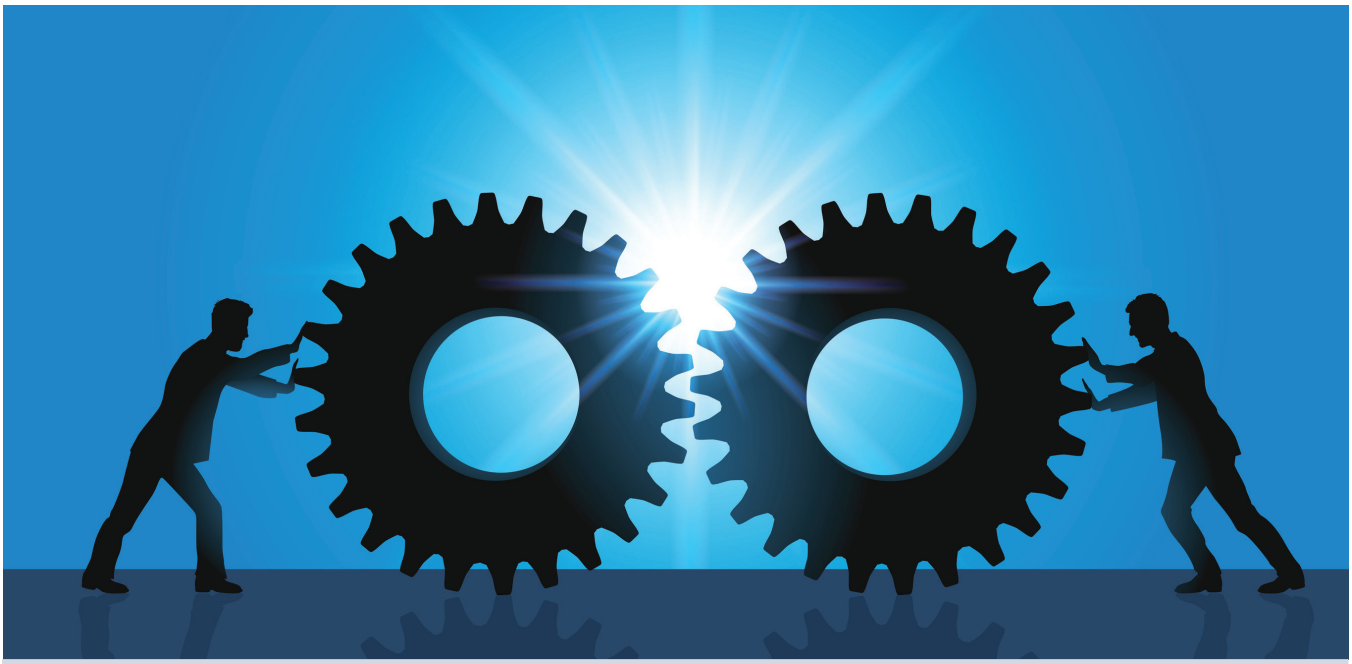

Ganzheitliches Risikomanagement nach ISO 31000 im mittelständischen Maschinen- und Anlagenbau

von Stephan Bartelt und Hans-Jürgen Wieben

RMA

Mittelständische, überwiegend eigentümergeführte Unternehmen stehen bei dem Vorhaben, ein effizientes Risikomanagement-System zu implementieren, oft ohne einen Bezugs- oder Orientierungsrahmen da. Anders als bei stark gesetzlich reglementierten Rechtsformen, wie der Aktiengesellschaft, besteht für die Unternehmen keine explizite gesetzliche Pflicht zur Einrichtung eines Risikofrüherkennungs- oder Risikomanagementsystems.[1] Mindestanforderungen können sich allenfalls aus den Sorgfaltspflichten der Geschäftsführung oder der Ausstrahlungswirkung von Regelungen des AktG oder des HGB ergeben.

Qual der Wahl

Als Bezugs- oder Orientierungsrahmen zur Implementierung eines Risikomanagementsystems bieten sich daher nationale wie internationale Risikomanagementstandards an. In der Risikomanagement-Literatur vielfach diskutiert werden die von nationalen Standardsettern entwickelten US-amerikanischen Standards COSO Enterprise Risk Management, der australisch/neuseeländische Risikomanagementstandard AS/NZS 4360 oder die österreichische Norm ONR 49000.[2] **Seit 2010 hat sich in diesem Kontext die internationale Normenfamilie „ISO 31000 Risk Management" etabliert**, und – trotz fehlender Zertifizierbarkeit – als international akzeptierter Standard für die Gestaltung von Risikomanagementsystemen durchgesetzt.[3] Der Rückgriff auf eine ISO-Norm bei der Gestaltung eines Risikomanagementsystems bietet den Vorteil einer weltweiten Verbreitung und Anerkennung des Risikomanagement-Standards, der bei international agierenden Maschinen- und Anlagenbauern einen Argumentationsvorteil gegenüber ihren Geschäftspartnern mit sich bringen kann. **Ein Risikomanagement-System nach ISO 31000 soll zudem kein weiteres isoliertes Managementsystem in der Organisation sein, sondern in bestehende Managementsysteme integriert werden.**[4] Mit der aktuellen Revision der ISO 9001 Rev. 2015 leistet die Normungsorganisation selbst einen Beitrag zu dieser stärkeren Integration, indem Qualitäts- und Risikomanagementsysteme enger verknüpft werden.[5] Die ISO 31000 beinhaltet darüber hinaus einen systematischen Ansatz zur Einführung eines Risikomanagement-Systems.[6] Beide Aspekte sind gerade für mittelständische Unternehmen weitere Vorteile bei der Einführung eines neuen Risikomanagement-Systems. Ihr systematischer Risikomanagementprozess wird dabei ganz überwiegend in den operativen Geschäftsprozessen stattfinden müssen, da der Aufbau mehrerer Verteidigungslinien im Sinne eines Three-Lines-of-Defence-Konzeptes an den zu geringen personellen Kapazitäten, der damit einhergehenden geringeren Dokumentationsdichte und den in der Regel nicht mehr wirtschaftlich darstellbaren Kosten schei-

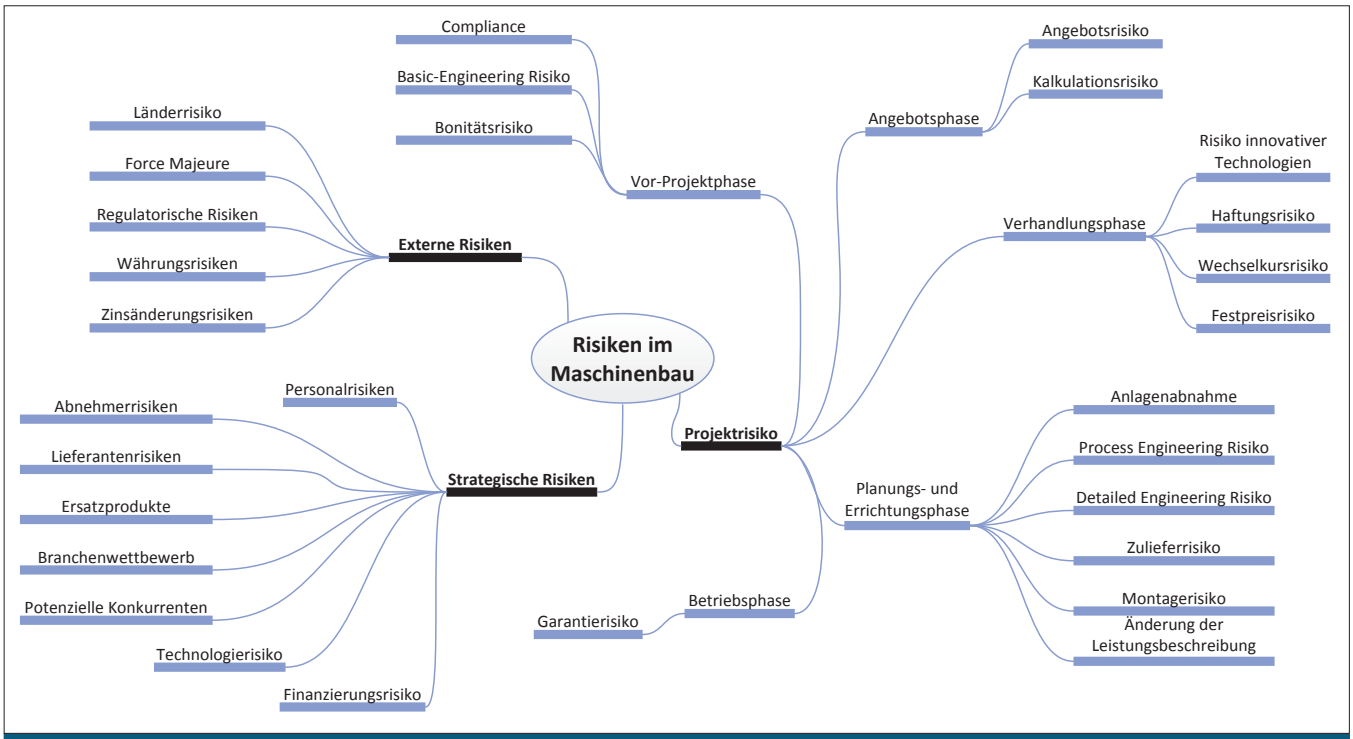

Abb. 1: Typische Risiken im Maschinen- und Anlagenbau

tern wird. Kritisch an der Norm 31000 wird vor allem ihre teils mangelnde Konkretisierung und Anwenderfreundlichkeit gesehen, die sich aber durch Rückgriff auf mit der ISO 31000 verwandte Normen wie die österreichische Norm ONR 49000ff. beherrschen lässt.[7] Ziel dieses Beitrags ist es, einen mittelstandstauglichen Risikomanagementprozess für den Maschinen- und Anlagenbau mit entsprechenden Risikomanagementinstrumenten unter Nutzung der ISO 31000-Normenfamilie zu entwickeln.

Risikoprofil eines Anlagenbauers als Ausgangspunkt

Der deutsche Maschinen- und Anlagenbau besteht als einer der größten und erfolgreichsten Industriezweige Deutschlands überwiegend aus mittelständischen Betrieben.[8] Kennzeichnend für viele Unternehmen der Branche sind u. a. folgende Merkmale:[9]

1. Eine **kundenindividuelle Auftragsfertigung** erfordert in der Regel eine zeit- und kapitalintensive Neu- und Variantenkonstruktion, die Auswirkungen auf die gesamte Unternehmensorganisation hat.
2. **Diskontinuitäten im Auftragseingang**, getrieben durch Sprunghaftigkeit des Technologiefortschritts und insbesondere der Konjunkturlage in den Abnehmerländern, haben nicht selten teils erhebliche Kapazitätsschwankungen in allen Wertschöpfungsstufen zur Folge. Bleiben Aufträge aus, entstehen Leerkapazitäten, wohingegen bei starker Nachfrage die Gefahr besteht, Aufträge aufgrund von Fehlkapazitäten nicht annehmen zu können.
3. **Internationale Handelsverflechtungen** in den Zulieferer- und Abnehmerstrukturen stellen die Unternehmen zunehmend vor die Herausforderung, unterschiedliche rechtliche, politische, wirtschaftliche und technische Rahmenbedingungen zu adaptieren und die Unternehmensorganisation daran auszurichten.
4. Durch die **Langfristigkeit der Aufträge** stellt das interne Projektmanagement einen essenziellen Erfolgsfaktor für einen reibungslosen und kundenorientierten Projektablauf dar. Hierbei haben sich im Maschinen- und

Risikomanagement…

- ...schafft und schützt Werte, da Ziele in allen Unternehmensbereichen besser erreicht werden.
- ...ist Bestandteil aller planenden und realisierenden Unternehmensprozesse.
- ...verbessert als integraler Bestandteil aller Entscheidungen deren Qualität.
- ...berücksichtigt explizit Unsicherheit und ihre Ursachen.
- ...basiert auf einer systematischen, strukturierten und Aktualität sichernden Vorgehensweise.
- ...verwendet die besten im Unternehmen verfügbaren Informationen.
- ...ist angepasst an die Risikosituation und die Organisationsstruktur des Unternehmens.
- ...berücksichtigt menschliche und kulturelle Faktoren aller beteiligten Personengruppen.
- ...sorgt für Transparenz durch Einbeziehung aller relevanten Stakeholder.
- ...ist dynamisch, iterativ und reagiert schnell auf Veränderungen der Risikosituation.
- ...unterliegt einer kontinuierlichen Verbesserung wie die übrige Organisation.

Abb. 2: Prinzipien des Risikomanagements nach ISO 31000

Risikoart	Einzelrisiko	Identifikation und Bewertung durch..	Turnus der Identifikation und Bewertung	Steuerung des Risikos durch..	Einzubeziehende interne Stakeholder
Strategisches Risiko	Finanzierungsrisiko	Controlling / Finanzen	Monatlich und bei Bedarf	Kfm. Geschäftsführung	Vertrieb Beschaffung
	Personalrisiko	Personal	Quartalsweise	Geschäftsführung	Bereichsleiter
Externe Risiken	Regulatorische Risiken	Exportkontrolle	Laufend	Geschäftsführung	Geschäftsführung Vertrieb Export/ Versand
	Währungsrisiken	Vertrieb Finanzen	Quartalsweise	Kfm. Geschäftsführung Finanzen	Vertrieb Projektmanagement Export/ Versand Controlling Geschäftsführung Bereichsleiter
Operatives Projektrisiko	Bonitätsrisiko (Vor-Projektphase)	Controlling / Finanzen	Bei Bedarf	Bereichsleiter	Kfm. Geschäftsführung
	Kalkulationsrisiko (Angebotsphase)	Vertrieb / Controlling	Auftragsbezogen	Geschäftsführung	Fertigung Beschaffung Konstruktion
	Wechselkursrisiko (Verhandlungsphase)	Controlling / Finanzen	Quartalsweise	Vertrieb	Kfm. Geschäftsführung
	Anlagenabnahme (Planungs- und Errichtungsphase)	Projektmanagement	Auftragsbezogen	Bereichsleiter	Finanzen / Controlling Technik
	Garantierisiko (Betriebsphase)	Projektmanagement	Auftragsbezogen	Techn. Geschäftsführung / Entwicklungskonstruktion	Bereichsleiter / Beschaffung / Fertigung / Konstruktion

Abb. 3: Organisation des Risikomanagements für typische Risikoarten anhand des Risikoprofils

Anlagenbau sechs Grobphasen für das Projektmanagement herauskristallisiert. Diese sind die Akquisitionsphase (Vor-Projektphase), Angebotsphase, Verhandlungsphase, Planungs-, Liefer- und Errichtungsphase, Inbetriebnahmephase und Betriebsphase.

5. Darüber hinaus stellen die **hohen Auftragswerte** im Anlagenbau, deren Ausführung je nach Branchenspezialisierung von modularen, flexiblen Mehrproduktanlagen bis hin zu World-Scale-Anlagen reichen, ein weiteres Spezifikum dar.
6. Hierdurch bedingt ergeben sich für die Maschinenbauer nicht selten hohe **Auftrags-(vor-)finanzierungs-Verpflichtungen**, die die liquiden Mittel der mittelständisch geprägten Unternehmen stark belasten können.

Maschinen- und Anlagenbauer sind damit vor die Herausforderung gestellt, besondere geschäftsimmanente Risiken zu identifizieren, zu bewerten und systematisch zu steuern, die in der Abbildung 1 dargestellt sind.

ISO-Prinzipien für die Gestaltung des Risikomanagements

ISO 31000 definiert zunächst Prinzipien, denen ein effektives Risikomanagement auf allen Ebenen der Organisation genügen muss (vgl. Abbildung 2).[10]

Aus diesen Prinzipien lassen sich folgende zentrale **Leitfragen für die Gestaltung des Risikomanagement-Systems** ableiten:

- Welche Unternehmensbereiche können die geschäftsimmanenten Risiken sinnvoll identifizieren, analysieren und möglichst objektiv und aktuell bewerten?
- Wie häufig sollten Risikoidentifikation, -analyse und -bewertung erfolgen, um einen möglichst hohen Informationsnutzen bei akzeptablen Kosten zu erreichen?
- Welche Instrumente können dafür eingesetzt werden?
- Welche Entscheider können die Risiken unmittelbar und im Sinne des Gesamtunternehmens steuern, d. h. in ihren planenden und realisierenden Aktivitäten berücksichtigen?
- Welche Stakeholder müssen regelmäßig über die Risikosituation informiert und in ggf. erforderliche Entscheidungen eingebunden werden?
- In welchem Turnus muss die Information erfolgen?

Die konkrete Beantwortung dieser Leitfragen für die wesentlichen Risikoarten des Risikoprofils eines Anlagenbauers zeigt auf, welche Ab-

Instrumente der Identifikation	Berichtswesen
Rollierende Finanzplanung	Monatlich
SWOT-Analyse Personalbedarfsanalyse	FK-Runde
Dual Use - Güterprüfung	FK-Runde
Experteneinschätzung von Banken (Außenhandel)	Monatlich
Kreditversicherungsanfrage Fundamentalanalyse	Quartalsweise
Abweichungsanalyse	Laufend
3-Monats-Libor	Quartalsweise
Mängelliste	Wöchentlich
After Work Check	Quartalsweise

teilungen und Unternehmensbereiche bei der Gestaltung des Risikomanagement-Systems zu berücksichtigen sind. In der Abbildung 3 sind entsprechende Beispiele dargestellt.

Strategische Ebene: Gestaltung des Risikomanagementsystems

Für die erstmalige Gestaltung oder die Verbesserung eines Risikomanagementsystems zeigt die ISO 31000 konkrete Prozessschritte auf und gibt eine Reihe von Hinweisen, die zu einer nachhaltigen Verankerung eines Risikomanagementprozesses im Unternehmen führen. Wesentliche Aspekte sind in Abschnitt 4 der ISO 31000 dargestellt.

Ausgangspunkt jeder Neugestaltung müssen die Rahmenbedingungen sein, unter denen der Risikomanagementprozess im Unternehmen den dargestellten Prinzipien genügen soll. Für den mittelständischen Anlagenbau sind insbesondere der internationale Kontext, eine geringe Personaldecke für administrative Aufgaben und eine von Vertrauen geprägte Unternehmenskultur wesentliche Nebenbedingungen für die Gestaltung des Risikomanagements. Risikomanagement muss soweit möglich in bestehende Prozesse und Informationssysteme integriert werden, um Akzeptanz bei allen wesentlichen Entscheidern und Stakeholdern im Unternehmen zu finden und nicht als zusätzliche administrative Belastung oder gar zusätzliche Leistungskontrolle wahrgenommen zu werden. Vorteile dieser integrativen Implementierungsform liegen darüber hinaus in der schnellen Reaktionsfähigkeit und der kontinuierlichen Verbesserung der bestehenden Unternehmensabläufe.

Organisatorische Verantwortung im Controlling

Die organisatorische Verantwortung für das Risikomanagement sollte im kaufmännischen Bereich liegen, da hier die kaufmännische Gesamtsicht auf das Unternehmen vertreten wird. Insbesondere bietet sich eine Verankerung im Controlling an, da das Controlling die Unternehmensplanung koordiniert und eine unterjährige Überprüfung der Zielerreichung vornimmt. Über das Berichtswesen besteht eine enge Zusammenarbeit mit allen relevanten Unternehmensbereichen, dem Top Management und ggf. zu informierenden Aufsichtsgremien.

Die Systemgestaltung an sich muss durch das Top Management festgelegt werden, um die Relevanz des Risikomanagements in allen Unternehmensbereichen zu betonen.
In einem Projekt zur Neugestaltung eines Risikomanagementsystems sollten dabei zumindest folgende Stakeholder eingebunden werden:

- Top Management, ggf. vertreten durch den CFO, als wesentliche Entscheider
- Aufsichtsgremien als Berichtsempfänger
- Leiter wesentlicher Bereiche / Tochtergesellschaften als Risikoverantwortliche
- Vertreter ausländischer Niederlassungen / Tochtergesellschaften, um der Internationalität gerecht zu werden
- Kaufmännische Funktionen mit Risikobezug, wie z. B. Controlling oder Finanzen, als Risikoverantwortliche oder Unterstützungsfunktionen mit kaufmännischer Expertise.

Sofern vorhanden, sollten auch die Compliance- oder Revisionsfunktion das Projekt unterstützen. Die Projektorganisation sollte von einer kleinen Gruppe getragen werden, die ein konkretes Risikomanagementrahmenwerk in Abstimmung mit den wesentlichen Entscheidern und Aufsichtsgremien erarbeitet. Die Projektleitung sollte in der zukünftig für den Risikomanagementprozess verantwortlichen Abteilung liegen.

Die zu erarbeitenden Risikomanagementvorgaben müssen zu einer **klaren Definition von Verantwortlichkeiten, Rollen und Aufgaben im Risikomanagementprozess** führen. Ausgangspunkt muss eine intensive Analyse des Risikoprofils des Unternehmens sein, um für die wesentlichen Risikoarten eine aktuelle, möglichst objektive Identifikation, Analyse, Bewertung und Kommunikation der Risiken sicherzustellen. Dem Verständnis der ISO 31000 entsprechend sollten Risiken dabei als positive wie negative Abweichungen (Chancen und Gefahren) von Unternehmenszielen verstanden werden.[11] Der Prozess muss eine regelmäßige Zusammenführung und Aggregation der Risiken und ein aussagekräftiges Berichtswesen gegenüber wesentlichen Stakeholdern vorsehen. Die Vorgaben sind schriftlich festzuhalten und sollten durch das Top Management verabschiedet und im Unternehmen kommuniziert werden.

Operative Ebene: Risikomanagement als Prozess

Den Ausgangspunkt für die operative Umsetzung des Risikomanagements nach ISO 31000 stellt der Risikomanagementrahmen dar, der auf strategischer Ebene entwickelt wurde und der die grundsätzliche organisatorische und sachliche Vorgehensweise für die Risikobeurteilung definiert. Die Risikobeurteilung hat dabei zum Ziel, notwendige Maßnahmen für eine effektive Risikobehandlung abzuleiten. Hierfür müssen sich die Verantwortlichen drei zentrale Fragen stellen:

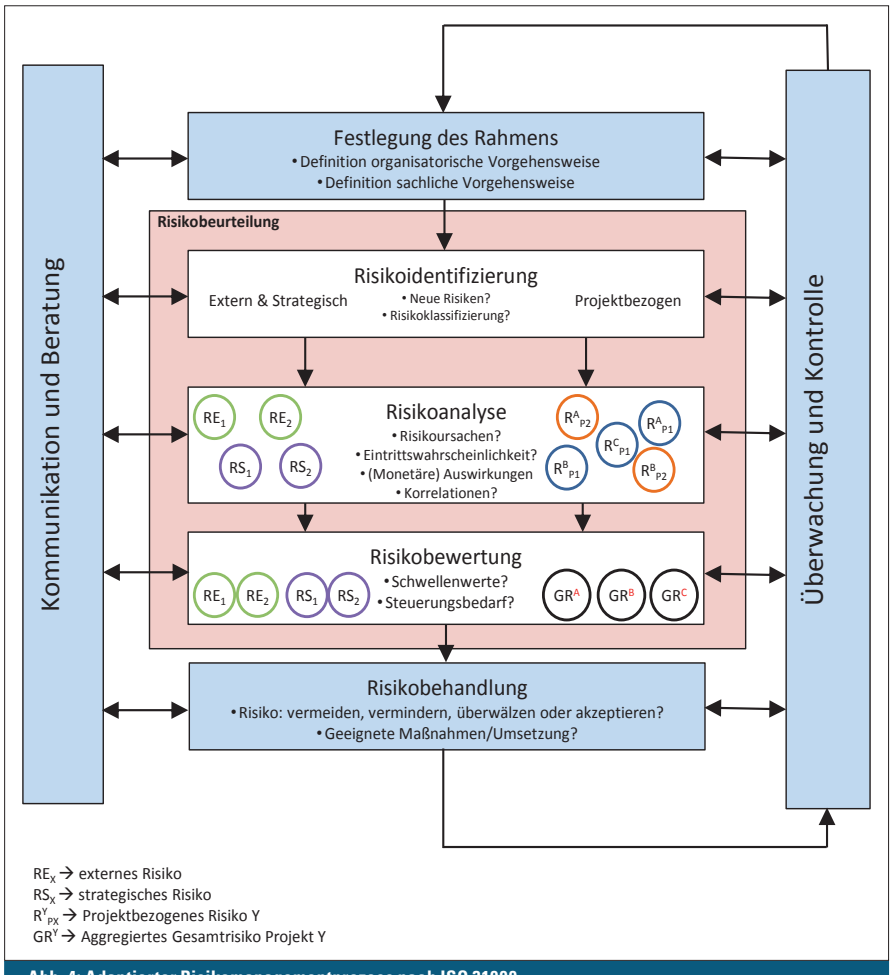

Abb. 4: Adaptierter Risikomanagementprozess nach ISO 31000

1. Welche Ereignisse können zu einer Zielabweichung führen? (**Risikoidentifikation**)
2. Was sind die Ursachen und Konsequenzen des Risikoeintritts und wie wahrscheinlich ist der Risikoeintritt? (**Risikoanalyse**)
3. Wie sind die einzelnen Risiken unter Berücksichtigung der internen und externen Rahmenbedingungen zu priorisieren? (**Risikobewertung**).

Die **Risikoidentifikation** umfasst dabei im Wesentlichen die kontinuierliche Ermittlung von Risiken und ihre Klassifizierung in externe Risiken, strategische Risiken oder operative Projektrisiken. Sie bildet die Basis für alle weiteren Schritte der Risikobeurteilung und sollte daher mit besonderer Sorgfalt durchgeführt werden.[12] Für die Risikoidentifikation stehen dem Risikomanagement eine Vielzahl von Methoden zur Verfügung (vgl. beispielhaft Abbildung 3, Spalte 7). Eine umfangreiche Beschreibung zahlreicher Instrumente der Risikoidentifikation und -analyse mit ihren Einsatzbereichen ist in der ISO 31010 enthalten, die zur Normenfamilie der ISO 31000 gehört.[13]

Nach der Risikoidentifikation folgt die **Risikoanalyse**, in der ein Verständnis und eine Bewertung für das Risiko entwickelt werden sollen. Die Analyse umfasst die Prüfung der Ursachen des Risikos sowie die quantitative und qualitative Abschätzung der Folgen und der Eintrittswahrscheinlichkeit. Ein wesentlicher Bestandteil liegt hierbei auch in der Identifikation von Korrelationen der Einzelrisiken.[14] Für die Ermittlung der Eintrittswahrscheinlichkeit und des Risikoausmaßes sind Verteilungsannahmen auf Basis von historischen Daten oder Experteneinschätzungen zu treffen, um die Unsicherheit über die zukünftige wirtschaftliche Entwicklung sachgerecht abzubilden. Die Einschätzung der wirtschaftlichen Folgen sollte dabei soweit als möglich quantitativ erfolgen.[15] Ergänzende qualitative Einschätzungen bieten sich z. B. für die Abbildung von Risikofolgen für die Unternehmensreputation an.

Basierend auf der Risikoanalyse erfolgt in der **Risikobewertung** eine Klassifizierung und Priorisierung der Risiken. Diese kann z. B. eine Beurteilung nach sogenannten Risikozonen in einer Risk Map vorsehen. Die Risikozonen (meist unterteilt in „kein Handlungsbedarf“, „Kosten/Nutzen abwägen“ und „Handlungsbedarf“) dienen der Orientierung bzw. Entscheidung, welche Risiken behandelt werden müssen.[16] Kommt es zu einer Überschreitung definierter Schwellenwerte, liegt es in der Verantwortung des Managements zu entscheiden, wie es das Risiko behandeln will. Hierzu stehen ihnen verschiedene Risikobehandlungsstrategien[17] zur Verfügung.

Dieser allgemeingültige Risikobeurteilungsprozess wird aufgrund der Besonderheiten im Maschinenbau weiterentwickelt und in zwei Vorgehensweisen in Abhängigkeit der Risikoarten differenziert, vgl. auch Abbildung 4:

1. Einzelbeurteilung für strategische und externe Risiken,
2. Multibeurteilung für projektbezogene Risiken.

Autoren

Stephan Bartelt M.B.A.

ist Teamleiter Controlling bei der TROESTER GmbH & Co. KG, einem mittelständischen Unternehmen des Maschinen- und Anlagenbaus.

E-Mail: stephan.bartelt@troester.de

Prof. Dr. Hans-Jürgen Wieben

ist Studiengangsleiter M Sc. Controlling, Finanzen und Risikomanagement an der Fachhochschule für die Wirtschaft (FHDW), Hannover.

E-Mail: hans-juergen.wieben@fhdw.de

1. Einzelbeurteilung für strategische und externe Risiken

Die Identifikation, Analyse, Bewertung und Überwachung von strategischen und externen Risiken unterliegt in einer mittelständischen Unternehmensorganisation der obersten Führungsebene des Unternehmens. Soweit ein Risiko identifiziert wird, ist dieses zwecks Analyse in das Controlling oder die Linie zu geben, um eine sachgerechte Ursache-Wirkungsanalyse durchzuführen und risikosteuernde Maßnahmen, wie z. B. Maßnahmen der Währungskursabsicherung, zu ergreifen. Wesentliche strategische und externe Risiken, die in das Risikoprofil der Gesellschaft eingeflossen sind, sollten regelmäßig mit bestehenden Instrumenten überwacht und kommuniziert werden. Eine zusammenfassende Darstellung der Risiken an interne Stakeholder sollte nur wesentliche strategische und externe Risiken beinhalten, um den administrativen Aufwand gering zu halten.

2. Multibeurteilung für projektbezogene Risiken

Für die projektbezogene Risikobeurteilung kann eine sogenannte Risikokarte eingesetzt werden. Diese begleitet jeden Kundenauftrag im Unternehmen während der gesamten Projektlaufzeit als übergeordnetes Koordinations- und Kommunikationsinstrument zur Abbildung identifizierter Risiken durch festgelegte Verantwortlichkeiten in abgestimmten Zeiträumen mit standardisierten Methoden (siehe beispielhaft Abbildung 3). **Die Risikokarte beinhaltet vier miteinander verzahnte Perspektiven aus den projektkritischen Bereichen Finanzen, Kunde, Termine und Qualität.** Jeder Risiko-Perspektive werden dabei artenspezifische Risikokennzahlen zugeordnet, die zu den definierten Projektmeilensteinen Anfang/Ende Angebotsphase, Verhandlungsphase, Planungs- und Errichtungsphase und Betriebsphase in Abhängigkeit von einem festgelegten Identifikations- und Bewertungsturnus erhoben werden. Hierbei übernimmt das Controlling die Rolle als zentraler Koordinator und verantwortlicher Akteur für das Zusammentragen der Ergebnisse und das kontinuierliche Risiko-Mapping, in enger Kooperation mit dem internen Projektmanagement.

Auf Ebene der Risikobewertung sind vier grundlegende Schritte vorzunehmen:

1. **Risikoquantifizierung** durch monetäre Bewertung des Risikos mit Hilfe geeigneter Risikomaße. Das bekannteste Risikomaß stellt hier der Value at Risk als Schadenshöhe, die während eines festgelegten Zeitraumes mit einer festgelegten Wahrscheinlichkeit nicht überschritten wird, dar.[18]
2. **Messung von Korrelationen** innerhalb der wesentlichen Einzelprojektrisiken.
3. **Risikoaggregation** von einzelprojektbezogenen Risiken auf Gesamtprojektebene zur Abschätzung des Gesamtrisikos pro Risikoart.
4. **Ableitung eines unternehmensspezifischen Rankings** zur Festlegung von Reihenfolgen in Bezug auf die Behandlung von Risiken und die risikoorientierte Steuerung von Kundenprojekten.

Durch diese Vorgehensweise wird das Unternehmen in die Lage versetzt, noch während des Kundenprojektablaufes auf mögliche Risiken zu reagieren und systematisch Maßnahmen zur Prävention der aufgetretenen Risiken für die Zukunft abzuleiten.

Der spezifische und kundenprojektorientierte Aufbau der Risikokarte ermöglicht dem Unternehmen darüber hinaus eine vielfältige Analyse durch die verschiedenen Betrachtungswinkel, wie bspw.:

- Gesamtrisiko pro Kunde,
- Gesamtrisiko pro Projektphase,
- Gesamtrisiko pro Profit Center,
- Währungsrisiko pro Absatzland,
- Qualitätsrisiko pro Produktgruppe.

Gesamtrisiko des Unternehmens

Die ISO 31000 überlässt es als allgemeingültiger Standard der Entscheidung des Managements, auf welchen Ebenen eine Risikobetrachtung erfolgt. Die externen und internen Rahmenbedingungen und daraus abgeleitete Schwellenwerte für das Unternehmen sind allerdings einzuhalten. Eine reine Betrachtung von Einzelrisiken oder Risikoarten dürfte danach nur für mittelständische Unternehmen mit besonders guter Kapital- und Liquiditätsausstattung ausreichen, wenn die Unternehmensexistenz dauerhaft gesichert sein soll. Gerade im mittelständischen Maschinen- und Anlagenbau sollte unseres Erachtens aufgrund des dargestellten Risikoprofils eine Aggregation der Einzelrisiken auf Ebene des Gesamtunternehmens erfolgen, um ein ganzheitliches Risikomanage-

ment zu gewährleisten und den Sorgfaltspflichten der Geschäftsführung für die frühzeitige Identifikation „**bestandsbedrohender Entwicklungen**“ und einer sachgerechten Ermessensausübung im Sinne der „Business Judgement Rule“ gerecht zu werden.[19] Die methodischen Ansätze zur Ermittlung des Gesamtrisikos, z. B. mit Hilfe der Monte-Carlo-Simulation, sind mittlerweile auch für Industrieunternehmen etabliert und weitgehend in die am Markt verfügbare Risikomanagement-Software integriert.[20] Im Sinne der ISO 31000 kann damit auch ein Beitrag zu einer Verbesserung der Chancen- und Risikokultur im Unternehmen geleistet werden.[21]

Zusammenfassung

Für mittelständische Unternehmen des Maschinen- und Anlagenbaus spielen bei der Entwicklung eines effizienten Risikomanagement-Systems Kosten-Nutzen-Überlegungen eine wesentliche Rolle. Ein systematischer Risikomanagementprozess wird in der Regel mit dem zur Verfügung stehenden Personal aufzubauen sein. Die Normenfamilie ISO 31000 kann einen sinnvollen Beitrag zur Gestaltung eines integrativen Risikomanagementanasatzes leisten, der sich auf die Risikoarten Strategische Risiken, externe Risiken und operative Projektrisiken fokussieren sollte. Während strategische und externe Risiken stark von der Geschäftsleitung und den kaufmännischen Bereichen zu identifizieren und zu überwachen sind, sollten die operativen Projektrisiken durch das interne Projektmanagement und die an den verschiedenen Projektphasen beteiligten Abteilungen über eine standardisierte Projektkarte erfasst werden. Es ist Aufgabe des Controllings, die Einzelrisikobetrachtungen zusammenzuführen und frühzeitig auf mögliche Einzelprojektrisiken und ein sich kumulierendes Gesamtrisiko hinzuweisen. Für die Risikokommunikation sollte eine standardisierte Berichterstattung über aktuell wesentliche Risiken auf Basis des Risikoprofils des Unternehmens erfolgen.

Fußnoten

[1] Kleine und mittlere Gesellschaften unterliegen lediglich den handelsrechtlichen Mindestanforderungen zum Nachweis von Risikomanagement im Rahmen der Erstellung von Jahresabschluss, Anhang und Lagebericht.

[3] Einen Überblick zu aktuellen Risikomanagementstandards und ihren Zielsetzungen geben z. B. Vanini, U.: Risikomanagement, 2012, S. 82-93, Winter, P.: Risikomanagement-Standards als Leitfaden für formalisierte Unternehmens-Risikomanagementsysteme – Überblick und Bewertung, in: ZRFG, Jg. 2 (2007), Heft 4, S. 149-155 oder Weidemann, M.; Wieben, H.-J.: Zur Zertifizierbarkeit von Risikomanagement-Systemen, in: Der Betrieb, Jg. 54 (2001), H. 34, S. 1789-1795.

[3] Vgl. OECD, Risk Management and Corporate Governance, OECD Publishing, Paris 2014, S. 16.

[4] Vgl. Weis, U.: Risikomanagement nach ISO 31000. System – Ist-Analyse – Methoden, Kissing 2009, S. 40.

[5] Vgl. Erben, R.; Vogel, D.: Qualitäts- und Risikomanagement wachsen weiter zusammen – ISO 9001 Rev. 2015, in: Controller Magazin, 41. Jg. (2016), H. 3, S. 24-30.

[6] Vgl. Brühwiler, B.; Romeike, F.: Praxisleitfaden Risikomanagement, Berlin 2010, S. 83.

[7] Zur Kritik vgl. etwa Kimpel, R.; Lissen, N.; Offerhaus, J.: Risikomanagement-Standards – Beschleuniger oder Bremser einer wert- und risikoorientierten Unternehmenssteuerung; in: Kalwait, R. (Hrsg.) Wert- und Risikoorientierte Unternehmenssteuerung, Duisburg 2009, S. 70 ff. oder Withus, K.-H.: Genormtes Risikomanagement – Die neue ISO Norm 31000 zu Grundsätzen und Richtlinien für Risikomanagement, in: ZRFG, Jg. 5 (2010), Nr. 4, S. 175 ff.

[8] 87 Prozent der ca. 6.000 Unternehmen beschäftigen weniger als 250 Mitarbeiter.

[9] Vgl. Voigt, K.-I.: Risikomanagement im Anlagenbau, Berlin, 2010, S. 24 ff.

[10] Vgl. ISO 31000, Gliederungspunkt 3: Principles.

[11] Vgl. ISO 31000, Gliederungspunkt 2.1 mit Referenz auf ISO Guide 73:2009.

[12] Vgl. ISO 31000, Gliederungspunkt 5.4.2.

[13] Vgl. Erben, R.; Offerhaus, J.; Sitt, A.: ISO 31010 – Inhalte und Nutzen des neuen internationalen Standards zur Risikoidentifikation und -bewertung, in: Risk, Compliance & Audit (RC&A), 2. Jahrgang (2010), Hefte 5 und 6.

[14] Vgl. Weis, U.: Risikomanagement nach ISO 31000. System – Ist-Analyse – Methoden, Kissing 2009, S. 60 f.

[15] Vgl. ISO 31000, Gliederungspunkt 5.4.3. Für eine praxisorientierte Einführung in Verteilungsannahmen und deren Einbindung in das Risikomanagement vgl. Gleißner, W.: Quantitative Verfahren im Risikomanagement: Risikoaggregation, Risikomaße und Performancemaße, in: Der Controlling-Berater, Band 16, 2011, S. 183-190.

[16] Vgl. Wolke, T.: Risikomanagement, 2. Aufl., München 2008, S. 67 f.

[17] Risikobehandlungsstrategien meinen die Ableitung und Umsetzung von Maßnahmen zur Vermeidung, Verminderung, Überwälzung oder Akzeptanz bestimmter Risiken. Siehe hierzu auch Romeike, F. / Hager, P.: Erfolgsfaktor Risikomanagement 3.0, (2013), S. 136 ff.

[18] Ansätze zur simulativen Risikoquantifizierung für komplexe Projekte finden sich z. B. bei Gleißner, W.: Quantifizierung komplexer Risiken – Fallbeispiel Projektrisiken, in: Risiko Manager, Ausgabe 22, 2014, S. 1, 7-10.

[19] Zur sachgerechten Ermessensausübung der Unternehmensleitung mit Hilfe der Business Judgement Rule vgl. Zöllner, W.; Noack, U.: § 43 GmbHG, in Baumbach, A.; Hueck, A.: GmbH Kommentar, 19. Auflage (2010), Rn. 22 ff.

[20] Vgl. zur steigenden Verbreitung professioneller Risikomanagement-Software Tilch, T.; Lenz, A., Scheffler, R. et al.: Risk-Management-Benchmarking 2015, S. 35. Zur methodischen Abbildung der Risikoaggregation vgl. Gleißner, W.: Grundlagen des Risikomanagements: Controlling, Unternehmensstrategie und wertorientiertes Management, 2011, S.159 ff. sowie den Überblick bei Vanini, U.: Integration von Risiken in die Unternehmensplanung durch Monte-Carlo-Simulationen, in: Controller Magazin, 41. Jg. (2016), H. 2, S. 27.

[21] Vgl. Flath, T.; Biederstedt, L.; Herlitz, A.: Mit Simulationen Mehrwert schaffen, in: Controlling & Management Review, 59. Jg. (2015), Sonderheft 1, S. 86.