

Betriebliche Kontinuität als Teil eines integrierten Risikomanagements

In den vergangenen Jahren haben die Begriffe „Risikomanagement“, „Corporate Governance“ und „internes Kontrollsystem“ weitreichende Popularität erlangt. Die Tendenz zur nahezu allumfassenden Kontrolle der Prozesse im Unternehmen wird stärker, zumal die Haftung der Vorstände und Aufsichtsräte ebenfalls erweitert wurde. Es leuchtet ein, dass Vertreter dieser Gruppen einer präventiven Absicherung zuneigen, die ihre Haftungsrisiken minimiert und zugleich eine klare Außenwirkung für das Unternehmen erzeugt. Im Ergebnis führt dieses Vorhaben jedoch häufig zu enorm komplexen und aufwändigen Kontrollsystemen, die durch ausufernde Mechanismen der Überwachung und Freigabe eine eigene Form der Bürokratie schaffen. Es ist ja gerade die Geschäftstätigkeit an sich, die ein unternehmerisches Risiko in sich birgt – dieses Risiko gilt es abzuwägen und in geeigneter Form zu begrenzen. Wäre das Kontrollsystem ausschließlich an der Vermeidung jeglicher Risiken ausgerichtet, so könnte dies in letzter Konsequenz nur zur Einstellung des Betriebs führen.



Autor

**Rolf von
Rössing**

ist als Partner im Bereich Advisory bei KPMG beschäftigt und betreut internationale Projekte in Prüfung und risikoorientierter Beratung. Er ist Vorstandsmitglied des Business Continuity Institute und als Mitglied in verschiedenen internationalen Gremien zu Business Continuity und Security tätig.

Ausgehend von der Prämisse des Fortbestands – englisch auch als „Going Concern“ bezeichnet – steht für den Risikomanager die Existenzsicherung des Unternehmens im Vordergrund. Risiken oder Krisen, die den Fortbestand gefährden, sind grundsätzlich auszuschließen. Diese Prämisse lässt sich ohne Schwierigkeiten als Prinzip der betrieblichen Kontinuität neu formulieren. Sowohl unter Normalbedingungen als auch unter erschwerten Bedingungen fordert dieses Prinzip, dass der Geschäftsbetrieb fortgesetzt wird und dass keine Bestandsgefährdung eintreten darf [AktG § 91 (2) iVm § 93, sinngemäß auch im GmbHG]. Der vorausschauende Unternehmer muss daher unter Wahrung der kaufmännischen Grundsätze geeignete Absicherungsmaßnahmen im Sinne der betrieblichen Kontinuität treffen.

Im Banken- und Finanzsektor ergeben sich vielfältige Anforderungen an das Risikomanagement, die unter anderem durch Bankenaufsicht, Basel II und internationale Vorschriften geregelt sind. Auch in anderen Branchen existiert eine Vielzahl einzelner Regelungen, die in der ein oder anderen Form eine Auseinandersetzung mit Risiken fordern – seien es Störfallverordnungen, kommunaler Katastrophenschutz oder besondere Regularien für gefahrgeneigte Indus-

trien. Bei näherem Hinsehen lassen sich diese jedoch auf einige Grundgedanken zurückführen.

Risikomanagement und Krisenereignisse

Das herkömmliche Risikomanagement bezieht sich im Regelfall auf Ereignisse, die in Form von Listen oder Katalogen aufgenommen und sodann bewertet werden. Als Risiken werden dabei die Ereignisse wahrgenommen, die sich der Kontrolle des Unternehmens entziehen, also außerhalb des Bezugssystems der Unternehmung stehen. Teilweise werden auch interne Ereignisse einbezogen, wenn sie subjektiv nahe liegend sind, beispielsweise unerlaubte Handlungen des Personals, Unfälle oder unabsichtliche Fehler. Im Verlauf der Zeit ist das Risikomanagement folglich mit einer mehr oder (seltener) minder großen Liste der Ereignisse konfrontiert, die durch Prävention zu vermeiden sind. Für Bedrohungen und Risiken katastrophalen Ausmaßes wird zumindest eine Schadensbegrenzung angestrebt.

Das Chancen-Risiko-Kalkül neigt sich hier zu einer Seite: unter der Annahme, das Geschäft in seiner bestehenden Form gegen Risiken schützen zu müssen, stehen zwangsläufig die Risiko-

Aversion und die Vermeidung im Vordergrund. In der Praxis ist immer wieder zu beobachten, dass „Risikomanagement“ sich darin erschöpft, bei einer Wahrnehmung des Risikos als „hoch“ durch immer neue Kontrollmaßnahmen und weitere Abstimmungsschleifen eine Absicherung zu schaffen. Diese Denkweise basiert auf der Vermutung, durch zusätzliche Kontrolle das Eintreten unangenehmer Ereignisse verhindern zu können. Die Erfahrung zeigt leider, dass diese Vermutung falsch ist: immer wieder werden Unternehmen von Krisen überrascht und erholen sich nicht von den Folgen. Zwischen Anspruch und Wirklichkeit des traditionellen Risikomanagements besteht also eine offensichtliche Diskrepanz.

Kontinuität in robusten Unternehmen

An dieser Stelle ist es nützlich, die ereignisbezogene Planung zu verlassen und das Bezugssystem der Unternehmung näher in Augenschein zu nehmen. Grundvoraussetzung der betrieblichen Kontinuität – auch unter widrigen Umständen – ist die Robustheit des Geschäftsmodells und seiner Prozesse. Dies bedingt auch, dass die Interaktion mit dem Umfeld des Unternehmens (Märkte, Kunden und Dienstleister) fortgesetzt wird. Schlussendlich sind auch jene Ressourcen verfügbar zu halten, derer sich die Unternehmung bedient, um das Geschäft am Laufen zu halten.

Unternehmen und Umfeld lassen sich recht simpel durch das Prozess- und Marktmodell von Porter abbilden; dieses Modell ist für die Zwecke des betrieblichen Kontinuitätsmanagements vollausreichend. Nach der Darstellung des Geschäfts in dieser Form sind die Bereiche zu bestimmen, die für die betriebliche Kontinuität in zeitlicher und finanzieller Hinsicht kritisch sind. Kerngeschäft und wichtige Unterstützungsfunktionen gehören zweifellos dazu; es kann aber bei näherem Hinsehen auch andere Bereiche des Unternehmens geben, die je nach Saisonalität und Verflechtung der Prozesse untereinander als kritisch einzustufen sind. Stört oder unterbricht man einen oder mehrere der kritischen Prozesse, tritt zunächst ein Schaden ein, der mit Verstreichen der Zeit immer größer und schließlich bestandsgefährdend wird. Bei genauem Hinsehen zeigt sich, dass diese Erkenntnis ereignisunabhängig gilt. Was immer das auslösende Ereignis gewesen sein mag – die Wirkung ist immer dieselbe. Die betriebliche Kontinuität wird nachhaltig gestört, und es kommt zu Konsequenzen bis hin zur Insolvenz.

Als Ergebnis dieser prozessorientierten Sicht der Kontinuität liegt ein ereignisunabhängiges Modell vor, das die „Verwundbarkeit“ des Bezugssystems Unternehmung gegenüber – bisher unbekanntem – Einflüssen darstellt. Die Wirkung ist bekannt und die Überlebensfähigkeit des Unternehmens kann in zeitlicher und finanzieller Hinsicht abgeschätzt werden. In der Sprache des betrieblichen Kontinuitätsmanagements wird diese Stufe als „Business Impact Analysis“ bezeichnet, während man im traditionellen Risikomanagement eher von einer Risiko-Diagnose sprechen wird.

Meist zeigt sich nach einer ersten Analyse des Geschäftsmodells, dass das Prinzip der betrieblichen Kontinuität nur unzureichend gewährleistet ist. Der Grund liegt in erster Linie in der zunehmenden Optimierung moderner Geschäftsprozesse. Kostensenkungen, Restrukturierungen, Automatisierung und Outsourcing gehören zu den Instrumenten, die eine höhere Profitabilität versprechen, zugleich aber Probleme aufwerfen. Natürliche Pufferzonen werden zugunsten einer schlankeren Organisation beseitigt. Häufig resultiert daraus eine insgesamt höhere Anfälligkeit des Unternehmens gegenüber kleinen oder größeren Abweichungen in der Umgebung. Ist der Betrieb (und seine Kontinuität) auch nur für kurze Zeit gestört, bauen sich mit großer Geschwindigkeit Schadenspotenziale auf, die in einer eher robust angelegten Unternehmung geringer ausfallen würden. Um diesen Risiken zu begegnen und das Prinzip der betrieblichen Kontinuität aufrechtzuerhalten, sind offenkundig Maßnahmen erforderlich.

Kontinuitätsmanagement und Risikomanagement

An diesem Punkt stellt sich in der Praxis die Frage nach dem optimalen Maßnahmenbündel, das die Robustheit der Unternehmung maximiert und zu vernünftigen Kosten vertretbar ist. Im Rückblick auf das traditionelle Risikomanagement gilt, dass nicht alles abgesichert werden kann. Der Satz „man kann sich nicht gegen alles schützen“ hat insofern durchaus seine Richtigkeit. Eine vollständige Vermeidung aller Risiken ist nicht nur unmöglich, sondern aus betriebswirtschaftlichen Gründen auch gar nicht wünschenswert. Es gilt vielmehr, das Geschäftsmodell genau so robust zu halten, dass es gegen Schäden und Störungen bis zu einem bestimmten Ausmaß weitgehend unempfindlich ist.

Anhand dieser Überlegungen wird deutlich, dass erst nach der Feststellung der Anfälligkeit

ten im Unternehmen eine genauere Betrachtung der auslösenden Faktoren erfolgen kann. Ohne den Zwischenschritt der Business-Impact-Analyse wäre die Anzahl möglicher Ereignisse und Einflussfaktoren unüberschaubar. Das traditionelle Risikomanagement versuchte in der Vergangenheit, durch die Aufzählung von Ereignissen und die Einschätzung der Eintrittswahrscheinlichkeit einen Weg zur Einordnung interner und externer Bedrohungen zu finden. Die Ergebnisse erwiesen sich allerdings als nur begrenzt brauchbar für die Praxis im Unternehmen, da schlicht zu wenige Daten für eine repräsentative Auswertung verfügbar waren (und sind). Eine nach Wahrscheinlichkeiten abgestufte Bewertung der Risiken führt daher aus der Sicht der betrieblichen Kontinuität nicht weiter: zu groß ist die Gefahr, dass ein nicht berücksichtigtes Krisenereignis zur Bestandsgefährdung führen könnte. Sichert man hingegen die Firma gegen eine maximale Anzahl möglicher Bedrohungen, führt dies schnell zu betriebswirtschaftlich ungünstigen Szenarien.

Der Ausweg ist überraschend simpel: durch Clustering der Risiken werden diese nur dort als relevant angesetzt, wo sie tatsächlich Auswirkungen entfalten können. Es mag schwierig sein, für ein ganzes Unternehmen die Wirkung eines Brandes zu bestimmen – für ein beliebiges Büro erweist sich dieselbe Übung als überraschend leicht.

Dabei unterscheidet man zwischen der allgemeinen Wahrscheinlichkeit eines Brandes in der Gegend (diese ist vernachlässigbar) und der konkreten Wahrscheinlichkeit im betrachteten Areal (das vermutlich bereits durch Schutzmaßnahmen gehärtet ist). Ähnliche Betrachtungen lassen sich auch für andere Ereignisse anstellen, die bei einer subjektiven „Risiko-Diagnose“ in den Sinn kommen. Durch strenges Clustering lässt sich die Anzahl wirklich relevanter Auslöser für eine Krise erfahrungsgemäß deutlich verringern.

Die so gewonnenen Erkenntnisse haben bis zu diesem Punkt einerseits das Schadenspotenzial, andererseits die realistischen Bedrohungs- und Krisenszenarien zumindest im Groben festgelegt. Damit ist die Betrachtung des Unternehmens als Bezugssystem erreicht. Ein solches Zwischenergebnis löst im Übrigen eines der Zentralprobleme, die bei der Verbindung zwischen betrieblicher Kontinuität und traditionellem Risikomanagement auftreten: Risikomanager aus der Welt der Versicherungen denken in Portfolio-Theorien und Verteilung der erkannten

Risiken über zahlreiche Akteure hinweg, während Unternehmen das eigene Interesse in den Vordergrund stellen müssen.

Das betriebliche Kontinuitätsmanagement beschränkt sich nicht auf die diagnostischen Schritte, sondern versucht eine Absicherung des Unternehmens gegenüber bekannten und unbekanntem Krisenszenarien. Getreu dem Grundsatz der Robustheit und jederzeitigen Fortführung der Geschäftstätigkeit ist keine Perfektion gefordert; es soll allerdings das wirtschaftlich Vernünftige unternommen werden, um eine möglichst hohe Krisenfestigkeit zu gewährleisten. Der Wissensstand nach Business Impact Analysis und Risiko-Clustering mündet in die Modellierung des robusten Unternehmens an sich. Das durch die führenden internationalen Verbände vorgeschlagene Modell wird nachfolgend beschrieben.

Der erste Schritt ist die Ermittlung strategischer Optionen, die bei besonders empfindlichen Prozessen oder Prozessclustern zu einer besseren Abfederung im tatsächlichen Krisenfall führen. Diese lassen sich anhand des Kosten-Nutzen-Verhältnisses kategorisieren, beispielsweise als „kleine“, „mittlere“ und „große“ Lösung. Mit zunehmender Investitionsneigung kann das Risiko im Krisenfall entsprechend weiter begrenzt werden. Gleichzeitig sollte die Investition nicht übermäßig belastend für das Geschäft sein. „Kleine“ Lösungen kennzeichnen fast immer eine investitionsabgeneigte und risiko-freudige Haltung der Unternehmensführung, während „große“ Lösungen eher risiko-averses Verhalten signalisieren und daher häufig in regulierten oder sehr großen Firmen anzutreffen sind. Den perfekten Schutz vor Krisen wird es nie geben – aber mehr Schutz für mehr Geld ist durchaus realisierbar. Wie alle unternehmerischen Entscheidungen ist auch die Absicherung der Firma gegenüber Krisen ein betriebswirtschaftlich kalkulierbares Risiko.

Unternehmensbetrachtung statt IT-Betrachtung

Anhand dieses Modells der betrieblichen Kontinuität und der Risiko-Betrachtung wird eines deutlich: früher übliche Begriffe wie „Notfallplanung“ oder „K-Plan“ greifen zu kurz und können die Anforderungen im Hinblick auf Corporate Governance keineswegs erfüllen. Die in den deutschsprachigen Ländern beharrlich vertretene Fehleinschätzung, es handle sich um ein technisches Thema der EDV, führt im Ausland bestenfalls zu Kopfschütteln, schlimmstenfalls

jedoch zu Verstößen gegen die dort geltenden Vorschriften. Das strategische Handeln im Sinne der betrieblichen Kontinuität betrifft stets das ganze Unternehmen und das Kerngeschäft. Das Delegieren der bis zu diesem Punkt geschilderten Aktivitäten an die IT-Leitung oder technische Abteilungen ist daher nicht nur ein falscher, sondern ein durchaus gefährlicher Weg. Technologie mag in vielen Fällen der Lösungsweg sein – die Motivation, sie einzusetzen, unterliegt jedoch rein betriebswirtschaftlichen Überlegungen. Noch nie hat die Wiederherstellung der IT allein ein Unternehmen gerettet.

Strategische Lösungsvorschläge ermöglichen einen bequemen Brückenschlag zum traditionellen Risikomanagement. Während dort die Vorstellung von Risiko-Vermeidung, -Begrenzung, -Transfer oder -Hinnahme vorherrscht, sind im Sinne der betrieblichen Kontinuität schon die Maßnahmen beschrieben, die beispielsweise für eine Begrenzung oder einen Transfer getroffen werden sollten. Erstere könnte etwa in der Einführung eines stringenten Krisenmanagements bestehen, das im Ernstfall den Schaden gering hält. Der Transfer wiederum könnte durch Auslagerung bestimmter Funktionen an einen Dienstleister erzielt werden. Betrachtet man Kontinuität und Risikomanagement aus strategischer Sicht, stellen sich schon nach kurzer Zeit viele Gemeinsamkeiten heraus.

Fast alle Entscheidungen, die der Risikomanager im Unternehmen trifft, dienen auch der betrieblichen Kontinuität. Es bedarf lediglich einer anderen Sprache und eines etwas anderen Zugangs, um die Gemeinsamkeiten im Sinne eines integrierten Risikomanagements zu erkennen.

Entsprechend dieser Annahme ist es auch die Entscheidung der oberen Führung im Unternehmen, die Maßnahmen des betrieblichen Kontinuitätsmanagements umzusetzen. Dabei liegt ein Risiko-Kalkül zugrunde, das durch Business Impact Analysis und Risiko-Clustering sehr viel transparenter gemacht werden kann, als es bei einer isolierten Sicht auf Prävention und Risiken möglich wäre. Die Entscheidungssicherheit steigt und das Management im Unternehmen kann auch zunächst fachfremde Sachverhalte zumindest in Zahlen und Schadenspotenzialen begreifen. Die Integration macht jedoch hier nicht halt, sondern setzt sich in weiteren Schritten fort. Ziel eines integrierten Risikomanagements ist nicht nur die Festlegung einer strategischen Wunschvorstellung, sondern auch die praktische Umsetzung im gegebenen Geschäftsmodell.

Umsetzung des Kontinuitätsgedankens

Hat sich die Führung im Unternehmen für eine finanziell und technisch optimale Lösung entschieden, ist diese im Wege der eigentlichen Kontinuitätsplanung umzusetzen. Die Ausarbeitung der strategischen Vision in Form von Einzelplänen wird in der englischsprachigen Literatur noch häufig als „Business Continuity Planning“ (BCP) bezeichnet.

Verbindungen zum traditionellen Risikomanagement sind dadurch gegeben, dass einzelne Pläne sich bestimmten Risiken und Prozessen widmen. Maßnahmen können aus der Sicht des Risikomanagers in die üblichen Kategorien eingeordnet werden. Für die Detailplanung der betrieblichen Kontinuität werden häufig die so genannten „Disaster Timeline“-Modelle eingesetzt, die anhand eines Zeitstrahls die Vorgänge nach Eintritt eines krisenhaften Zustands skizzieren. Typische Planvorlagen umfassen Sofortmaßnahmen, Wiederanlaufpläne und Wiederherstellungspläne. Die Einzelplanung ist zugleich das am ehesten etablierte Teilgebiet des betrieblichen Kontinuitätsmanagements, da Methode und Ergebnis auf militärische und industrielle Krisenszenarien des 19. Jahrhunderts zurückgehen. Daraus erklärt sich auch die im deutschsprachigen Raum oft intuitiv geäußerte Vorliebe für die operative Planung.

Anhand der zuvor beschriebenen Voraussetzungen wird allerdings deutlich, dass ohne strategisches Gerüst keine sinnvolle Detailplanung möglich ist. Das entscheidende Element liegt hier im Überbau, der eine strategisch richtige Zuweisung knapper Ressourcen und Mittel im Ernstfall sicherstellt. Gäbe es diese strategische Richtung nicht, wären Einzelpläne von vorneherein zum Scheitern verurteilt. Auch im Vergleich zum traditionellen Risikomanagement zeigt sich, dass in der Krise Prioritäten gesetzt werden müssen, die unter Umständen zur Aufgabe bestimmter Unternehmensteile zwingen können, zumindest aber das „Leben mit Einschränkungen“ durchsetzen. Auf der Heide [1989] verdeutlichte dies wegweisend anhand der schwierigen Entscheidung über die medizinische Erstversorgung in Krisenfällen – ganz ähnlich hat man sich die Frage vorzustellen, was im Unternehmen am ehesten gerettet werden sollte. Die Einzelplanung hat also einen hohen, aber keineswegs ausschließlichen Stellenwert im Lebenszyklus der betrieblichen Kontinuität und Robustheit. Detailpläne sind lediglich Umset-

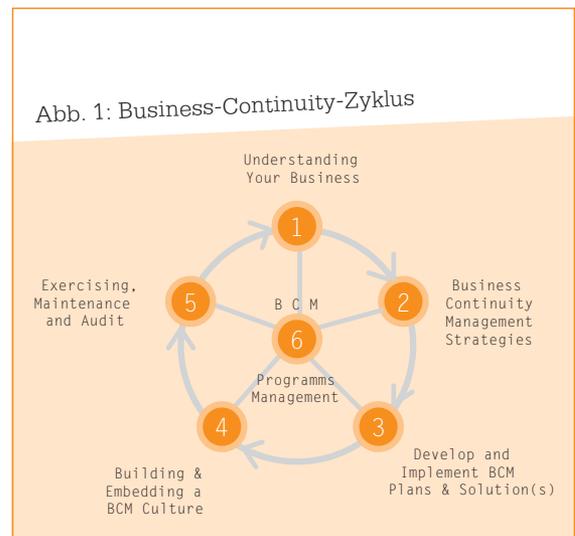
zung eines übergeordneten Gedankens, der von der Führung zu bestimmen ist.

Mit der Vollendung einer detaillierten Kontinuitätsplanung sind die Weichen für die praktische Erprobung und die Verbreitung des Robustheitsgedankens im Unternehmen gestellt. Die „Version 1“ eines Kontinuitätsplans ist zu testen, nachzubessern und wiederum zu testen. Test und Wartung bilden eine Schleife, die schrittweise zu einem höheren Reifegrad des Unternehmens führt. In vielen Fällen wird in diese Schleife auch die interne Revision eingebunden, um möglichst unabhängige Bewertungen zu ermöglichen. In der Praxis wird besonderer Wert auf die Durchführung umfassender Tests gelegt; beispielsweise sind im Bankensektor größere Krisensimulationen regelmäßig vorgesehen. Ziel dieser relativ aufwändigen Test- und Wartungsschleifen ist die Schaffung eines unternehmensweiten Bewusstseins für die Krise und die Robustheit des eigenen Unternehmens – englisch als „Awareness“ bezeichnet. Diese Vorstellung umfasst auch das organisatorische Selbstbewusstsein, das man häufig nach erfolgreich gemeisterten Krisen beobachten kann: Belegschaft und Management treten neuen Bedrohungen gelassener gegenüber, weil sie ja bereits gemeinsam eine Krise überstanden haben. Eine ähnliche psychologische Wirkung soll mit möglichst realistischen Testszenarien erreicht werden.

Der Prozess der Kontinuität

Die betriebliche Kontinuität wird hier also zum Prozess und bleibt nicht länger statisches Planungsmodell. Mit zunehmender Reife können Investitionen genauer gesteuert werden und die BKM-Fähigkeit des Unternehmens nimmt zu. Sowohl technisch als auch betriebswirtschaftlich ist eine höhere Krisenfestigkeit erreicht.

Der Gedanke der Kontinuität ist jedoch eng verzahnt mit dem internen Risikomanagement. Ein robustes Unternehmen kann aus Sicht des Managements eher risiko-freudig agieren, zumal auch in einer Krise der Bestand voraussichtlich nicht gefährdet wird. Ein Unternehmen ohne dieses Selbstvertrauen wird zu anderen Mechanismen greifen, um die Situation zu erklären und Risiken möglichst von vorneherein zu vermeiden. Turner [1976], Pauchant und Mitroff [1992], Mitroff und Pearson [1993] und viele Autoren der eher soziologisch geprägten „Disaster Research“-Schule prägten den Begriff der „krisengeneigten Organisation“ (Crisis-prone Organization), um die Denkmuster zu beschreiben, die



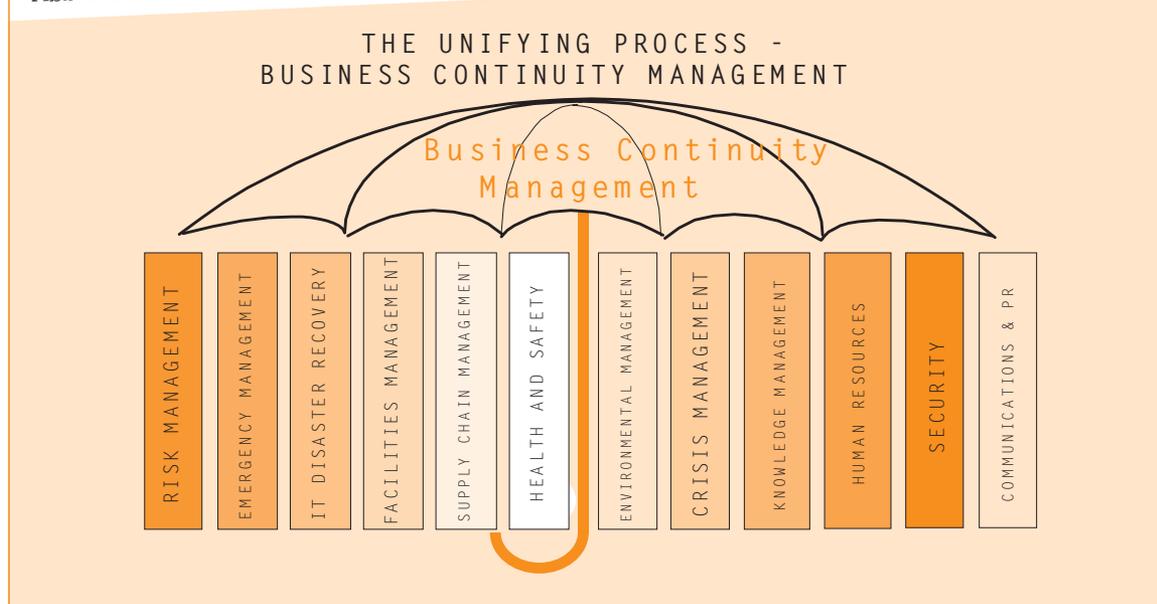
bei einer allgemeinen Ablehnung des Kontinuitäts- und Risiko-Gedankens auftreten. Bereits zuvor hatte Simon [1957] den noch wesentlich schärferen Begriff der „beschränkten Rationalität“ (Bounded Rationality) geprägt, um das selbstbezogene Argumentieren und Handeln der Unternehmensführung in bestimmten Unternehmenskulturen zu kennzeichnen.

Der Prozess der betrieblichen Kontinuität im weitesten Sinne führt mithin dazu, dass Risiken und Gefährdungen objektivierbar und realistisch betrachtet werden – eine verdrängende oder einseitige Sicht der Dinge wird verhindert. Die in der Literatur geschilderten Phänomene können bereits zu einem frühen Zeitpunkt abgefangen werden, da aus der Sicht des Unternehmens eine offene, aber präzise Risiko-Einschätzung zu treffen ist.

Das Business Continuity Institute (BCI) schlägt in den so genannten „Good Practice Guidelines“ [BCI 2005] einen Lebenszyklus-Ansatz vor, um den Prozess der Kontinuität zu beschreiben. Der Lebenszyklus (vgl. Abb. 1) findet sich auch in der Spezifikation BS PAS 56 der British Standards Institution wieder [BSI 2003].

Das Risikomanagement als Bestandteil des grundlegenden Kontinuitätsmanagements bildet dabei eine stets wiederkehrende Phase, die zusammen mit der Business Impact Analysis eine untrennbare Basis für spätere strategische Entscheidungen bildet. Risiken, die durch die Betrachtung der Wirkungen auf das Unternehmen objektiv bewertet werden können, sind zugleich im Sinne des Risikomanagements qualifiziert, da die möglichen Maßnahmen zu ihrer Beherrschung vollständig integriert sind. So gehen beispielsweise Präventivmaßnahmen eben-

Abb. 2: Komponenten des Business Continuity Management



so in ein Gesamtkonzept der betrieblichen Kontinuität ein wie Transfers oder Risiko-Minderung.

Fazit

Nach wie vor ist in den deutschsprachigen Ländern vor allem die IT-orientierte, rein technische Planung der Kontinuität anzutreffen. Gleichzeitig steht aus den Überlegungen des traditionellen Risikomanagements heraus die Prävention im Vordergrund. Die Vorstellung, durch intensivere Kontrolle und Regelung eine bessere Beherrschbarkeit der Risiken zu erzielen, ist nach wie vor weit verbreitet. Die Erkenntnis, dass sich Unwägbarkeiten und Krisen dennoch nicht ausschließen lassen, setzt sich erst nach und nach durch. Als Konsequenz dieser grundlegenden Perspektive sind Risiko- und Kontinuitätsmanagement häufig organisatorisch getrennt. In vielen Fällen stehen sie sogar in Konkurrenz zu-

einander. Die Gemeinsamkeiten werden oft übersehen, sind jedoch offenkundig. Im Sinne einer Bestandssicherung und Robustheit des Unternehmens gegenüber allfälligen Risiken sind beide Fachdisziplinen miteinander zu verbinden.

Das traditionelle Risikomanagement bleibt ohne die Fähigkeit zum flexiblen Handeln zwangsläufig beschränkt; die betriebliche Kontinuität braucht das Risikomanagement, um strategisch richtige Entscheidungen zu treffen und umzusetzen. Die Anforderungen im Sinne der Corporate Governance zeigen jedoch, dass aus Sicht des Unternehmers kein Unterschied zwischen Risiko- und Kontinuitätsmanagement bestehen darf. Beide Komponenten sind Teil der vorausschauenden Führung und der kaufmännischen Sorgfalt, die den Fortbestand des Unternehmens auch in kritischen Situationen sicherstellen muss. ■

Literaturverzeichnis: Auf der Heide, E.: Disaster Response – Principles of Preparation and Coordination (1989), Online-Ausgabe (2000): Center of Excellence in Disaster Management and Humanitarian Assistance, elektronisch veröffentlicht unter www.paho.org/BritishStandardsInstitution (BSI): BS PAS 56 – Betriebliches Kontinuitätsmanagement; Dt. Übers. d. Originalausgabe, London 2003 / Business Continuity Institute (BCI): Good Practice Guidelines for Business Continuity Management; 2. Aufl., Caversham 2005 / Mitroff, I.; Pearson, C.: Crisis Management – A Diagnostic Guide for Improving Your Organisation's Crisis Preparedness, San Francisco 1993 / Pauchant, T.; Mitroff, I.: Transforming the Crisis-Prone Organisation, San Francisco 1992 / Porter, M. A.: Competitive Strategy – Techniques for Analyzing Industries and Competitors, New York 1980 / Porter, M. A.: Competitive Advantage – Creating and Sustaining Superior Performance, New York 1985 / Simon, H. A.: Administrative Behavior, 2. Aufl., New York 1957 / Turner, B. A.: The Organizational and Interorganizational Development of Disasters, in: Administrative Science Quarterly, 21. Jg., September 1976.