichbar. Sie registrieren Veränderungen innerhalb eines Organismus und lösen Warnungen aus. Wenn die „Schmerzgrenze" überschritten ist, reagiert der Körper und versucht, die negative Situation zu ändern, damit die Schmerzen eliminiert oder reduziert werden.

Nun ist der menschliche Körper ein sehr komplexer Organismus, der sich für einen Vergleich mit den Risiko-Indikatoren nur bedingt eignet (obwohl Unternehmen und Finanzinstitute ebenfalls komplexe Organisationen sind). Sowohl der menschliche Körper als auch die Organisation einer Bank werden als offene Systeme gekennzeichnet, weil sie externen Einflüssen ausgesetzt sind.

Ist dies nicht der Fall, bezeichnet man das System als geschlossenes System. Ein bekanntes Beispiel ist die Zentralheizung in Häusern, die sich wie in ▶ **Abb. 01** abbilden lässt.

Der Thermostat registriert, dass die Temperatur in einem Raum unter einer gewissen vorher eingestellten Grenze bleibt. Diese Situation kann als kritisch eingestuft werden, wenn sich die Temperaturen unter dem Gefrierpunkt bewegen, da sich dann Schäden im Leitungssystem einstellen können. In einem geschlossenen System muss nicht eingegriffen werden. Der Thermostat gibt der Heizung ein Signal und diese beginnt sofort, warmes Wasser in die Heizkörper zu pumpen. Der Thermostat stellt irgendwann fest, dass die gewünschte Temperatur erreicht ist. Er sendet der Heizung wieder ein Signal und danach stoppt diese den Heizungsvorgang wieder.

Bei der Zentralheizung ist die Messung eindeutig. Die Temperatur wird festgestellt, mit der gewünschten Temperatur abgeglichen und bei Abweichungen wird der Heizungsvorgang gestartet. Außerhalb geschlossener Systeme stellen wir jedoch fest, dass dieser Regelmechanismus nicht mehr so einfach ist. Es existieren nun mehrere Einflussfaktoren, die nicht mehr alle bekannt sind. Selbst wenn einige Einflussfaktoren bekannt sind, dann ist trotz alledem deren Auswirkung nicht immer eindeutig prognostizierbar. Diese Wechselwirkungen können wie in ▶ **Abb. 02** dargestellt werden.

Die Störungen aus der Umgebung sind nun nicht mehr eindeutig vorhersehbar; sie gehören nicht zu festen Klassen und nicht alle Treiber sind vorweg bekannt. Es kann daher passieren, dass die Einflüsse aus der Umgebung gar nicht wahrgenommen werden, weil überhaupt kein Indikator zur Messung solcher Einflüsse vorgesehen ist. Ebenfalls können die Einflüsse auf das gesteuerte System nicht genau vorhergesagt werden. Sie sorgen aber für eine Abweichung im gesteuerten Prozess.

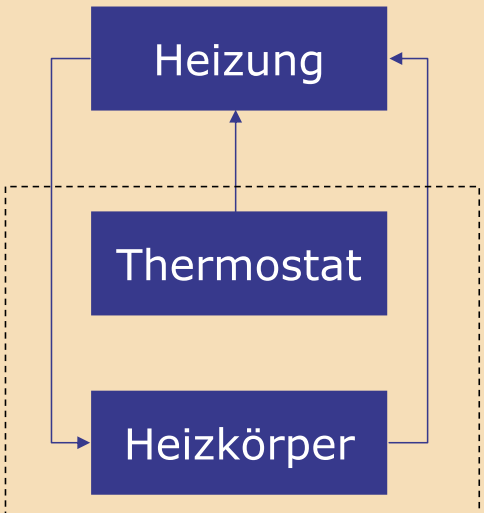
Auch hier gilt, dass die Indikatoren bezüglich des Systemzustands nicht immer alle Einflüsse wahrnehmen werden und Probleme im gesteuerten System vom Steuerungssystem gar nicht erfasst werden. Es findet daher auch keine Gegensteuerung statt.

Risikomanagement – und hier auch die Beachtung von Frühwarnindikatoren – waren schon immer wichtige unternehmenspolitische Instrumente zur Erreichung der Unternehmensziele. In den Anfängen des Risikomanagements wurde auf Risiken primär reaktiv (oder auch situativ bzw. retrospektiv) reagiert.

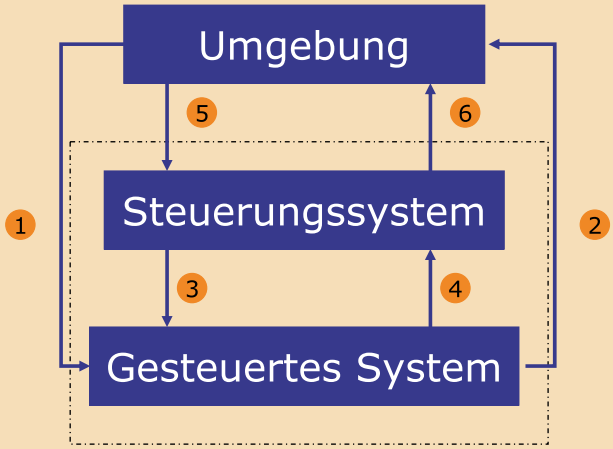
Risikomanagement hat jedoch per definitionem nicht das Ziel, die Vergangenheit zu erklären, sondern will zukünftige Chancen und Risiken antizipieren und teilweise auch einfach nur helfen, bessere Antworten auf Fragen zu finden.

Risikomanagement sollte daher proaktiv (oder auch prospektiv) ausgerichtet sein. Ein wesentlicher Ansatzpunkt hierfür sind Frühaufklärung, Früherkennung und Frühwarnung.

Beispiel für ein geschlossenes System ▶ **Abb. 01**



Ein offenes System ▶ **Abb. 02**



(1) Störungen aus der Umgebung
(2) Ergebnis aus dem System
(3) Steuerungsmaßnahme
(4) Indikator bezüglich Systemzustand
(5) Beeinflussung aus der Umgebung
(6) Beeinflussing der Umgebung

Frühaufklärung, Früherkennung und Frühwarnung

Ein wichtiges Instrument zur Risikoidentifikation sind Frühwarnsysteme, mit deren Hilfe Frühwarnindikatoren (etwa externe Größen wie Zinsen oder Konjunkturindizes, aber auch interne Faktoren wie etwa Fluktuation in Management oder Forderungspositionen) ihren Benutzern rechtzeitig latente (d. h. verdeckt bereits vorhandene) Risiken signalisieren, sodass noch hinreichend Zeit für die Ergreifung geeigneter Maßnahmen zur Abwendung der Bedrohung oder Schadensbegrenzung besteht.

Hierdurch kann die Entwicklung des Unternehmenswertes stabilisiert und gesteigert werden. Immer häufiger fokussieren sich moderne Frühwarnsysteme nicht nur auf die Erkennung von zukünftigen Entwicklungen und Ereignissen, sondern vor allem auch auf die Erklärung von Ursache-Wirkungs-Beziehungen. Bereits bei der Definition von Frühwarnindikatoren (etwa in Form von Key Risk Indikatoren) erfährt man viel über die kausalen und strukturellen Zusammenhänge sowohl innerhalb als auch außerhalb des Unternehmens.

Da in der Praxis immer auch latente Chancen signalisiert werden, spricht man auch von **Früherkennung**. In der unternehmerischen Praxis lassen sich Chance und Risiko nicht losgelöst voneinander analysieren. Chancen und Risiken sind jeder Entscheidung und jeder Führungstätigkeit immanent, quasi die beiden Seiten ein und derselben Medaille. Jedes „Risikomanagement"-System ist damit auch gleichzeitig ein „Chancenmanagement"-System [vgl. Romeike/Finke 2003]. Wird zusätzlich noch der Prozessschritt der Risikosteuerung und Risikokontrolle berücksichtigt, d. h. die entsprechenden Maßnahmen zur Realisierung der Chancen bzw. der Abwehr/Minderung der Bedrohungen, so wird der Begriff **Frühaufklärung** verwendet (vgl. ► **Abb. 03**).

Von der zielgerichteten und systematischen Suche nach Frühwarnsignalen ist die Identifikation von Trends abzugrenzen. Hierbei wird versucht, bewusst unstrukturiert – beispielsweise in Form des Brainstormings – Chancen und Risiken transparent zu machen.

Moderne Frühwarnsysteme können sowohl auf qualitativen als auch auf quantitativen Methoden basieren. Qualitative Frühwarnsysteme (etwa basierend auf Branchentrends, rechtliche Informationen, Veröffentlichungen über Wettbewerber) eignen sich vor allem für Langfristprognosen, um beispielsweise strukturelle Veränderungen zu identifizieren und zu analysieren. Quantitative Methoden hingegen nutzen statistische und ökonometrische Verfahren und quantitative Informationen. Hier sei beispielsweise an komplexe Zeitreihenanalysen (etwa ARIMA- oder GARCH-Modelle) gedacht.

So basieren moderne Frühwarnsysteme u. a. auf neuronalen Netzwerken, deren Strukturen und Funktionen sich an den Nervennetzen lebender Organismen orientieren. Ein Vorteil des menschlichen Gehirns besteht ja darin, dass auch dann noch korrekte Ergebnisse geliefert werden, wenn es zu einem Ausfall einiger für die Problemlösung notwendiger Nervenzellen kommt.

Selbst wenn bestimmte Daten ungenau sind, also etwa ein Text durch Verschmutzung unleserlich geworden ist, kann das Gehirn den Inhalt des Textes noch erkennen und verstehen. Das Ziel solcher künstlichen Netzwerke ist die Simulation der „massiv parallelen" Informationsverarbeitung im Gehirn unter Berücksichtigung der Lernfähigkeit. Neuronale Netze zeichnen sich durch eine hohe Fehlertoleranz und die verteilte Wissensrepräsentation aus, wodurch ein zerstörtes Neuron nur einen relativ kleinen Wissensausfall bedeutet. Schwächen haben rein quantitative Frühwarnsysteme jedoch vor allem beim Aufspüren von strukturellen Veränderungen, so genannten Diskontinuitäten.

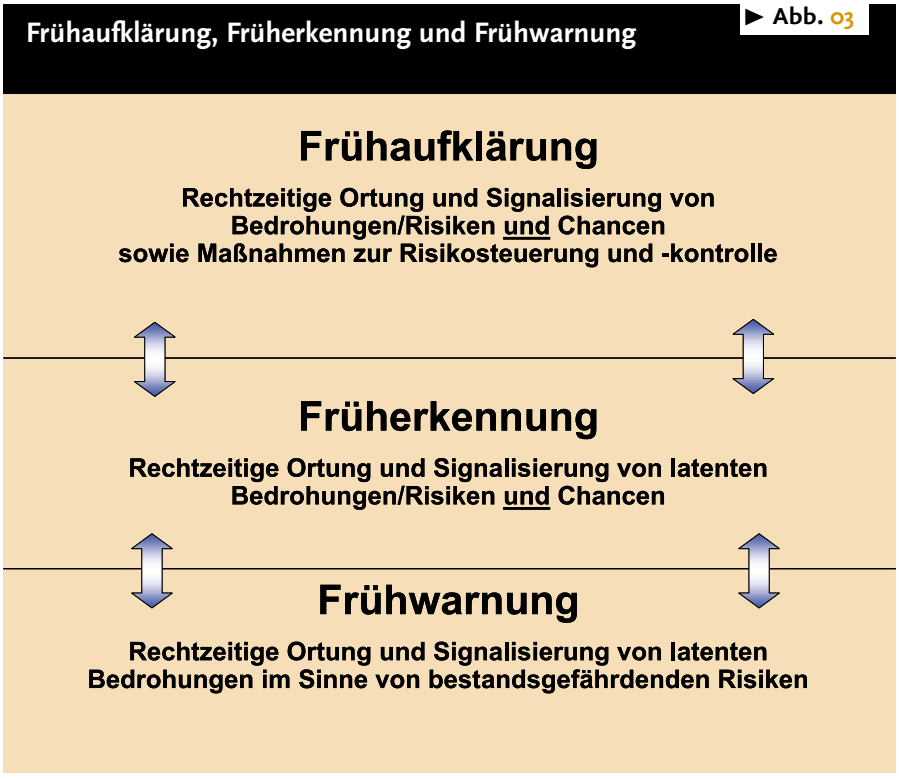
Allgemein können drei unterschiedliche Arten bzw. Generationen von Frühaufklärungssystemen unterschieden werden:

- Kennzahlen- und hochrechnungsorientierte,
- Indikatororientierte und
- Strategische Frühaufklärungssysteme.

Kennzahlen- und hochrechnungsorientierte Frühaufklärungssysteme basieren auf einem periodischen Vergleich von Kennzahlen bzw. auf innerjährigen Hochrechnungen von Über- und Unterschreitungen bestehender Jahrespläne (Budgets) und eignen sich daher vor allem für das operative Controlling. Hierbei werden insbesondere Soll-Ist-Zahlen bzw. Soll-Wird-Zahlen verglichen. Beim Unter- bzw. Überschreiten definierter Schwellenwerte sollen adäquate Warnmeldungen ausgelöst werden. Kritisch ist hierbei anzumerken, dass kennzahlen- und hochrechnungsorientierte Frühaufklärungssysteme auf vergangenheitsorientierten Daten basieren und eine längerfristige Früherkennung von Chancen und Risiken nicht möglich ist.

Zentrale Elemente von **indikatororientierten Frühaufklärungssystemen** sind

Frühaufklärung, Früherkennung und Frühwarnung ► **Abb. 03**



Indikatoren (leading indicators), die Informationen über die zukünftige Entwicklung der Umweltveränderungen im unternehmensinternen und externen Bereich liefern. Die Definition und Erhebung von Indikatoren sollte sinnvoller Weise im Rahmen von existierenden Planungs- und Berichtssystemen bzw. im Zusammenhang mit einer implementierten Balanced Scorecard erfolgen. Die größte Herausforderung bei indikatorbasierten Frühaufklärungssystemen besteht bei der Selektion geeigneter Indikatoren, da Kausalzusammenhänge in einer komplexen Wirtschaftswelt nur selten über singuläre und statische Indikatoren erklärt werden können.

Indikatoren spiegeln nicht selten lediglich die bisherigen Erfahrungen und Kenntnisse wider und blenden potenzielle neue Entwicklungen und Kausalitäten aus. Adäquate Indikatoren müssen insbesondere eindeutig, vollständig und rechtzeitig verfügbar sein, frühzeitig auf zukünftige Entwicklungen hinweisen sowie effizient erfasst werden können.

Insbesondere im Zusammenhang mit dem Erkennen von operationellen Risiken wurden in den vergangenen Jahren sowohl bei Banken als auch bei Versicherungsunternehmen große Anstrengungen unternommen, um adäquate Key Risk Indikatoren zu definieren und zu erfassen. Key Risk Indicators sind Parameter, die sich auf Geschäftsprozesse oder Prozessbündel beziehen und in der Lage sind, Veränderungen im Risikoprofil dieser Geschäftsprozesse oder Prozessbündel vorherzusehen. Die Risiko-Indikatoren sollen folgende Ziele erfüllen: Risikoereignissen soll vorgebeugt und ungünstige Trends sollen rechtzeitig erkannt werden [Romeike 2004a].

Strategischen Frühaufklärungssystemen liegt das Konzept der schwachen Signale von Ansoff zugrunde [Krystek/Müller 1999, S. 181ff. sowie Ansoff 1976, S. 133-136.]. Ansoff geht davon aus, dass tief greifende Umbrüche (etwa im ökonomischen, sozialen und politischen Bereich) nicht plötzlich entstehen, sondern sich lange im Voraus durch schwache Signale (weak signals) ankündigen. Oft handelt es sich um Informationsrudimente, d. h. unscharfe und wenig strukturierte Informationen, wie beispielsweise

- Gefühle, dass mit Bedrohungen bzw. Chancen zu rechnen ist (etwa basierend auf Presseberichten, Studien von Zukunftsforschungsinstituten, Informationen aus Diskussionsforen im Internet oder Informationen bezüglich der allgemeinen wirtschaftlichen Entwicklung),
- nur vagen Informationen über mögliche Quellen und Ursachen latenter Gefahren
- nur vagen Informationen bzgl. konkreter Bedrohungen und Chancen, aber klaren Vorstellungen hinsichtlich ihrer strategischen Relevanz
-

Schwache Signale verstärken sich häufig im Zeitablauf und weisen immer stärker auf Trend-/Paradigmawechsel hin.

Nach Ansoff gibt es unerwartete Diskontinuitäten nur, weil die Empfänger dieser Signale nicht darauf reagieren. Zur Vorbeugung von strategischen „Überraschungen" müssen schwache Signale daher rechtzeitig geortet werden. Dies bedingt eine Sensibilisierung aller Mitarbeiter für schwache Signale, da mit zunehmender Konkretisierung der Signale im Zeitablauf die Reaktionsfähigkeit des Unternehmens abnimmt.

Insbesondere erfordert die Umsetzung des Konzepts von schwachen Signalen eine Abkehr von starren und streng hierarchisch strukturierten Denk- und Organisationsstrukturen. Frühaufklärungssysteme der dritten Generation werden auch unter dem Begriff des „strategischen Radars" bzw. „360-Grad-Radars" zusammengefasst, da das Ortungssystem offen und ungerichtet ist. Das „strategische Radar" verwendet vor allem die Instrumente des „scanning" und „monitoring".

Ersteres stellt ein ungerichtetes Abtasten des gesamten Unternehmensumfeldes dar und bezweckt das Erkennen trendartiger Entwicklungen. Diese werden im Rahmen des „Monitoring" gezielten und tief greifenden Analysen unterzogen. Ziel dabei ist es, möglichst viele unscharfe Signale zu empfangen, die erst in einem weiteren Schritt hinsichtlich ihres Verhaltens- bzw. Ausbreitungsmuster sowie ihrer Ursachen und Wirkungen analysiert werden.

In einem weiteren Schritt wird die Relevanz der analysierten Signale beurteilt und hinsichtlich ihrer Dringlichkeit in eine Rangordnung gebracht. Erst in einem abschließenden Schritt werden adäquate Reaktionsstrategien entwickelt und umgesetzt. Bei der Analyse von strategischen Frühaufklärungssystemen können Instrumente aus dem strategischen Marketing (Erfahrungskurve, Produktlebenszyklus etc.) und auch andere etablierte und praxiserprobte Methoden (Szenario-Technik, Portfoliomethode, Delphi-Verfahren, Trend-Impact-Analyse etc.) verwendet werden.

Ziele von Risiko-Indikatoren

Die Ziele der Risiko-Indikatoren sind sowohl interner als auch regulatorischer Natur. Ein gutes Risk Management wird sicherlich auch dadurch ausgezeichnet, dass die Effekte von Risikoereignissen abnehmen oder im Idealfall sogar verschwinden. Die Effekte sind nicht nur direkte Folgen eines Risikoereignisses, sondern auch dessen indirekten Folgen:

1. Die Kundenzufriedenheit nimmt ab, wenn die Kunden die Folgen von operationellen Risiken (etwa einer Betriebsunterbrechung in der IT) zu spüren bekommen. Wenn Zahlungsaufträge regelmäßig zu spät ausgeführt werden, dann ist damit zu rechnen, dass die Kunden die Dienstleistungen der betreffenden Bank nicht mehr in Anspruch nehmen. Der Deckungsbeitrag dieser Kunden geht der Bank verloren.
2. Die Mitarbeiterzufriedenheit hängt ebenfalls mit der Fehleranfälligkeit in der Bank zusammen. Zum Beispiel wird anderen Banken relativ schnell klar, ob die Zahlungsverkehrsabteilung einer Bank mit gutem Personal besetzt ist. Gute Mitarbeiter realisieren darum schnell, dass die Fehleranfälligkeit ihren Marktwert reduziert. Sie werden eventuell versuchen, den Arbeitgeber zu wechseln, um ihren persönlichen Schaden zu begrenzen.

Neben dem Vorbeugeaspekt von Risiko-Indikatoren verfolgen Unternehmen ergänzend auch das Ziel, dass Trends frühzeitig entdeckt werden. Hier geht es darum, dass etwaige Management-Reaktionen Zeit benötigen, bevor sie überhaupt wirksam werden. Davon ausgehend, dass beispielsweise die Motivation der Belegschaft gemessen werden kann, ist zu überlegen, ab wann die Gegenmaßnahmen gegen eine abnehmende Motivation eingeleitet werden müssen.

Die entscheidende Frage ist, wie viel Zeit verloren geht, bis die Maßnahmen wirksam werden. Eine sinkende Motivation geht nicht selten mit einem Vertrauensverlust einher. Dieser Vertrauensverlust

muss zunächst überwunden werden, bevor die Mitarbeiterinnen und Mitarbeiter die Gegenmaßnahmen wahrnehmen können. Wenn solche Maßnahmen zu spät eingeleitet werden, wird die Situation automatisch im roten Bereich enden. Es ist wichtig, die negativen Änderungen der Risiko-Indikatoren frühzeitig zu erkennen. Wenn solche Änderungen rechtzeitig erkannt werden, können Maßnahmen so eingeleitet werden, dass sie effektiv sind. In ► **Tab.** 01 wurden exemplarisch Risiko-Indikatoren im Bereich der Informationstechnologie zusammengestellt.

Definitionsprozess von Risiko-Indikatoren

Bei der Definition von Risiko-Indikatoren wird ein fester Prozess durchlaufen, der in komprimierter Form in ► **Abb.** 04 skizziert ist.

Zunächst sollte festgelegt werden, welche Objekte mit Hilfe der Risiko-Indikatoren überwacht werden sollen. Die in der Praxis am häufigsten praktizierte Vorgehensweise orientiert sich an den bereits vorhandenen Risikoinformationen, wie etwa Verlustereignissen und Risikoprofilen. Es werden jedoch auch die Erfahrungen der Prozessverantwortlichen berücksichtigt. Bevor der Definitionsprozess gestartet wird, ist es sinnvoll, zunächst zu analysieren, ob die Risiken reduziert oder gar vermieden werden können. Dieser Lösungsansatz sollte immer an erster Stelle stehen.

Wenn aber festgestellt wird, dass die Risiken nicht aufgehoben werden können, dann sollte der Definitionsprozess eingeleitet werden. Die Risiko-Indikatoren werden dann als „first line of defense" verstanden, da sie bei einer rechtzeitigen Warnung die Schadensbegrenzung ermöglichen.

Neben den risikobehafteten Prozessen sollen in dieser ersten Phase ebenfalls die Risikoursachen festgehalten werden. Die Risikoursachen spielen eine wichtige Rolle, wenn es darum geht, die Risikotreiber zu identifizieren.

Ein Beispiel ist diesem Kontext das Risiko einer unzureichenden Personalausstattung. Es handelt sich hier sowohl um qualitative als auch um quantitative Mängel. Folgende Risikotreiber können hier identifiziert werden:

- Die Art und Weise der Organisation kann bereits zu Problemen bei der Personalausstattung führen. Wenn die Gruppen zu klein gewählt werden, entsteht automatisch das Problem des Schüsselpersonals. Wenn die Gruppen kleiner als vier Personen sind, kann es zu Personalengpässen kommen, die oftmals durch eine Kombination von Urlaub und Krankheit hervorgerufen werden.
- Die Reputation als Arbeitgeber bestimmt, in wiefern das Unternehmen in der Lage ist, die besten Talente anzuwerben. Diese Reputation wird unter Studenten national und international gemessen. Diese Information ist extern verfügbar. Nun muss man sich auch in diesem Fall überlegen, welches Ranking das Unternehmen erreichen soll, damit es seine Ziele verwirklichen kann. Es wird inzwischen immer mehr deutlich, dass der Kampf um Talente bereits begonnen hat und die Effekte in den kommenden Jahren sichtbar werden. Wenn Studenten ein Unternehmen als Arbeitgeber nicht attraktiv finden, dann hängt das oft mit der Wahrnehmung einer mangelnden Innovationskraft zusammen. Ein Unternehmen, das nicht innovativ ist, ist auf lange Sicht nicht überlebensfähig. Wenn das Unternehmen aber auf der Rankingliste weiter sinkt, wird es umso schwieriger, geeignete Mitarbeiter zu werben. Die Folge erfährt das Unternehmen zunächst aus qualitativer und später aus quantitativer Sicht.
- Strukturelle Überstunden sind ein Zeichen einer dünnen Personaldecke. Die Überstunden müssen immer relativ zu den üblich geleisteten Stunden gesehen werden, denn sonst könnte man leicht zu einer Fehlinterpretation kommen. In manchen Abteilungen gehört es ja „zum gutem Stil" lange anwesend zu sein. In solchen Fällen sollte dieser Umstand adäquate Berücksichtigung finden.

Definitionsprozess von Risiko-Indikatoren ► **Abb.** 04

Beispiele für KRI im Bereich der Informationstechnologie

▶ Tab. 01

Key Risk Indicator	Einheit	Definition	Treiber
Auswertung der Systemauslastung	Prozent	Kapazität der Systeme, Auslastung der Systeme (etwa Anzahl der Transaktionen)	Zu hohe Auslastung der Systeme
Auswertung des Netzwerk-Traffics	Prozent	Netzwerk-Kapazität; Netzwerk-Belastung	Zu hoher Auslastung des Netzwerkes
Durchschnittliches Alter der Systeme	Jahre	Alter der vorhandenen Systeme	Anfälligkeit der Systeme
Anzahl von Release Changes	Zahl	Nach einem Change Release können z.B. Prozessfehler entstehen oder das gesamte System ausfallen	Systemfehler, die aufgrund der Veränderungen entstanden sind
Anzahl von Firewall Changes	Zahl	Nach einem Firewall Change kann es zu einem Systemsicherheitsbruch kommen	Systemunsicherheit aufgrund des Firewall Changes
Aktualität der IT-Anwendungs-Dokumentation (Anteil der IT-Anwendungsdokumentationen, die älter als 12 Monate sind)	Prozent	Gesamtanzahl der IT-Anwendungs-Dokumentationen; Anzahl der IT-Anwendungs-Dokumentationen, die seit zwölf Monaten nicht aktualisiert wurden	Fehler durch nicht aktuelle IT-Anwendungs-Dokumentationen
Dokumentationsquote der IT-Applikationen Ist/Soll	Prozent		Fehler durch fehlende Dokumentation der IT-Anwendungen
Wartung des Netzwerks Ist/Soll	Prozent	Abweichung der Häufigkeit der Netzwerkwartung	Störungsanfälligkeit
Wartungsdokumentationsquote für Netzwerk Ist/Soll	Prozent		Fehlende Informationen aufgrund unvollständiger Dokumentationen
Wartung von IT-Applikationen Ist/Soll	Prozent	Abweichung der Häufigkeit der Wartung von IT-Applikationen	Störungsanfälligkeit
Wartungsdokumentationsquote von IT-Applikationen Ist/Soll	Prozent		Fehlende Informationen aufgrund unvollständiger Dokumentationen
Anzahl der Plausibilitätsprüfungen der Daten in den IT-Applikationen Ist/Soll	Prozent	Abweichung der Anzahl der Plausibilitätsprüfungen	Mangelhafte Datenqualität
Occupancy pro Hotline Ist/Soll	Prozent		Verfügbarkeit des Helpdesk Callcenter
Aktualität der Zugriffs- und Zulassungsrechte Ist/Soll	Prozent		Verletzung der Sorgfaltspflicht durch verantwortliche Mitarbeiter
Quote der „Super-User“	Prozent	Anzahl der „Super-User“ / Gesamtanzahl der User	Zu hoch gesetzte Rechte
Anteil User-Dokumentationen älter als 12 Monate	Prozent	Gesamtanzahl der User-Dokumentationen; Anzahl der User-Dokumentationen, die seit zwölf Monaten nicht aktualisiert wurden	Falsche Informationen aufgrund nicht aktuellen User-Dokumentationen
User-Dokumentationsquote Ist/Soll	Prozent	Soll-Anzahl der User-Dokumentationen; tatsächlich vorhandene User-Dokumentationen	Mangelhafte Informationen aufgrund unvollständiger User-Dokumentationen
IT-Security-Maßnahmen Ist/Soll	Prozent	Temporärer KRI	Häufigkeit der Sicherheitsmaßnahmen im IT-Bereich
Netzwerk-Security-Maßnahmen Ist/Soll	Prozent	Temporärer KRI	Häufigkeit der Netzwerk-Sicherheitsmaßnahmen
IT-Funktionalität Ist/Soll	Prozent	Unfähigkeit der Systeme, gewisse Funktionen auszuführen	Ungenügende Funktionalität und Verfügbarkeit der IT-Systeme
Redundanzquote im IT-Bereich Ist/Soll	Prozent	Sicherung der wichtigen Informationen durch doppelte Speicherung	Verlust der Informationen beim Systemausfall
Redundanzquote im IT-Bereich	Prozent	Verschiedene IT-Systeme mit den gleichen Informationen, etc.	Mangelhaftes IT-Architekturmanagement
Anzahl der Hacker-Angriffe pro Periode	Zahl		Nur über Ereignis messbar

- Die Ausbildung als solche bestimmt die Qualität der Mitarbeiter. Dieser Punkt umfasst sowohl die Ausbildung an Schulen und Universitäten als auch die darauf folgende berufsbegleitende Weiterbildung. Sie bestimmen den qualitativen Stand der Mitarbeiterinnen und Mitarbeiter und sind somit entscheidend für den Risikogehalt, der durch die Personalausstattung hervorgerufen wird.
- Die Motivation darf als Risikotreiber nicht fehlen. Motivierte Mitarbeiterinnen und Mitarbeiter sorgen bereits selbst dafür, dass ihr Bildungsstand auf einem aktuellen Stand bleibt. Wer motiviert ist, nimmt außerdem viel mehr auf und versucht die Prozesse, für die er verantwortlich ist, ständig zu optimieren.
- Probleme mit der Qualität und Quantität der Personalausstattung können auch durch eine falsche Selektion bei neuen Mitarbeitern auftreten. Je weniger von den geforderten Kenntnissen und Fähigkeiten durch einen neuen Mitarbeiter mitgebracht werden, umso schwieriger wird es, dem definierten Qualitätsanspruch gerecht zu werden.

Dieses Beispiel verdeutlicht, dass die Identifikation von Risikotreibern keine einfache, jedoch eine machbare Aufgabe ist. Es können noch weitere Risikotreiber für die besprochenen Ursachekategorien gefunden werden, die ebenfalls aufgenommen werden können. Die Effizienz setzt dieser Aktivität eine natürliche Grenze, aber die Qualität der Indikatoren ist von der Identifizierung der wichtigen Risikotreiber abhängig.

Nun reicht es nicht aus, die Risikotreiber zu identifizieren – sie müssen auch messbar sein. Es ist vorteilhaft, wenn die Werte objektiv und quantitativ bestimmt werden können, denn das vermeidet viele Nachfragen von betroffenen Kollegen. Bei der Analyse der Risikotreiber für das Personalausstattungsrisiko fällt sofort auf, dass nicht jede gedachte Lösung in der Praxis umgesetzt werden kann.

Es handelt sich hierbei oft um Einschränkungen, die zum Beispiel durch das Betriebsverfassungsgesetz oder auch durch unternehmensspezifische Vertriebsvereinbarungen auferlegt sind. Es ist zum Beispiel in Deutschland nicht möglich, Schlüsselpersonal zu bestimmen und diese Bestimmung in einer Akte festzuhalten. Dies würde schnell einer verdeckten Mitarbeiterpotenzialbeurteilung gleichkommen.

Besonders oft wird nach der Messbarkeit der Mitarbeiter-Motivation gefragt. Diese Frage ist berechtigt, da Motivationsprobleme sich oftmals schlecht messen und außerdem nur beheben lassen, wenn sie frühzeitig entdeckt worden sind. Es gibt Umfragen, deren Auswertung der Unternehmensleitung ein Bild über die Motivation der Mitarbeiter verschaffen soll. Diese Umfragen sind meistens nur bedingt geeignet, die wirklichen Motivationsprobleme zu erkennen. Es gibt verschiedene Verzerrungen, die hier auftreten können:

- Suggestive Fragen, also Fragen, die Antworten in eine gewisse Richtung führen
- Unsicherheit bezüglich der Anonymität, insbesondere dann, wenn die Beantwortung über das firmeneigene Intranet durchgeführt wird
- Unzureichendes Wollen oder Können der befragten Mitarbeiter, ihre wirkliche Gefühlslage nur mit Hilfe der vorgegebenen Fragen und Antwortmöglichkeiten abzubilden
- Fehlen der notwendigen Transparenz bezüglich der Auswertung. Die befragten Mitarbeiter erhalten zum Beispiel die Auswertungen nicht.

Um die Motivation einigermaßen geeignet abbilden zu können, wird ein Mix unterschiedlicher Elemente benötigt. Auch hier sollte man berücksichtigen, dass es eine adäquate Reaktionszeit gibt. Die Umfrage – wenn richtig entworfen – ist ein Element. Nun sollte man sich Gedanken machen, an welcher Stelle sich ein Motivationsverlust bemerkbar macht. Ein Motivationsverlust führt in der Regel zu einer begrenzten Loyalität. Die Mitarbeiterinnen und Mitarbeiter spüren, dass das Unternehmen ihnen gegenüber nicht die gewünschte Loyalität aufweist und deshalb schrauben sie ihr Engagement ebenfalls zurück.

Nun stellt sich die Frage, an welcher Stelle eine solche Veränderung festgestellt werden kann. So könnte etwa die Anzahl der neuen oder prämierten Ideen ein Indikator sein. Wenn die Mitarbeiterinnen und Mitarbeiter nicht mehr „richtig bei der Stange sind“, dann werden sie sich weniger mit der Zukunftssicherung der Firma auseinander setzen.

Die Produktinnovationsquote könnte ebenfalls als Kennzahl zur Identifizierung des Motivationsverlustes genommen werden. Weitere Indikatoren sind beispielsweise die Krankheitsquote (außer in wirtschaftlich angespannten Zeiten), die Überstundenquote (sie wird bei Motivationsverlust eher zurückfallen) oder die Fehlerquote (wer nicht mehr motiviert ist, ist oft nicht so konzentriert). Die Kennzahl „Fluktuationsquote“ erlaubt dagegen keine Reaktionszeit und ist daher weniger als Frühwarnindikator geeignet.

Neben der Umfrage unter den Mitarbeitern ist es sicherlich sinnvoll, die Führungskräfte, die Personalabteilung und eventuelle Vertrauensleute um eine Einschätzung der Motivation der Belegschaft zu bitten, da die unterschiedlichen Perspektiven das Gesamtbild vervollständigen. Der Mix kann sicherlich noch mehr Elemente umfassen, um das gesamte Motivationsbild darzustellen. □

5. Fazit und Ausblick

Frühwarnsysteme sind eine wesentliche und wichtige Komponente eines modernen und proaktiven Risikomanagement-Systems. Bis in die jüngste Vergangenheit dominierte (auch bei Banken) nicht selten ein eher reaktives Risikomanagement: Anstatt einen Blick auf Frühwarnindikatoren zu werfen, erfolgte die Unternehmenssteuerung eher durch einen Blick in den Rückspiegel. Reagiert wurde bei diversen Unternehmens- oder Beinahezusammenbrüchen – wenn überhaupt – erst, als die Katastrophe bereits eingetreten war.

Frühwarnsysteme setzen früher ein und sollen rechtzeitig auf latente (d. h. verdeckt bereits vorhandene) Risiken hinweisen, so dass noch hinreichend Zeit für die Ergreifung geeigneter Maßnahmen zur Abwendung oder Reduzierung der Bedrohung besteht. Frühwarnsysteme verschaffen dem Unternehmen Zeit für Reaktionen und optimieren somit die Steuerbarkeit eines Unternehmens, d. h. sie tragen zur Reduzierung potenzieller „Überraschungen“ bzw. Risiken bei. Hierdurch kann die Entwicklung des Unternehmenswertes stabilisiert und gesteigert werden.

In diesem Kontext ist jedoch auch auf das immanente Problem aller Frühwarnsysteme hinzuweisen. Da Risiken stark von unserer individuellen Risikowahrnehmung, also von unseren Urteilen, Meinungen, Erfahrungen, kulturellen Werten, Moralvorstellungen usw. abhängen, werden die Signale eines Frühwarnsystems auch aus einem höchst subjektiven

Blickwinkel wahrgenommen. Unsere Sinne konstruieren ein Bild einer Realität und gaukeln uns eine subjektive Wirklichkeit vor. Ob etwas als Gefahr betrachtet wird, entscheiden erst die individuellen und gesellschaftlichen Bewertungen.

Da sich die Risikowahrnehmung stetig wandelt, ist auch die Risikolandkarte einer permanenten und immer schnelleren Veränderung unterworfen. Insbesondere Phantomrisiken resultieren aus gesellschaftlicher Ungewissheit und individueller Risikowahrnehmung. Was für den Einen ein Risiko ist, braucht für den Anderen noch lange keines zu sein. Hierbei kann ein ursächlicher Zusammenhang (Kausalität) zwischen Ereignis und Schaden nicht nachgewiesen werden, vielmehr basieren Phantomrisiken auf Vermutungen. Gleichzeitig wird das Gefährdungspotenzial aufgrund der unterschiedlichen Betroffenheit und der ungleichen Verteilung der Verluste divergierend wahrgenommen.

Effiziente Frühwarnsysteme verstärken Signale nicht durch Extrapolation von – möglicherweise irrelevanten – Einzelinformationen, sondern durch die Aggregation vieler, interdisziplinärer Informationen zu einem Gesamtbild. Kommunikation heißt vor allem auch, sich in sein Gegenüber hinein zu versetzen und über den eigenen Tellerrand zu schauen. Dann werden manche Gespenster zu Hirngespinsten – und manche zu realen Risiken.

Literaturverzeichnis sowie weiterführende Literaturhinweise:

Ansoff, H. I. (1976): *Managing Surprise and Discontinuity – Strategic Response to Weak Signals (dt. Übersetzung: Die Bewältigung von Überraschungen – Strategische Reaktionen auf schwache Signale), in: Zeitschrift für betriebswirtschaftliche Forschung 28 (1976), S. 129-152.*

Brink, G. J. van den (2004): *Alles im grünen Bereich, in: RISKNEWS 01/2004*

Brink, G. J. van den (2002): *Operational Risk, The new challenge for Banks, Palgrave Publishers Ltd, Basingstoke, Hampshire (UK).*

Committee of Sponsoring Organizations of the treadway Commission (COSO) (1992): *Internal Control – Integrated Framework, Jersey City.*

Hoffman, D. G (2002):, *Managing operational risk, 20 Firmwide Best Practice Strategies, New York.*

Krystek, U.; Müller, M. (1999): *Frühaufklärungssysteme – Spezielle Informationssysteme zur Erfüllung der Risikokontrollpflicht nach KonTraG, in: Controlling, H. 4/5 (1999), S. 177-183.*

Romeike, F. (2004a): *Lexikon Risiko-Management, Weinheim.*

Romeike, F. (2004b): *Integration des Managements der operationellen Risiken in die Gesamtrisikosteuerung, in: Banking and Information Technology - A Strategic Report for Top Management, Band 5, Heft 3 (2004b), S. 41 – 54.*

Romeike, F.; Finke, R. (2003): *Erfolgsfaktor Risiko-Management – Chance für Industrie und Handel, Wiesbaden.*

Schweizerische Rückversicherungs-Gesellschaft: *Risikolandschaft der Zukunft, Zürich 2004.*

Autoren:

Frank Romeike ist verantwortlicher Chefredakteur der Zeitschrift RISIKO MANAGER, Vorstand der Risk Management Association e.V. (RMA e.V.) sowie Lehrbeauftragter an verschiedenen Hochschulen.
Dr. Gerrit Jan van den Brink ist Head of Operational Risk Control der Dresdner Bank AG und Lehrbeauftragter an der Johann-Wolfgang Goethe Universität und der Hochschule für Bankwirtschaft in Frankfurt am Main.

TICKER +++ TICKER +++ TICKER+++ TICKER +++ TICKER

+++ Das Committee of European Banking Supervisors (**CEBS**) hat seinen Jahresbericht 2005 veröffentlicht. Neben der Darstellung und Bewertung der Arbeit des Gremiums im vergangenen Jahr enthält dieser auch grundlegende Informationen zur Struktur und Aufgaben des CEBS und vermittelt einen Ausblick auf künftige Projekte. Das Dokument steht unter www.c-ebs.org zum Download zur Verfügung +++ Die Ratingagentur Moody's beurteilt die kurzfristigen Aussichten für **asiatische Banken** als stabil. Ausschlaggebend für die positive Einschätzung des Sektors ist vor allem die Tatsache, dass sich das Risikomanagement der Finanzinstitute verbessert hat und die Volkswirtschaften der Region inzwischen offener, liberaler und besser diversifiziert sind. +++ Die **Reuters Group** hat das Unternehmen Application Networks, einen Anbieter von Risikomanagement Software, gekauft. Mit der Übernahme strebt Reuters eine Beschleunigung des Wachstums im Bereich „Trade and Risk Management" an. Der Kaufpreis betrug 41 Millionen US-Dollar. +++ **Phishing** – also das „Abgreifen" geheimer Zugangsdaten wie PINs oder TANs mit Hilfe gefälschter E-Mails und Webformulare – erfreut sich vor allem in Deutschland steigender Beliebtheit. Nach aktuellen Zahlen der Virenschutzfirma RSA Security stieg der „Marktanteil" der Phishing-Angriffe auf Deutsche Unternehmen im vergangenen Jahr von acht auf 14 Prozent. Im weltweiten Vergleich belegt Deutschland damit den zweiten Platz. Unangefochtener Spitzenreiter sind die USA mit 54 Prozent der entdeckten Phishing-Angriffe. Mit einem Anteil von 74 Prozent waren vor allem amerikanische Banken das Ziel der Internet-Betrüger. Auf deutsche Finanzinstitute zielten elf Prozent der Attacken. Insgesamt wurden im vergangenen Jahr weltweit 157 Unternehmen aus dem Finanzsektor angegriffen. +++ Die Credit Suisse Group verkauft ihre Versicherungstochter **Winterthur** für 12,3 Milliarden Franken (7,9 Milliarden Euro) in bar an den französischen Axa-Konzern. Darüber hinaus übernehmen die Franzosen Schulden in Höhe von gut einer Milliarde Franken. Durch die Winterthur-Übernahme stärkt die Axa vor allem ihr Lebens- und Krankenversicherungsgeschäft in Deutschland und der Schweiz. +++ Laut einer Mitteilung des Anti-Virus-Software-Anbieters Kaspersky Labs wurde in der Nacht zum 13. Juni 2006 der 200.000. **Computer-Virus** registriert. Ein Ende der Verbreitung ist damit allerdings nicht in Sicht: Einen Tag später waren bereits knapp 200.300 bekannte Viren verzeichnet. +++ Vor der CSU-Landesgruppe im Deutschen Bundestag äußerte sich Stephan Götzl, Präsident des Genossenschaftsverbandes Bayern (GVB), kritisch zur Rolle der Bundesanstalt für Finanzdienstleistungsaufsicht (**BaFin**). Götzl sagte, die Bafin „... könne einem sehr wohl als Prüfungs-Perpetuum Mobile erscheinen." Er wies darauf hin, dass zwischen 2003 und 2005 die Zahl der Beschäftigten in der Behörde um über 30 Prozent auf mittlerweile 1.631 Mitarbeiter zugenommen hat. Götzl forderte weiterhin, die BaFin sollte an den Kosten der durch sie anberaumten Sonderprüfungen beteiligt werden. +++ Weltbankpräsident **Paul D. Wolfowitz** will Bolivien und andere lateinamerikanische Länder auch dann mit Beratung und Krediten unterstützen, wenn sie ihre Gas- und Ölfelder verstaatlichen. In einem Interview mit der ZEIT sagte er, „... Wünsche nach politisch motivierter Kreditvergabe" seien ihm noch nicht untergekommen. Seiner Meinung nach sei auch im Nahen Osten eine Ausbreitung der Demokratie keine zwingende Voraussetzung für wirtschaftliche Entwicklung: „Sie können bereits viele Reformen und eine Öffnung des ökonomischen Systems erreichen – ohne politischen Wandel, den diese Länder vielleicht im Augenblick nicht wollen." +++ Laut einer aktuellen Studie des Chipherstellers Intel sehen 54 Prozent der IT-Manager in Deutschland das **Computernetzwerk** ihres Unternehmens vor allem durch die eigenen Anwender gefährdet. Angriffe von Außen halten demgegenüber nur 34 Prozent der Befragten für die wichtigste Bedrohung. +++

Verstehen jeden Spaß. Aber nicht den RISIKO MANAGER.

Mitarbeiter im Risk Management verstehen den RISIKO MANAGER – als Pflichtlektüre in Banken und Versicherungen. Besorgen Sie sich jetzt die neue Fachzeitschrift mit dem unverzichtbaren Wissen. Ihr kostenloses Probeheft erhalten Sie unter **www.risiko-manager.com**

RISIKO MANAGER

- KREDITRISIKO
- MARKTRISIKO
- OPRISK
- ERM