THE AUDIT COMPANY

Quo vadis Risikomanagement?

Unternehmerische Aktivitäten eröffnen zwar große Chancen, bergen aber immer auch große Risiken: Investitionen in neuen Märkten werfen nicht den gewünschten Profit ab? Probleme in der Datenverarbeitung behindern massiv die laufenden Arbeitsprozesse? Der Umsatz eines Unternehmens bricht aufgrund eines massiven Shitstorms ein? Ein Brand zerstört Produktionsanlagen? Ein Unternehmen wird Opfer eines Hackerangriffs?

Mit einem Risikomanagementsystem auf Basis der ISO 31000 können unternehmerische Risiken systematisch im Vorfeld identifiziert, bewertet und bewältigt werden. So enthält jedes Risiko eine potentielle Chance. Daneben bietet dieses Vorgehen in jedem Fall einen zusätzlichen Informationsgewinn für die Unternehmensleitung, weil es parallel zum prozessualen Berichtsweg eine zusätzliche Informationsquelle darstellt, die die Überwachung wichtiger Kennzahlen garantiert und standardisiert.

Deshalb sollte jedes unternehmerische Handeln einen risikobasierten Ansatz aufweisen, der das präventive Denken in den Vordergrund rückt, wie es die zukünftige ISO 9001:2015 fordert. Unternehmen, die aufgrund ihrer Größe, ihrer Komplexität oder der besonderen Forderungen von interessierten Parteien (z. B. Kunden, Mitarbeiter, Gesellschafter, Versicherungen) explizit ein Risikomanagement einführen wollen, sollten sich an der ISO 31000 orientieren, auf die in den Anmerkungen der ISO 9001:2015 verwiesen wird.

Gesetzliche und normative Grundlagen

Die Einführung eines Risikomanagements ist für AGs und größere GmbHs gemäß der gesetzlichen Änderungen des Aktiengesetzes und des Handelsgesetzbuches, die mit dem KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) 1998 eingeführt wurden, Pflicht. Diese Entwicklung zeigt sich auch in Hinsicht auf normative Entwicklungen für internationale Standards.

Normen mit Bezug zur Informationstechnologie (z. B. ISO/IEC 27001 oder ISO/IEC 20000-1) oder für das Gesundheitswesen (ISO 15224) setzen teilweise schon seit vielen Jahren auf Risikomanagement als Grundlage jedes unternehmerischen Handelns. Das Erkennen von Risiken und die Verfolgung der daraus abgeleiteten Maßnahmen sind zentrale Komponenten dieser Normen. Sie stellen die Basis für Unternehmen dar, die nachhaltig ihre Existenz sicherstellen und gleichzeitig die Chance nutzen wollen, für ihre Kunden an Attraktivität zu gewinnen.

Die ISO 31000 beschreibt die Grundsätze und Richtlinien zur Anwendung von Risikomanagement in Organisationen und Unternehmen. Dabei setzt sie den Fokus auf die Eingliederung des Risikomanagementprozesses in ein bereits bestehendes Managementsystem. Auf diese Weise lassen sich die präventiven Maßnahmen des Risikomanagements optimieren. Die Norm dient dabei als Leitfaden und zeigt vielfältige Möglichkeiten der Umsetzung im eigenen Unternehmen auf. Somit eignet sie sich hervorragend als Nachschlagewerk, wenn es darum geht, eine individuelle Strategie und Definition des Risikomanagementprozesses für das eigene Unternehmen zu finden. Ergänzend dazu stellt die ONR 49000-Normenserie „Risikomanagement für Organisationen und Systeme, Anwendung der ISO 31000 in der Praxis“ eine konstruktive Umsetzungshilfe dar.

Normen setzen auf Risikomanagement als Grundlage jedes unternehmerischen Handelns.

Nutzen durch die Einführung eines Risikomanagements nach ISO 31000

Vordergründig wird immer die Bedeutung eines systematischen Compliance-Managements als zentraler Teil eines Risikomanagements hervorgehoben, weil damit eine größere Rechtssicherheit und somit eine Haftungsreduzierung erreicht werden soll.

Mit den Werkzeugen des Risikomanagements wird aber darüber hinaus auch eine Risikokultur geschaffen: Führungskräfte und Mitarbeiter werden sensibilisiert, Dinge aus einer anderen Perspektive zu betrachten und weitere Lösungsansätze in den Blick zu nehmen. Das Bewusstsein, die Ursache eines Risikos genau zu beleuchten, wird verstärkt.

Eine effiziente Risikokultur in einem Unternehmen wirkt sich auch positiv in Hinsicht auf die Erfüllung von aktuellen und zukünftigen Kundenanforderungen aus. Hier ist z. B. die künftige Ausrichtung des Produktportfolios systematisch zu betrachten, damit entscheidende Wettbewerbsvorteile gesichert oder Trends nicht verschlafen werden: Aus Risiken Chancen machen – das ist das Ziel/der Effekt eines risikobasierten Denkansatzes!

Wohl überlegte und organisierte Maßnahmen machen es zudem einfacher, in Notfallsituationen die Geschäftskontinuität zu sichern und damit auch das Ansehen bei den Kunden oder anderen interessierten Parteien zu steigern. Und nicht zuletzt erspart das Verhindern von Gefahrereignissen dem Unternehmen Kosten, die beim Eintritt von Schadensfällen auftreten können. Auch Imageschäden können begrenzt oder ausgeschlossen werden.

THE AUDIT COMPANY

Risikomanagement als Regelprozess – ein an die ISO 31000 angelehntes Beispiel

Der Risikomanagementprozess könnte z. B. folgendermaßen festgelegt und eingeführt werden:

Phase 1: Risikoidentifizierung

Risiken werden mit Methoden und Techniken, die in den Leitfäden beschrieben sind, erkannt und erfasst.

Phase 2: Risikoanalyse und Risikobewertung

Mit einer für das Unternehmen individuell definierten Methode werden die identifizierten Risiken analysiert und bewertet. Diese kann einer einfachen Systematik folgen, bei der die Fragen nach der Eintrittswahrscheinlichkeit und der möglichen Auswirkung des Risikos auf das Unternehmen beantwortet werden.

Phase 3: Risikobeobachtung und Risikobewältigung

Aus den Erkenntnissen der zweiten Phase werden Vorbeugungs- und Korrekturmaßnahmen abgeleitet. Diese könnten folgende Strategien zur Bewältigung des Risikos verfolgen:

- Die Risikovermeidung
- Die Risikoüberwälzung, z. B. an Versicherungen oder über die Vertragsgestaltung
- Die Risikoreduzierung, wenn das Risiko nicht ganz zu vermeiden ist
- Die Risikoakzeptanz, die eine ständige Überwachung zur Folge hat: Hier gilt es, zusätzlich korrektive Maßnahmen zu definieren, um geeignete Möglichkeiten zur Schadensreduzierung, z. B. durch erprobte Notfallpläne, zu haben.

Sobald die Rahmenbedingungen und der Prozess für das Risikomanagement festgelegt sind, beginnt die wichtigste und gleichzeitig schwierigste Phase: der Betrieb des Risikomanagements als Regelprozess, der durch folgende Aspekte geprägt sein könnte:

- Die identifizierten Risiken müssen beobachtet und regelmäßig berichtet werden.
- Es gilt, neue Risiken zu identifizieren und zu melden.
- Schulungen und Awareness-Veranstaltungen werden durchgeführt.
- Der Aufwand für das Risikomanagement sollte durch eine kontinuierliche Verbesserung schrittweise reduziert werden.

Es werden neue Forderungen aus dem Management oder Controlling sowie neue gesetzliche Rahmenbedingungen oder geänderte Standards ihren Weg in das laufende Risikomanagement finden, was die Bewertung von bereits identifizierten Risiken verändern oder neue Risiken hervorbringen kann. Eine offene Kommunikation zwischen Führungsetage und Mitarbeitern ist hierfür das erforderliche Fundament.

Beim Risikomanagement muss jedoch zwischen kommunizierbaren und nichtkommunizierbaren Risiken unterschieden werden, denn letztere ziehen die Einschränkung des Adressatenkreises aufgrund ihrer Brisanz nach sich. Dies kann durch eine klare Rollendefinition in der „Risikoorganisation“ mit Verantwortungen und Befugnissen transparent für alle geregelt werden.

Fazit: Aus Risiken Chancen machen!

Ein funktionierendes, gelebtes Risikomanagement ist mehr als reines Compliance-Management. Es stärkt eine Kultur der präventiven Herangehensweise im Unternehmen. Themen, die für das Unternehmen brisant werden können, werden erkannt und vorab durchleuchtet, sodass das Eintreten dieser Risiken gesenkt werden kann und im Falle eines Falles mehrere mögliche Varianten zum Umgang mit der eingetretenen Gefahr zur Verfügung stehen. Plötzliche Umsatzeinbußen, Ausfälle in der Datenverarbeitung, Hackerangriffe oder ein Brand im Produktionsbereich verlieren zwar nicht den Schrecken, können aber durch geeignete und vorab definierte Korrekturmaßnahmen in ihrer Auswirkung deutlich gemildert werden. Bei einem zusätzlichen Informationsgewinn werden so gleichzeitig mögliche Kosten für das Unternehmen gesenkt.

Erfolgreiches Risikomanagement ist also auch wesentlich mehr als nur die Erfüllung gesetzlicher Rahmenbedingungen. Durch das Erkennen von Chancen und den Vertrauensbonus der Kunden trägt es dazu bei, den Wettbewerbsvorteil zu sichern. Und das in einem individuellen Rahmen, der auf die jeweiligen Bedürfnisse des Unternehmens/der Organisation abgestimmt umgesetzt werden sollte, abhängig von der Größe und Komplexität der Organisation sowie der Risikoexposition durch die Organisation.

Die Integration in ein bereits bestehendes Managementsystem lässt ein Risikomanagement nicht als „Fremdkörper“ im Unternehmen erscheinen, sondern verzahnt geschickt die Ziele von ersterem mit dem Nutzen von letzterem. Risiken und Chancen werden systematisch erkannt und können so nachhaltig zur kontinuierlichen Verbesserung beitragen. Die ISO 31000 und weitere genannte Normen bieten dabei den Unternehmen eine wertvolle Unterstützung.

Andreas Altena
DQS-Auditor
andreas.altena@dqs.de