Expertenwissen für DGQ-Mitglieder

Risikomanagement – Eine Einführung

DGQ

Deutsche Gesellschaft
für Qualität

Risikomanagement – Eine Einführung

Von Andreas Altena und Frank Moritz

Unternehmerische Aktivitäten bergen zu jeder Zeit große Chancen, 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? Währungsschwankungen bewirken finanzielle Verluste? Ein Geschäftspartner im Ausland bekommt Probleme mit der Justiz?

In der Vergangenheit zeigten sich viele Unternehmen von der schnellen Veränderung dieser Risiken überrascht und waren wenig vorbereitet, sodass es sich der Gesetzgeber zur Aufgabe gemacht hat, bestimmte Mindestanforderungen an das Unternehmens-Risikomanagement für bestimmte Unternehmensformen durchzusetzen. Bei Nicht-Befolgung dieser Gesetze reicht die Palette der Sanktionen vom drohenden finanziellen Verlust durch Strafzahlungen bis hin zur persönlichen Haftung von Geschäftsführern und Vorständen.

Modernes Risikomanagement bietet hier einen beachtlichen Informationsgehalt für die Unternehmensleitung, weil es quasi parallel zum prozessualen Berichtsweg eine zusätzliche Informationsquelle bereitstellt, die die Überwachung überlebenswichtiger Kennzahlen garantiert und standardisiert. Wichtig dabei ist, sich im Vorfeld Gedanken zur Implementierung, Umsetzung und Aufrechterhaltung solcher Risikomanagement- Systeme zu machen, um so den angemessenen Rahmen definieren zu können.

Wir wollen Ihnen mit einem komprimierten Überblick zum Risikomanagement ein sehr interessantes und vielfältiges Thema vorstellen. Ein Thema, das jedes Unternehmen, unabhängig von Größe und Branche, betrifft.

Gesetzliche und normative Grundlagen
Die Einführung eines Risikomanagements ist für kleinere Unternehmen empfehlenswert, für AGs und größere GmbHs gemäß des KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) Pflicht.

Schaut man sich die weiteren Entwicklungen in der Welt der ISO-Normen an, so zeichnet sich schon heute die Anforderung nach einem systematischen Risikomanagement in vielerlei Hinsicht ab. 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 ist aus Sicht solcher Normen eine zentrale Komponente bei diesen Anforderungen. Es ist die Basis für Unternehmen, die nachhaltig ihre Existenz sicherstellen und gleichzeitig die Chance nutzen wollen, für ihre Kunden an Attraktivität zu gewinnen. In der weiteren Entwicklung dieser internationalen Regelwerke für Managementsysteme zeichnet sich schon heute ab, dass dies auch die ISO 9001, die voraussichtlich im September 2015 in einer neuen Revision veröffentlicht wird, betreffen wird. Auch hier fordern die bisherigen Entwürfe, dass relevante Risiken für eine nachhaltige Aufrechterhaltung von Qualität und Managementsystem betrachtet werden müssen.

Im Jahr 2009 wurde ein weltweit gültiger Standard für das Risikomanagement festgelegt, die Geburtsstunde der ISO 31000. Diese Norm legt den Fokus darauf, den Prozess des Risikomanagements an ein bereits bestehendes Managementsystem anzugliedern, um den Risikomanagementprozess zu optimieren. Sie dient als Leitfaden und zeigt vielfältige Möglichkeiten der Umsetzung im eigenen Unternehmen auf. Die österreichische Normenreihe ONR 4900x ergänzt diesen Leitfaden durch Informationen zur Anwendung in der Praxis.

Jedem Unternehmen ist die Nutzung von international anerkannten Regelwerken zu empfehlen, um sich seine eigene, individuelle Strategie für die Einführung von Risikomanagement zu definieren.

Nutzen durch die Einführung eines Risikomanagements
Legt man das Augenmerk nicht nur auf die gesetzlichen oder normativen Anforderungen an ein Risikomanagement, so gibt es darüber hinaus einige bedeutende Punkte, die den Nutzen für das Unternehmen unterstreichen.

Nachvollziehbar liegt ein Hauptfokus auf der Rechtssicherheit und somit der Haftungsreduzierung durch ein systematisches Compliance-Management. Dies ist deshalb ein zentraler Teil eines Risikomanagements.

Mit den Werkzeugen des Risikomanagements wird eine Risikokultur geschaffen, soll heißen: Führungskräfte und Mitarbeiter werden sensibler und lernen Dinge aus einer anderen Perspektive bzw. unter weiteren Lösungsansätzen zu betrachten. Das Bewusstsein, die Ursache genau zu beleuchten, wird verstärkt. Darüber hinaus sollte in diesem Zusammenhang betont werden, dass eine effiziente Risikokultur in einem Unternehmen dazu beiträgt, aktuelle und auch zukünftige Kundenanforderungen zu erfüllen. Hier ist z. B. die künftige Ausrichtung des Produktportfolios systematisch zu betrachten, damit entscheidende Wettbewerbsvorteile gesichert oder Trends nicht verschlafen werden: Aus Risiken werden Chancen.

Ebenso machen es vorbereitete Maßnahmen einfacher, in Notfallsituationen die Geschäftskontinuität zu sichern und damit auch das Ansehen bei den Kunden oder anderen Stakeholdern (z. B. Gesellschafter, Versicherungen, Finanzinstitute etc.) zu steigern. Das Verhindern von Gefahrereignissen erspart dem Unternehmen zudem drohende Kosten, die beim Eintritt von Schadensfällen auftreten können. Auch Imageschäden können begrenzt oder ausgeschlossen werden.

Die Systematik eines funktionierenden Risikomanagement-Systems bedeutet zugleich eine klare Definition von Verantwortungen und Zuständigkeiten. Dies schafft Transparenz im Unternehmen, denn Verantwortliche sind benannt und Befugnisse klar geregelt. In einem späteren Abschnitt des Artikels zeigen wir daher auch eine mögliche Rollendefinition auf.

Strategien und Ziele bei der Einführung eines Risikomanagements
Unter dem Managen von Risiken kann die aktive Steuerung der Lebenszyklen der größten im Unternehmen bestehenden Risiken verstanden werden, deren Erkennung, Dokumentation, Analyse, Bewertung, Bewältigung und Überwachung.

Mithilfe unterschiedlicher Strategien und Methoden können Risiken in einem ersten Schritt identifiziert und analysiert werden. Wir möchten hier auf vier Beispiele eingehen:

- Bei der Strategie „Follow-the-process“ folgt der Verantwortliche den Kernprozessen und prüft auf eventuelle mögliche Abweichungen, z. B. durch Dokumentenanalyse oder Begehungen.
- Bei der Strategie „Follow-the-money“ folgt man dem Geldfluss in Unternehmen, um einzuschätzen, wo größtmögliche Schäden lauern können. Zudem müssen hier Haftungsrisiken ergänzt werden.
- Teilweise kann der Verantwortliche auch vorhandenen Checklisten folgen. Hierbei ist jedoch auf die Individualität (Stärken und Schwächen) eines jeden Unternehmens zu achten.
- Mit Kreativitätstechniken bei einem Workshop, wie z. B. einem Brainstorming oder einer Reizwortanalyse, bezieht der Verantwortliche direkt oder indirekt Betroffene mit ein.

Zunächst einmal gilt es, möglichst viele Informationen über identifizierte Risiken zu sammeln und zu verdichten. Wichtig ist es, nicht den Break-even zu verpassen, den Punkt, an dem „viel Information“ in „zu viel Information“ umschlägt. Hier ist das Fingerspitzengefühl des verantwortlichen Projektleiters gefragt. Neben der Herausforderung einer vollständigen, aber gleichzeitig wirtschaftlichen Erfassung von Risiken gilt es, noch weitere Herausforderungen zu stemmen. So muss zunächst erst einmal das Bewusstsein für eine gewisse Risikokultur im Unternehmen geschaffen werden. Des Weiteren ist die hohe Vielfalt der identifizierten Risiken durch eine qualifizierte Bewertung zu verringern.

Hieran fügt sich das Ziel, geeignete Maßnahmen zur Bewältigung von Risiken zu finden, die eine angemessene Vorsorge und Sicherheit bieten. Gerade der Punkt der „Angemessenheit“ spielt auch beim strategischen Vorgehen eine wichtige Rolle: Es gilt, nicht immer jedes kleine Risiko systematisch zu verfolgen oder eine wirklich vollständige Erfassung und Dokumentation von allen Risiken des Unternehmens zu gewährleisten. Wichtig ist, die richtige Balance zwischen Wertschöpfungs-(Ertrags-) und Sicherheitsinteressen zu finden.

Möglicher Ressourceneinsatz
Im Sinne der erwähnten Normen könnte ein Rollenkonzept folgendermaßen aussehen, es dient als Erläuterungsbasis im weiteren Verlauf dieses Artikels:

Rollenmatrix Risikomanagement	***Prozesssteuerung***	***Einzelrisikosicht***
Verantwortung und Befugnisse	Risiko-Prozesseigner	Risiko-Eigner
Operative Durchführung (inkl. definiertem Handlungsrahmen)	Risiko-Prozessmanager	Risiko-Manager

- Der Risiko-Prozesseigner ist der Verantwortliche für den gesamten Risikomanagement-Prozess, von der Einweisung und Schulung der Prozessbeteiligten über den Aufbau des Erfassungssystems und die Erhebung der Einzelrisiken bis hin zum Reporting in ggfs. mehrere Gremien. Wichtig ist, dass der Risiko-Prozesseigner auch über die für den Prozess notwendigen Ressourcen entscheiden kann.
- Der Risiko-Prozesseigner beauftragt wiederum den Risiko-Prozessmanager mit der Durchführung der Tätigkeiten. In dieser Rolle kann noch unterschieden werden zwischen einem Projektmanager, der für die Ersteinführung zuständig ist, und einem Linienmanager, der schließlich den Betrieb übernimmt.
- In der Einzelrisikosicht gibt es im Unternehmen mehrere Risiko-Eigner. Ein Risiko gehört immer nur zu einem Risiko-Eigner, auch wenn dieser ruhig mehrere Risiken besitzen kann. Es bietet sich an dieser Stelle ggfs. an, die Überwachung und/oder Minimierung der Risiken in die Zielvereinbarung mit aufzunehmen. Die Minimierung dieser Risiken wird in der Regel als normale Linientätigkeit betrachtet und somit auch von dieser finanziert.
- Der vom Risiko-Eigner beauftragte Risiko-Manager ist wiederum zuständig für die Überwachung der Entwicklung des Risikos und sollte in enger Verbindung mit dem Risiko-Eigner stehen, d. h. diesen bei relevanten Änderungen der Parameter sofort informieren. Risiko-Manager werden auch eingesetzt für Risiken, die unterhalb einer Meldegrenze liegen. In diesem Fall haben sie die Aufgabe, die Risiken in ihrer Entwicklung zu beobachten: besonders in Hinsicht darauf, ob sie sich nicht doch nach oberhalb der Meldegrenze verschieben.

- Zudem gibt es, je nach Berichtsprozess, weitere Rollen, an die der Risiko-Prozesseigner und/oder - manager zu berichten hat, sowie einen Lenkungsausschuss, der ggfs. Korrekturen am Prozess oder Ergebnis im Sinne der Geschäftsleitung einfordert. Dies kann z. B. der Verantwortliche für das Managementsystem (Verantwortlicher der obersten Leitung) sein. Der Berichtsprozess mit seinen einzelnen Rollen sollte abhängig von der Größe und Komplexität der Organisation sowie der Risikoexposition durch die Organisation individuell festgelegt werden.
- Mögliche andere Herangehensweisen sind z. B. in der ONR 49001 zu finden.

Die Einführung eines Risikomanagements: Aspekte im Projekt

Zunächst muss ein Unternehmen eine Einführungsstrategie festlegen. Das Ziel hierbei ist es: Aufmerksamkeit auf allen Führungsebenen (Management-Attention) und bei den zukünftigen Risiko-Eignern und Risiko-Managern herstellen. Erst zu einem späteren Zeitpunkt sollten Mitarbeiter einbezogen werden (z. B. über eine aktive Kommunikation wie das Intranet bzw. Informationsveranstaltungen).

Vor allem das Verständnis der Risiko-Manager wird zu einem zentralen Erfolgsfaktor des später laufenden Prozesses, denn sie beobachten die Entwicklung des Risikos, setzen Meldegrenzen und Variablen fest und übernehmen den Meldepart im Prozess.

Zu Beginn der Einführung eines Risikomanagements müssen Personen ausgewählt und ein Team gebildet werden, dass das Implementierungsprojekt durchführt. Dieses Risikomanagement-Team sollte von einem Lenkungsausschuss gesteuert werden. Die einzelnen Risiken werden von einem Risiko-Eigner verantwortet. Dieser beauftragt einen Risiko-Manager mit der operativen Steuerung eines einzelnen Risikos. Hierbei kann es sich um eine Einzelperson oder ein Team handeln, das an den Risiko-Prozesseigner berichtet.

Wichtig ist an dieser Stelle, dass sich der Risiko-Eigner seiner Verantwortung für das Risiko bewusst bleibt, eine Übergabe an den Risiko-Manager nach dem „Hey-Joe"-Prinzip („Machen Sie das doch mal eben!") muss prozessual, z. B. durch eine Unterschriftenregelung, verhindert werden.

Das Risikomanagement-Team definiert die Methodik und somit den Regelprozess, wie das Risikomanagement insgesamt im Unternehmen betrieben werden soll. Die Phasen eines solchen Prozesses müssen reproduzierbare Ergebnisse liefern, um Veränderungen bei den Risiken oder in der Bewertung im Reporting widerspiegeln zu können.

Ausgehend von dem entstandenen gemeinsamen Verständnis für Risikomanagement ist irgendwann der Zeitpunkt gekommen, an dem man seine Mitarbeiter miteinbeziehen sollte. Nur so kann ein erfolgreiches und nachhaltiges Risikomanagement betrieben werden. Denn die Mitarbeiter der einzelnen Unternehmensbereiche sind es, die ad hoc Risiken und Chancen in ihrem direkten Arbeitsgebiet erkennen und die Unternehmensleitung darüber informieren können.

Es bietet sich an, dass das Risikomanagement-Team in jeder Unternehmenseinheit Befragungen der Mitarbeiter durch das Risikomanagement-Team durchführt. Hierfür können verschiedene Techniken benutzt werden, von Fragebögen oder Checklisten über strukturierte Interviews bis hin zu Workshops. Durch solche Befragungen werden die Mitarbeiter in den Prozess des Risikomanagements involviert und für potenzielle Risiken sensibilisiert.

Diese Vorgehen seien hier beispielhaft erwähnt, denn bezogen auf den Hintergrund der Erfassung können selbstverständlich auch andere Techniken bzw. Methoden ergänzend zur Anwendung kommen. Im Bereich des Arbeitsschutzes werden z. B. darüber hinaus Begehungen/Besichtigungen vor Ort durchgeführt.

Wichtig ist hier, dass nur Risiken oberhalb einer gewissen Meldegrenze in das System einfließen. Diese Meldegrenze trennt für das Unternehmen wesentliche von unwesentlichen Risiken. Die wesentlichen werden weiter betrachtet, die unwesentlichen nur freiwillig (Entscheidung liegt beim Risiko-Eigner) beobachtet. Auch die präzise Formulierung, Zusammenfassung und Abgrenzung zu anderen Risiken spielt in dieser Phase eine entscheidende Rolle.

Erst nach der Individualisierung des Risikomanagements durch das Unternehmen bietet sich ein Folgeprojekt „Einführung einer Standard-Software" an. Jetzt erst ist es möglich auf der Basis der gesammelten Erfahrungen einem Software-Anbieter auf Augenhöhe entgegenzutreten und

die gewonnenen Erkenntnisse in die Auswahl einer geeigneten Software einfließen zu lassen.

Am Ende des Projektes stehen ein Portfolio von Risiken, ein funktionierendes System von Meldern und ein regelmäßig anzufertigender Risiko-Bericht. Das Risikomanagement geht in den Regelprozess über.

Risikomanagement als Regelprozess
Im Einführungsprojekt könnte der Risikomanagement-Prozess z. B. folgendermaßen festgelegt und eingeführt worden sein:

1. Phase: Risiko-Identifizierung
Risiken werden mit den bereits erwähnten Methoden und Techniken erkannt und erfasst.

2. Phase: Risiko-Bewertung
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.

3. Phase: Risiko- Beobachtung und -Bewältigung
Aus den Erkenntnissen der zweiten Phase werden Vorbeugungs- und Korrekturmaßnahmen abgeleitet. Diese können folgende Möglichkeiten 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

Neben der ständigen Überwachung gilt es im letzten Fall auch 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.

- Die identifizierten Risiken müssen beobachtet und regelmäßig berichtet werden.
- Es gilt neue Risiken zu identifizieren und zu melden.
- Neue Risikomelder müssen eingebunden werden.
- Schulungen und Awareness-Veranstaltungen werden durchgeführt.
- Der Aufwand für das Risikomanagement sollte durch eine kontinuierliche Verbesserung schrittweise weiter reduziert werden.
- „Schlechtmelder“ müssen identifiziert und ggfs. nachgeschult bzw. ersetzt werden.

Darüber hinaus werden neue Anforderungen 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. Jedoch sollte beim Risikomanagement zwischen kommunizierbaren und nicht- kommunizierbaren Risiken unterschieden werden, denn letztere ziehen die Einschränkung des Adressatenkreises aufgrund ihrer Brisanz nach sich.

Das Risikomanagement steht und fällt mit dem Umgang mit „Schlechtmeldern“. Diese melden zu spät oder gar nicht, nehmen das Thema nicht ernst oder melden permanent die gleichen Werte, um endlich wieder „ihre Ruhe zu haben“. Weiterhin gibt es den dramatisierenden Typ, der unbedingt auf das Ziel, nämlich den bewussten Umgang mit Risiken hingewiesen werden muss. 20 Prozent der Risiko-Manager verursachen in der Regel 80 Prozent der Aufwände der Risiko-Eigner. Wenn ein Risikomanagement aussagekräftig und doch kostenminimal betrieben werden soll, müssen Schlechtmelder geschult oder aus dem Prozess entfernt werden.

Fazit

Ein funktionierendes, gelebtes Risikomanagement bietet einem Unternehmen einen zusätzlichen Informationsgewinn und stärkt eine Kultur der präventiven Herangehensweise im Unternehmen. Themen, die für das Unternehmen brisant werden können, werden erkannt und vorab durchleuchtet, sodass es diese Risiken im Vorhinein einschränken kann und im Falle eines Falles mehrere mögliche Varianten zum Umgang mit der eingetretenen Gefahr hat. Plötzliche Umsatzeinbußen, Ausfälle in der Datenverarbeitung, Hackerangriffe oder ein Brand im Produktionsbereich verlieren nicht den Schrecken, können aber durch geeignete und vorab definierte Korrekturmaßnahmen in ihrer Auswirkung deutlich harmloser ausfallen.

Erfolgreiches Risikomanagement ist also 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 des Managementsystems mit dem Nutzen des Risikomanagements. Risiken und Chancen werden systematisch erkannt und können so nachhaltig zur kontinuierlichen Verbesserung beitragen.

Die dargestellten Entwicklungen in den normativen Regelwerken stützen diesen Mehrwert durch die schon heute bestehenden oder zukünftigen Anforderungen.

Über die Autoren:

Andreas Altena, Geschäftsführer der Altena-TCS GmbH
Seine Kernkompetenzen sind Qualitäts-, Informationssicherheit-, Datenschutz- und (IT-)Service-Managementsysteme sowie Service-Excellence. Über seine Tätigkeit als Geschäftsführer hinaus begutachtet er seit 2007 als DQS-Senior-Auditleiter Managementsysteme in den genannten Gebieten und arbeitet seit 2012 als Trainer für die DGQ Weiterbildung GmbH in den Bereichen Qualitätsmanagement- und Auditorenausbildung.

Frank Moritz, Partner der Altena-TCS GmbH, Risiko-Manager sowie Auditor (ISO/IEC 20000-1).
Seine Kernkompetenzen sind Risikomanagement-System-Einführungen, Interim-Prozess-Management, Projektleitung, Coaching und Training. Er arbeitet branchenübergreifend und besitzt exzellente Kenntnisse für Merger-, IT-Projekte (ITIL), sein Spezialgebiet ist die Übernahme „notleidender Projekte“.