



Risikomanagement nach ISO 31000 Umsetzung in der Organisation

1	Zweck dieser Abhandlung	2
2	Grundlagen zum Risikomanagement	3
2.1	Gemeinsamkeiten der Risikobetrachtung	3
2.2	Risikobetrachtung nach ISO 31000	4
3	Risikobewertungsschritte auf Grundlage der ISO 31000	5
3.1	Analysephase	5
3.2	Maßnahmenphase	6
3.3	Überwachungsphase	6
4	Risikobewertungsbeispiele	6
4.1	Produkte	6
4.2	Prozesse	7
4.2.1	Hauptprozesse	7
4.2.2	Teilprozesse	8
4.2.3	Prozesskette	10
4.2.4	Tätigkeitsschritte	10
4.2.5	Zusammenfassende Betrachtung dieser Risikoquellen	11
5	Risikobetrachtung Tätigkeiten	12
5.1	Analysephase: Risikoquelle bis Risikozahl	12
5.1.1	Risikoquelle und Risikofall	12
5.1.2	Risikoauswirkung und Risikoursache	14
5.1.3	Risikoeinfluss und Risikofeststellung	15
5.1.4	Risikohöhe und Risikozahl	16
5.2	Maßnahmenphase: Geplante Maßnahme bis Umsetzungsverantwortung	16
5.3	Überwachungsphase: Maßnahmenkontrolle bis Abschluss	17
6	Zusammenfassung	18



Risikomanagement nach ISO 31000 Umsetzung in der Organisation

1 Zweck dieser Abhandlung

Mit der ÖNORM ISO 31000:2010-02 liegt in deutscher Sprache eine Übersetzung der ISO 31000:2009 zum Risikomanagement vor. Der Entwurf für eine deutsche Ausgabe liegt mit Datum 01.01.2011 zwar vor, jedoch hat das national zuständige DIN-Gremium in 2011 entschieden, dass es keine entsprechende DIN ISO 31000-Norm geben wird. Der vorliegende Norm-Entwurf bleibt in unveränderter Form bestehen und wird nach Ende der zweijährigen Laufzeit ersatzlos zurückgezogen. Die ÖNORM bleibt aber weiterhin gültig, deshalb beziehen sich alle nachfolgenden Ausführungen auf diese Norm.

Hauptzweck dieser Abhandlung ist es, potentiellen Anwendern Hinweise zu geben, wie Sie diese Empfehlungen in der Praxis umsetzen können. Dabei ist es unerheblich ob die jeweilige Organisation zertifiziert ist oder nicht. Selbstverständlich ist es **sehr hilfreich**, wenn eine Prozessbeschreibung vorliegt, aber selbst das Fehlen einer solchen, sollte die Organisation nicht daran hindern, eine angemessene Risikobetrachtung durchzuführen, denn es sind immer Mindeststandards zu erfüllen.

Zu diesen **Mindeststandards** zählen die gesetzlichen und behördlichen Forderungen sowie die Forderungen aus Vertragswerken der Organisation (z.B. mit Kunden, Lieferanten, Verbänden, anderen Organisationen).

Weisen Vertragswerke oder eigenen Ansprüche auf weitere Standards hin, wie z.B.:

- ISO 9001 (Qualitätsmanagement)
- ISO/TS 16949 (Qualitätsmanagement Automobilindustrie) und
- ISO 14001 (Umweltmanagement)
- OHSAS 18001 (Arbeits- und Gesundheitsschutz)
- ISO 50001 (Energiemanagement)

(in jeweils gültiger Fassung) erhöhen sich automatisch die Mindeststandards und damit auch die Risiken, diese Mindeststandards nicht zu erfüllen.

Eine Nichterfüllung hat in den meisten Fällen als Konsequenz, dass

- sich Mitglieder und Kunden der Organisation oder sonstige Interessengruppen ärgern,
- dass der Organisation zusätzlich Kosten entstehen oder
- gar persönliche Haftungsfragen behandelt werden müssen.

Die folgenden Ausführungen sollen Hilfestellung geben, diese Konsequenzen zu vermeiden oder wenigsten deutlich zu reduzieren.

Gensingen, den 17. Februar 2012

Peter Wintzer
Management- und Organisations-Beratung
www.pwmp.de

Risikomanagement nach ISO 31000

Umsetzung in der Organisation

2 Grundlagen zum Risikomanagement

2.1 Gemeinsamkeiten der Risikobetrachtung

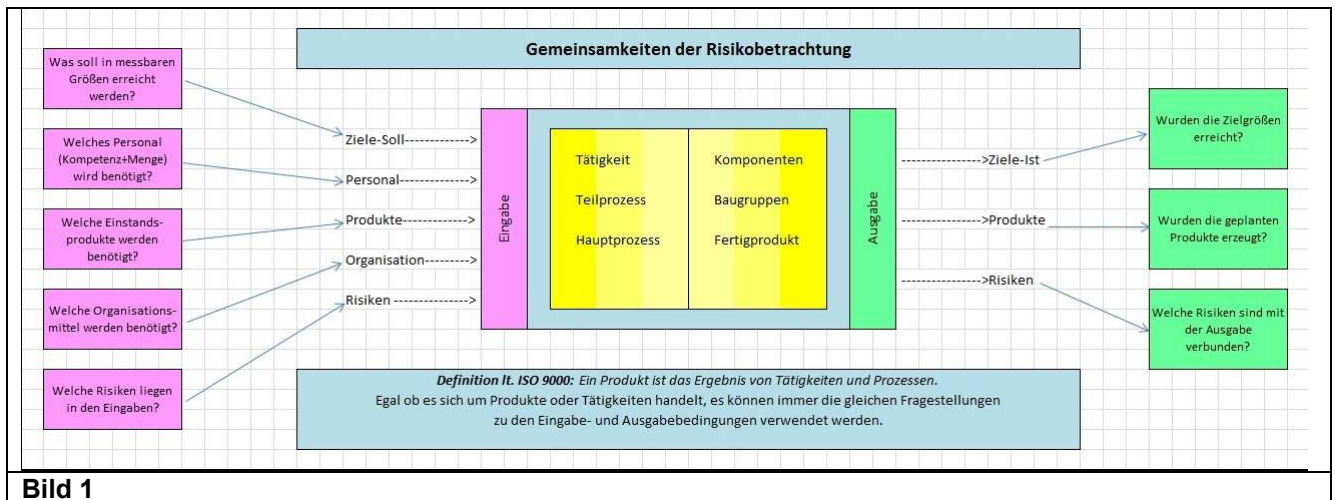
Es spielt keine Rolle, ob Risiken betrachten werden, die von **Produkten** ausgehen oder von **Prozessen**. Dazu muss zunächst geklärt sein, was unter dem Begriff „Produkt“ zu verstehen ist.

Gemäß ISO 9000: Ein Produkt ist das Ergebnis von Tätigkeiten und Prozessen.

Es gibt vier anerkannte übergeordnete Produktkategorien:

- Dienstleistungen (z.B. Transport),
- Software (z.B. Rechnerprogramm, Wörterbuch);
- Hardware (z.B. mechanisches Motorteil);
- verfahrenstechnische Produkte (z.B. Schmiermittel).

In allen Fällen haben wir es mit den gleichen Eingabe- und Ausgabebedingungen zu tun (**Bild 1**).



Stellt man die beiden Gruppen **Produkte** und **Prozesse** mit Ihren Eingabe- und Ausgabebedingungen gegenüber, ist bei den Verarbeitungsbedingungen zu erkennen, dass es lediglich um sprachliche Unterschiede handelt. So wird bei Produkten in der Regel von **Merkmale und Merkmalsausprägungen** und bei Prozessen von **Zielen und Zielgrößen** gesprochen. In der eigentlichen Bedeutung unterscheiden sich diese Sachverhalte aber nicht (**Bild 2**).

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

Eingaben	Verarbeitungsbedingungen		Ausgaben
	Tätigkeiten	Produkte	
Was soll in messbaren Größen erreicht werden?	Wer hat bis wann welche Ziele zu erreichen?	Welche Produktmerkmale mit welcher Ausprägung sollen erzeugt werden?	Wurden die Zielgrößen erreicht?
Welches Personal (Kompetenz+Menge) wird benötigt?	Wieviel Personal mit welcher Ausbildung wird benötigt?	Wieviel Personal mit welcher Ausbildung wird benötigt (Die Personalmenge wird oft über Zeitbedarf in den Arbeitsplänen ermittelt)?	War genügend Personal vorhanden?
Welche Einstandsprodukte werden benötigt?	Welches Material in welcher Menge hat die Organisation zur Verfügung zu stellen?		Entsprechen die Produkte den Forderungen?
	Alle Hilfsmaterialien	Produktbestandteile, die meistens über eine Stückliste ausgewiesen sind, inkl. Hilfsmaterialien.	
Welche Organisationsmittel werden benötigt?	Welche Organisationsmittel muss die Organisation zur Verfügung stellen?		Waren die Organisationsmittel geeignet?
	Hard- und Software	Alle Produktionseinrichtungen und Hilfsvorrichtungen, meistens über einen Arbeitsplan ausgewiesen sowie Hard- und Software	
Welche Risiken liegen in den Eingaben?	Betrachtung der Risiken, die in den Eingaben zu Tätigkeiten, Teil- oder Hauptprozessen liegen	Betrachtung der Risiken, die in den Eingaben zu Rohstoffen, Komponenten oder Fertigprodukten liegen	Welche Risiken sind mit den Ausgaben verbunden?

Bild 2

Auch wenn man die Risikobereiche von **Produkten** und **Prozessen** gegenüberstellt (Bild 3), ist zu erkennen, dass sich Risikoquellen und Risikoauswirkungen nicht unterscheiden.

Risikobereiche	Risikoquellen		Risikoauswirkung
	Tätigkeiten	Produkte	
Was soll in messbaren Größen erreicht werden?	Festlegung falscher Ziele oder Zielgrößen.	Festlegung falscher Merkmale oder Merkmalsausprägungen.	Die messbaren Größen sind nicht erreicht.
Welches Personal (Kompetenz+Menge) wird benötigt?	Personalqualifikation und -kapazität nicht ausreichend.		Arbeitsergebnis entspricht nicht den Anforderungen.
Welche Einstandsprodukte werden benötigt?	Falsche oder fehlerhafte Produkte kommen zum Einsatz.		Arbeitsergebnis entspricht nicht den Anforderungen.
Welche Organisationsmittel werden benötigt?	Es werden falsche oder fehlerhafte Organisationsmittel verwendet.		Arbeitsergebnis entspricht nicht den Anforderungen.

Bild 3

2.2 Risikobetrachtung nach ISO 31000

Die Einleitung zur **ÖNORM ISO 31000:2010** enthält u.a. folgende Abschnitte:

Alle Aktivitäten einer Organisation sind mit Risiken verbunden. Organisationen behandeln diese Risiken, indem sie sie identifizieren und analysieren und dann beurteilen, ob das Risiko durch Maßnahmen der Risikobewältigung so verändert werden soll, dass es den jeweiligen Risikokriterien entspricht. Während des gesamten Prozesses kommunizieren sie mit Stakeholdern, konsultieren diese und überwachen und überprüfen die Risiken sowie die Kontrollen zur Veränderung des Risikos, um sicherzustellen, dass keine weiteren Maßnahmen zur Risikobewältigung erforderlich sind. Diese Internationale Norm bietet eine detaillierte Beschreibung dieses systematischen und logischen Prozesses.

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

Zwar behandeln alle Organisationen Risiken in einem gewissen Ausmaß, aber diese Internationale Norm legt eine Reihe von Grundsätzen fest, die für ein wirkungsvolles Risikomanagement einzuhalten sind. Diese Internationale Norm empfiehlt, dass Organisationen einen Rahmen entwickeln, umsetzen und laufend verbessern, um den Prozess für die Behandlung von Risiken in die allgemeinen Führungs- (Governance), Strategie- und Planungs-, Management- und Berichterstattungsprozesse, Politik, Werte und Kultur einzubinden.

Die ISO 31000 unterscheidet sich von anderen Managementsystemnormen wie z. B. ISO 9001, ISO 14001 oder OHSAS 18001 dadurch, dass Sie keine Vorgaben für die Gestaltung von Einzelprozessen der Organisation beinhaltet, sondern eine Methode beschreibt, wie Risiken in bestehenden Organisationen erkannt und gesenkt werden können. Dieses wird auch im Kapitel 1 der Norm durch den nachfolgenden Abschnitt verdeutlicht:

*Diese Internationale Norm kann während des gesamten Bestehens einer Organisation auf ein breites Spektrum von **Tätigkeitsbereichen** angewandt werden, wie zum Beispiel **Strategien und Entscheidungsfindung, operativer Betrieb, Prozesse, Funktionen, Projekte, Produkte, Dienstleistungen und Vermögenswerte.***

Für die Durchführung von Risikobeurteilungen an **Produkten** und **Prozessen** gibt ISO 31000 auch keine Einheitsmethode vor. Deshalb ist es erforderlich, sich innerhalb einer Organisation auf die Anwendung bestimmter Methoden festzulegen, die für die Beurteilung der spezifischen Produkte und Prozesse geeignet und nutzbringend sind. Das heißt nicht, eine eigene Methode zu erfinden, sondern aus dem Angebot der ISO 31000 eine eigene methodische Vorgehensweise zu entwickeln.

3 Risikobewertungsschritte auf Grundlage der ISO 31000

Abgeleitet aus den Abschnitten 5.3 – 5.6 der Norm ergeben sich die nachfolgenden drei Phasen mit einzelnen Methodenschritten:

3.1 Analysephase

Beginnt mit der Feststellung des Risikos und endet mit der Ermittlung einer Risikozahl (**Bild4a**).

	Methodenschritte:	Methodenhinweise:	Umsetzungshinweise
Analyse	Risikoquelle	Wo tritt das Risiko auf?	Risikoquellen können sein: Produktbezogen = Komponenten, Baugruppen, Fertigprodukte Prozessbezogen = Tätigkeitsschritte, Teilprozesse, Hauptprozesse
	Risikofall	Um welches Risiko handelt es sich?	Risiken können immer liegen in einer fehlerhaften Planung, Durchführung oder Überwachung von Zielen, Personal, Organisation oder Produkten (Details dazu siehe Merkmalskatalog).
	Risikoauswirkung	Wohin wirkt sich das Risiko aus?	Hier kann das Spektrum gehen von kaum feststellbar, deutlich sichtbar, Umweltschaden, Unfallgefährdung bis Tod eines Menschen mit oder ohne persönliche Haftung des Verursachers.
	Risikoursache	Welche Ursache hat der Risikofall?	Hierbei handelt es sich um einen weiteren Detaillierungsgrad des Risikofalls, weshalb hier die gleiche Logik zur Anwendung kommt (Details dazu siehe Merkmalskatalog).
	Risikoeinfluss	Welche Faktoren nehmen Einfluß auf die Risikoursache?	Hier wird die Risikoursache aus dem Blickwinkel der internen und/oder externen Umfeldgestaltung betrachtet (z. B. Personalqualifikation, Fähigkeiten der technischen Einrichtungen, Klima)
	Risikofeststellung	Welche Maßnahmen zur Risikofeststellung sind implementiert?	Hier werden die Maßnahmen betrachtet, die in der Organisation implementiert sind, um rechtzeitig zu erkennen, dass sich eine Risikosituation entwickelt.
	Risikohöhe; absolut	Bewertungszahlen	Bewertungszahlen zur Auswirkung , Ursache, Feststellung (wie z. B. bei dem etablierten Verfahren FMEA von 1-10).
	Risikohöhe; akzeptierbar	Bis zu welcher Höhe kann das Risiko akzeptiert werden?	Akzeptanzgrenzen für Auswirkung , Ursache, Feststellung oder die Risikozahl (passend zu den Bewertungszahlen).
	Risikozahl	Summe aus Bewertungszahlen	Risikozahl, gebildet aus der Summe der einzelnen Bewertungszahlen (z.B. analog FMEA, dort RPZ (Risiko-Prioritäts-Zahl) genannt).

Bild 4a

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

3.2 Maßnahmenphase

Beginnt mit der Erarbeitung von Vorschlägen zur Beseitigung oder Minimierung des Risikos und endet mit dem Beschluss zur Durchführung von konkreten Einzelmaßnahmen mit Verantwortungen und Terminen (**Bild 4b**).

	Methodenschritte:	Methodenhinweise:	Umsetzungshinweise
Maßnahmen	Maßnahmen; Plan	Welche Maßnahmen sind geeignet?	Erarbeiten von Maßnahmen (eine oder mehrere), die geeignet sind, das festgestellte Risiko zu beseitigen oder zu minimieren.
	Ressourcen	Welche Ressourcen werden zur Umsetzung der Maßnahme benötigt?	Benennen der dazu erforderlichen Ressourcen (Personal, Material, Technik, Organisation), letztlich zusätzlich in Kosten ausgedrückt.
	Genehmigung	Wer darf die Maßnahme genehmigen?	Ermitteln, wer die Kompetenz hat, die Maßnahmen bewerten und entscheiden zu können.
	Maßnahmen; Ist	Welche Maßnahmen wurden ausgewählt?	Dokumentieren, welche Maßnahme(n) zur Umsetzung ausgewählt wurde.
	Begründung	Warum wurde die Maßnahmen ausgewählt?	Begründen, warum diese Maßnahme(n) ausgewählt wurde und ob ggf. noch ein Restrisiko besteht.
	Vorgabe	Bis wann ist die Maßnahme umzusetzen?	Zu jeder einzelnen Maßnahmen die Ausführungstermine festlegen.
	Verantwortung	Wer hat die Maßnahme umzusetzen?	Zu jeder einzelnen Maßnahmen die Ausführungsverantwortung festlegen.

Bild 4b

3.3 Überwachungsphase

Beinhaltet die Überwachung der Maßnahmendurchführung und endet mit einer abschließenden Prüfung des Gesamtvorgangs (**Bild 4c**).

Überwachung	Maßnahmenkontrolle	Wurde die Maßnahme planmäßig umgesetzt?	Festlegen, in welcher Form die Realisierung der Einzelmaßnahme überwacht werden soll und wer diese durchführt.
	Maßnahmenwirksamkeit	War die Maßnahme auch wirksam?	Festlegen, in welcher Form die Wirksamkeit der Einzelmaßnahme überwacht werden soll und wer diese durchführt.
	Restrisiko	Besteht noch ein Restrisiko?	Festlegen, wer nach der Wirksamkeitsprüfung bewertet, ob noch ein Restrisiko bestehen bleibt.
	Abschluss	Wurde das Endergebnis bewertet?	Feststellen, ob alle zuvor genannten Einzelschritte ordnungsgemäß abgearbeitet wurden.

Bild 4c

4 Risikobewertungsbeispiele

Nachfolgend sind einige klassische Risikogruppen benannt und mit praktischen Umsetzungsbeispielen belegt oder auf entsprechende Verfahren verwiesen.

4.1 Produkte

Was unter dem Begriff „Produkt“ verstanden wird, ist bereits in Pkt. 2.1 definiert.

Somit fallen hierunter alle Produkte, die von einer Organisation ihren Kunden angeboten werden (gegen Entgelt oder als Serviceleistung), aber auch Verbrauchsmaterialien der Organisation.



Risikomanagement nach ISO 31000 Umsetzung in der Organisation

Hier liegen die Risikoquellen in der Entwicklung (Planung) der Produkte, deren Herstellung sowie Auslieferung und können u. a. nachfolgende Sachverhalte umfassen:

- Produkt und Marktanforderungen stimmen nicht überein (Absatzchancen)
- Produkt entspricht nicht den Vorstellungen des Kunden/Abnehmers (so habe ich mir das nicht vorgestellt)
- Produkt erfüllt nicht die vorgesehenen Funktionen (Produkt hat einen Fehler)
- Produkt und deren Herstellung wirken sich negativ auf die Umwelt aus (Emissionen)
- Produkt kann nicht in gewünschter Menge hergestellt werden (Engpassressourcen)
- Produkt enthält Anwendungsrisiken (Verletzungsgefahr)
- Produkt ist mit Transportschäden behaftet (Kundenverärgerung)

Hierfür gibt es bereits etablierte Verfahren zur Risikobewertung, am bekanntesten dürfte das in der Automobilindustrie verwendete Verfahren der FMEA sein, das auch Komponenten, Baugruppen und Fertigprodukte umfasst. Da mir bekannt ist, dass diese Methode die unter Pkt. 3 genannten Methodenschritte grundsätzlich enthält und es hierzu reichlich Literatur am Markt gibt, gehe ich auf diesen Aspekt nicht weiter ein.

4.2 Prozesse

4.2.1 Hauptprozesse

Selbstverständlich ist es möglich, auch für Hauptprozesse eine Risikobewertung durchzuführen. Nach meiner Meinung ist diese Prozessebene aber zu abstrakt, um eine umfassende Erhebung der Risikofälle vornehmen zu können. Da die Vorgehensweise aber die gleiche ist, die auch für einen Teilprozess oder Tätigkeitsschritt zutrifft, kann der Anwender selber entscheiden, welche Betrachtungsebene er wählen will. Beispiele für Hauptprozesse können **Bild 5** entnommen werden.

Risikomanagement nach ISO 31000 Umsetzung in der Organisation



Bild 5: Prozesslandschaft

4.2.2 Teilprozesse


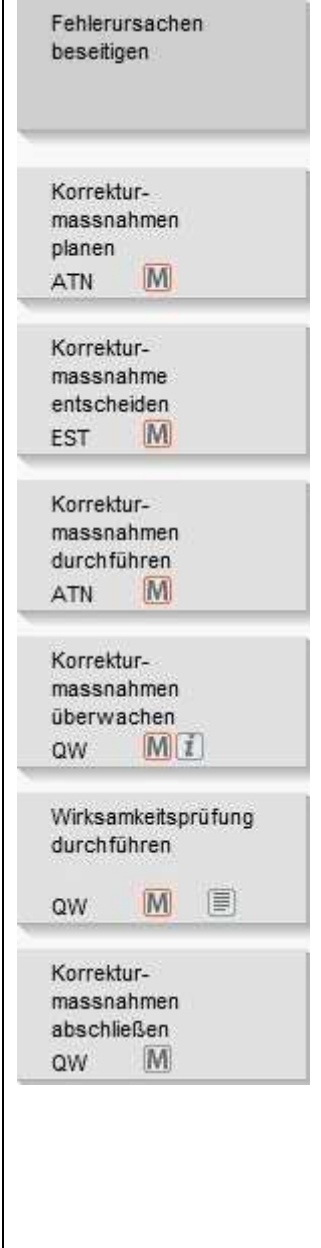
Bei Teilprozessen handelt es sich nach meiner **eigenen Definition** um eine unmittelbare Folge von Tätigkeitsschritten, mit einer klar festgelegten Eingabe- und Ausgabebedingung. Egal mit welchem Teilprozess man sich in einer Organisation beschäftigt, immer besteht das Risiko einer Fehlhandlung:

- bei der Festlegung von Kompetenzen,
- bei der Planung von Schulungsmaßnahmen,
- bei der Bewertung möglicher Währungsschwankungen,
- bei der Erstellung von Angeboten,
- bei der Entwicklung von Produkten,
- bei der Beschaffung von Rohstoffen,

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

- bei der Lagerung,
- bei der Verpackung,
- beim Transport

um nur einige wenige Beispiele zu benennen. Zwei Beispiele für mögliche Teilprozesse siehe nachfolgende **Bilder 6a+b**:

	<p>Hierbei handelt es sich um einen Auszug aus dem Hauptprozess „Kundenbetreuung“.</p> <p>Eingabebedingung: Eine Kundenanfrage liegt vor</p> <p>Ausgabebedingung: Angebot wurde an Kunden gegeben und in eine Überwachungsdatei eingetragen.</p> <p>Verarbeitung: Die Tätigkeitsschritte werden in einem Hauptprozess in unmittelbarer Folge ausgeführt</p>		<p>Hierbei handelt es sich um einen Auszug aus dem Hauptprozess „Reklamationsmanagement“.</p> <p>Eingabebedingung: Eine Abweichung aus verschiedenen Gründen liegt vor</p> <p>Ausgabebedingung: Die Korrekturmaßnahme wurde erfolgreich abgeschlossen.</p> <p>Verarbeitung: Die Tätigkeitsschritte werden in einem Hauptprozess in unmittelbarer Folge ausgeführt</p>
<p>Bild 6a</p>	<p>Bild 6b</p>		

Risikomanagement nach ISO 31000 Umsetzung in der Organisation



Die Höhe des Risikos nimmt mit Art und Menge der Einflussfaktoren auf die Tätigkeit zu. **Beispiel:**

- **bei der Entwicklung von Produkten:** Forderungen aus diversen Gesetzen (z. B. Umwelt, Produkthaftpflicht), von Behörden/Kommunen (z. B. Betriebsgenehmigungen) und Kunden (z. B. Vorgaben aus Lastenheften), Normen und Regelwerken, Stand der Technik, Fähigkeiten der Herstellungsprozesse und Prüfmittel
- **bei der Beschaffung von Rohstoffen:** Vielzahl der in- und ausländischen Anbieter, Währungsschwankungen, Versorgungsengpässe

4.2.3 Prozesskette

Bei einer Prozesskette handelt es sich nach meiner **eigenen Definition** um eine zusammenhängende Folge von Tätigkeitsschritten über **mehrere** Hauptprozesse, mit einer klar festgelegten Eingabe- und Ausgabebedingung.

Auch hierzu nachfolgend ein **nicht vollständiges** Beispiel zum „**Ausgangsrechnungsfluss**“:

Auftragsbestätigung erstellen VT 	Im Zuge der Erstellung eine Auftragsbestätigung im Hauptprozess „Kundenbetreuung“ werden die Grundlagen für die aus dem Auftrag resultierende Rechnung gelegt.
Versandgut vorbereiten und verladen 	Im Hauptprozess „ Logistik “ wird mit der Versandbereitstellung und entsprechenden Buchungen die Grundlage für die Rechnungsstellung gelegt.
Ausgangsrechnungen erstellen und verbuchen RW	Im Hauptprozess „ Finanzmanagement “ erfolgt die Rechnungsstellung und deren Versand an den Kunden.
Zahlungseingänge buchen RW	Ebenfalls Im Hauptprozess „ Finanzmanagement “ wird der Eingang der Rechnungssumme verbucht.

Ansonsten gelten die gleichen Ausführungen wie unter dem Abschnitt „Teilprozesse“.

4.2.4 Tätigkeitsschritte

Die Quellen für Risiken liegen ausschließlich auf der Ebene von Tätigkeitsschritten. Ob es immer sinnvoll ist, die Risiken nur auf dieser Ebene zu betrachten, ist abhängig von den in den vorausgegangenen Abschnitten genannten Ausgangssituationen. Allerdings ist die Logik zum Vorgehen in allen Fällen gleich und wird deshalb von mir ausschließlich auf dieser Ebene beschrieben.

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

4.2.5 Zusammenfassende Betrachtung dieser Risikoquellen

Selbstverständlich kann davon ausgegangen werden, dass in vielen Organisationen heute schon vorausschauend, systematisch und reproduzierbar Risikomanagement betrieben wird. Dieses umfasst nach meinen Erfahrungen **mindestens** folgende Sachverhalte:

Risikoart	Methode	Erläuterung
Umweltrisiken	Umweltaspekte	<p>Organisationen, die nach ISO 14001 zertifiziert sind, müssen ein Verfahren zur Ermittlung der Umweltrisiken praktizieren. Hierzu gibt es keine etablierte Methodenvorgabe, aber vielfach wird dazu die FMEA-* Struktur verwendet. Die Ermittlung der Umweltraspekte umfasst:</p> <ul style="list-style-type: none"> • Risiken die vom Produkt selbst ausgehen und Gefährdungen der Umwelt nach sich ziehen können • Risiken die in der Herstellung des Produktes liegen und Gefährdungen der Umwelt nach sich ziehen können • Betrachtung der Einsparpotentiale von Ressourcen
Produkttrisiken	Produkt-FMEA*	<p>Bei Zertifizierungen nach ISO 9001 (kann) und ISO/TS 16949 (muss) eine Methode zur Feststellung der von einem Produkt ausgehenden Risiken praktiziert werden. Sehr häufig wendet man hier die Methode FMEA* an, für die es in der Automobilindustrie eine Methodenvorgabe gibt, die allerdings auch von anderen Industriezweigen übernommen wurde. Im wesentlichen sind es zwei Betrachtungen, die hier angestellt werden:</p> <ul style="list-style-type: none"> • Welchen Risiken ist der Anwender der Produkte ausgesetzt? • Wie ist gewährleistet, dass das Produkt die gewünschten Eigenschaften über die Lebensdauer behält?
Herstellungsprozessrisiken	Prozess-FMEA*	<p>Bei Zertifizierungen nach ISO 9001 (kann) und ISO/TS 16949 (muss) eine Methode zur Feststellung der sicheren Herstellung eines Produkts praktiziert werden. Auch hier wendet man häufig die zuvor beschriebene Methode FMEA* an. Im wesentlichen sind es zwei Betrachtungen, die hier angestellt werden:</p> <ul style="list-style-type: none"> • Wie sicher ist der Herstellungsprozess, um zu gewährleisten, dass die gewünschten Produkteigenschaften dauerhaft hergestellt werden können? • Wie sicher ist der Herstellungsprozess, um zu gewährleisten, dass die Produkte gemäß den Kundenvorgaben angeliefert werden?
Finanzrisiken	Betriebsprüfung	<p>Eine systematisch durchgeführte Betriebsprüfung wird selbstverständlich auch Risikopotentiale feststellen, aber sie ist nicht als vorausschauend zu betrachten, sondern wird immer den Ereignissen nachlaufen. Deshalb kann sie nicht als Risikoermittlungsmethode eingesetzt werden.</p>

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

Risikoart	Methode	Erläuterung
Geschäftsprozessrisiken	Prozessanalyse	<p>Selbstverständlich wäre es möglich, die einzelnen Tätigkeitsschritte eines Geschäftsprozesses auch mit der FMEA*-Methode zu analysieren. Mir sind nur wenige Einzelfälle bekannt, in denen das tatsächlich geschieht. Das heißt aber nicht, dass hier keine Risikobetrachtungen angestellt werden. In den Fällen, in denen bei der Erstellung der Beschreibung der Geschäftsprozesse konsequent das EVA-Prinzip zur Anwendung kommt, ist hier bereits ein hohes Maß an Risikobetrachtung erfolgt. EVA-Prinzip heißt:</p> <ul style="list-style-type: none"> • Eingabe: Was wird alles benötigt, um den Tätigkeitsschritt fehlerfrei ausführen zu können? • Verarbeitung: Was geschieht im Einzelnen und was muss bei der Ausführung des Tätigkeitsschrittes berücksichtigt werden? • Ausgabe: Was ist das Ergebnis des Tätigkeitsschrittes und entspricht es den Anforderungen des Kunden (in diesem Fall der nächste Tätigkeitsschritt)?

**FMEA = Fehler-Möglichkeiten- und Einfluss-Analyse: Eine in der Automobilindustrie übliche und auch teilweise von Kunden vorgeschriebene Methode zur Ermittlung von Produkt- und Herstellungsprozessrisiken.*

Werden also in einer Organisation bereits Umweltaspekte ermittelt und FMEAs* erstellt, kann dieser Bereich zunächst im Sinne der ISO 31000 als erledigt betrachtet werden, auch wenn vielleicht einige Detailkriterien nicht enthalten sind (siehe Tabellen unter Pkt. 3). Unabhängig davon beziehen sich die folgenden Ausführungen auf alle Prozesse einer Organisation.

5 Risikobetrachtung Tätigkeiten

Das Vorgehen für eine Risikobetrachtung wird nachfolgend auf der Grundlage der in Abschnitt 3 dokumentierten Phasen an einem Tätigkeitsbeispiel erläutert. Da mir für die Risikobetrachtung an Prozessen keine **integrierte** Software bekannt ist, kann die nachfolgend beschriebene Vorgehensweise auch als Aufforderung an Softwareorganisationen verstanden werden, hier Abhilfe zu schaffen. Selbstverständlich handelt es sich hier um die Meinung des Autors, Varianten sind möglich.

5.1 Analysephase: Risikoquelle bis Risikozahl

5.1.1 Risikoquelle und Risikofall

In den meisten mir bekannten Managementsystembeschreibungen wird auch das EVA-Prinzip eingehalten (siehe Tabelle Abschnitt 4.2.5 und **Bild 7**). Deshalb setze ich hier mit der Betrachtung an.

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

Prozess: Kundenbetreuung		Hier sollte jeweils eine zusätzliche Schaltfläche/Auswahlbutton RG eingefügt sein, nach deren Betätigung sich pro Pos. ein neues Eingabefeld mit Risikoquellen öffnet (Bild 8a-c).
Tätigkeit: Machbarkeit Kundenanfrage klären		
Eingabe:	RG Kundenanfrage, Fähigkeitsdaten, Kaufmännische Kundendaten	
Verarbeitung:	RG Prüfen der Anfrage auf Machbarkeit, sofern erforderlich unter Einbeziehung der betroffenen Fachbereiche	
Ausgabe:	RG Produkt- und Herstellungsprozessdaten als Grundlage zur Kalkulation und zur Angebotserstellung	

Bild 7

Risikogruppe Eingabe		Bei den Risikoquellen zur „Eingabe“ sollte in der linken Spalte eine individuelle Anzahl von Eingabefeldern vorgesehen werden, die in Stammdaten vordefiniert sind. Auch die rechte Spalte muss pro Risikoquelle eine individuelle Anzahl von Eingabefeldern vorsehen, die allerdings nicht vorbelegt sind, die aber durch Zugriff auf Stammdaten gefüllt werden können. Bei „ Ziele: “ kann ggf. auf die Inhalte der bereits an anderer Stelle definierten Felder mit Zieleangaben zugegriffen werden.
Risikoquellen:	Risikofälle lt. Merkmalsliste (Auswahl)	
Ziele:	Richtpreis als Kundenvorgabe fehlerhaft Lieferdatum falsch Prozeßfähigkeiten nicht eingehalten	
Personal:	Personalqualifikation nicht ausreichend Personalkapazität nicht ausreichend Rahmenbedingungen ungeeignet	
Material:	Materialverfügbarkeit nicht gewährleistet Materialeigenschaft nicht gewährleistet Umwelteigenschaften nicht gewährleistet	
Organisation:	Planungsvorgaben fehlerhaft Maschinenkapazität nicht ausreichend Software nicht verfügbar	

Bild 8a

Risikogruppe Verarbeitung		Bei den Risikoquellen zur „Verarbeitung“ sollte in der linken Spalte eine individuelle Anzahl von Eingabefeldern vorgesehen werden, die in Stammdaten vordefiniert sind, ohne dass diese hier benötigt werden. Auch die rechte Spalte muss pro Risikoquelle eine individuelle Anzahl von Eingabefeldern vorsehen, die allerdings nicht vorbelegt sind, die aber durch Zugriff auf Stammdaten gefüllt werden können.
Risikoquellen:	Risikofälle lt. Merkmalsliste (Auswahl)	
Allgemein:	Dateneingaben fehlerhaft Datenbewertung fehlerhaft Fachbereiche nicht einbezogen	

Bild 8b

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

Risikogruppe Ausgabe		<p>Auch bei den Risikoquellen zur „Ausgabe“ sollte in der linken Spalte eine individuelle Anzahl von Eingabefeldern vorgesehen werden, die in Stammdaten vordefiniert sind, ohne dass diese hier benötigt werden.</p> <p>Auch die rechte Spalte muss pro Risikoquelle eine individuelle Anzahl von Eingabefeldern ermöglichen, die allerdings nicht vorbelegt sind, die aber durch Zugriff auf Stammdaten gefüllt werden können.</p>
Risikoquellen:	Risikofälle lt. Merkmalsliste (Auswahl)	
Allgemein:	Empfängeradresse falsch ausgewählt	
	Vorgang in falsche interne Ablage	
	Vorgang verwechselt	

Bild 8c

Hier liegt der Schlüssel für die Akzeptanz einer Risikobetrachtung, indem eine **direkte Verknüpfung** zwischen den jeweiligen Tätigkeitsschritten (Prozessen) und einer Risikomanagement-Software besteht. Wird an der Prozessbeschreibung irgendetwas geändert, kann sofort die Risikobetrachtung mit angepasst werden. Alles was danach folgt, kann in der Risikomanagement-Software getrennt betrachtet werden.

5.1.2 Risikoauswirkung und Risikoursache

Jedem einzelnen Risikofall muss jetzt eine **Auswirkung** zugeordnet werden. Dabei sollte es sich immer um die kritischste Auswirkung handeln, deshalb besteht hier eine 1 zu 1 Beziehung zwischen dem Risikofall und der Auswirkung (**Bild 9**). Auch eine nicht wahrgenommene Chance ist hier als Auswirkung zu betrachten.

Allerdings gibt es hier noch **eine andere Betrachtungssicht**, die auch ihre Berechtigung hat: Einem Risikofall sollten mehrere mögliche Auswirkungen zuzuordnen sein, um im Falle der Abarbeitung des einen Risikos auch auf das Nächste (geringerwertige) aufmerksam gemacht zu werden.

Zur fehlerfreien Erfassung von Risikoauswirkungen sollte es Stammdaten geben, aus denen eine Auswahl getroffen werden kann, aber auch die freie Texteingabe muss möglich sein, um neue Situationen erfassen zu können.

Risikofälle lt. Merkmalsliste (Auswahl)		Risikoauswirkung
Richtpreis als Kundenvorgabe fehlerhaft	----->	Deckungsbeitragsverlust wegen fehlendem Auftrag
Lieferdatum falsch	----->	Konventionalstrafe wegen Terminüberschreitung
Prozeßfähigkeiten nicht eingehalten	----->	Personenschaden wegen Fehlfunktion

Bild 9

Anders sieht es bei der Feststellung der **Fehlerursache** aus. Hier kann es durchaus mehrere Ursachen für einen Risikofall geben (**Bild 10**). Eine Risikoursache ist von ihrer Natur her immer dann ein neuer Risikofall, wenn noch die Frage gestellt werden kann „**Warum ist die Ursache aufgetreten?**“ Deshalb kann für die Risikoursache auch auf die Merkmalsliste zugegriffen werden, es ist also kein neuer Stammdatensatz erforderlich.

Risikomanagement nach ISO 31000 Umsetzung in der Organisation

Risikofälle lt. Merkmalsliste (Auswahl)		Risikoursache
Dateneingaben fehlerhaft	----->	Lieferdatum falsch übertragen
	----->	Produkt-Nr. falsch übertragen
	----->	Mengenangaben falsch übertragen
	----->	usw.
Datenbewertung fehlerhaft	----->	Marktpreis falsch eingeschätzt
	----->	Falsches Vergleichsprodukt ausgewählt
Fachbereiche nicht einbezogen	----->	Fachbereichsvorgabe nicht aktuell
	----->	Rohstoffbeschaffung falsch eingeschätzt
	----->	

Bild 10

5.1.3 Risikoeinfluss und Risikofeststellung

Diese Aspekte können sich immer nur auf die Risikoursache beziehen und sollen ausweisen, welche Einflüsse (einer oder Mehrere) auf die mögliche Ursache(n) wirken (**Bild 11**) und wie das Eintreten des Risikos frühzeitig festgestellt werden kann (**Bild 12**).

Risikoursache		Risikoeinfluss (Beispiele)
Lieferdatum falsch übertragen	----->	Ablenkung durch Geräuschkulisse, keine Formatprüfung bei Datumseingabe, Monotonie in der Datenbearbeitung, usw.
Produkt-Nr. falsch übertragen		
Mengenangaben falsch übertragen		
usw.		
Marktpreis falsch eingeschätzt	----->	Informationsquelle nicht gesichert, Marktpreis unterliegt hohen Schwankungen
Falsches Vergleichsprodukt ausgewählt		
Rohstoffbeschaffung falsch eingeschätzt	----->	Rohstoffquelle unsicher, Rohstoffpreise stark schwankend, Rohstoffmenge begrenzt
Fachbereichsvorgabe nicht aktuell		

Bild 11

Risikoeinfluss (Beispiele)		Risikofeststellung
Ablenkung durch Geräuschkulisse, keine Formatprüfung bei Datumseingabe, Monotonie in der Datenbearbeitung, usw.		
Informationsquelle nicht gesichert, Marktpreis unterliegt hohen Schwankungen		
Rohstoffquelle unsicher, Rohstoffpreise stark schwankend, Rohstoffmenge begrenzt	----->	Übersicht der Rohstoffquellen aktuell halten
	----->	Aktuelle Trendbeobachtung der Rohstoffpreise
	----->	Warenfluss am Markt aktuell beobachten

Bild 12



Risikomanagement nach ISO 31000 Umsetzung in der Organisation

5.1.4 Risikohöhe und Risikozahl

Allein die Erfassung der Risiken ist nicht ausreichend für eine wirksame Gegensteuerung. Es muss auch eine Bewertung vorgenommen werden, um letztlich zu einer Bearbeitungsfolge zu kommen. Dazu muss den Methodenschritten **Risikofall**, **Risikoauswirkung** und **Risikofeststellung** eine Bewertungszahl zugeordnet werden. Hierzu enthält die ISO 31000 keine Vorgaben, aber es gibt hier Beispiele aus der geübten Praxis.

In der FMEA-Methode werden hier Bewertungszahlen zwischen 1 und 10 als **Risikohöhe** verwendet, denen folgende Bedeutung zugeordnet wird (die nachfolgenden Beispiele enthalten nur die Eckpunkte der jeweiligen Bewertungstabellen).

Risikofall/Fehlerfall (Häufigkeitszahl des Auftretens des Risikofalles)

- 1 = Es ist unwahrscheinlich, dass der Fehler auftritt.
- 10 = Es ist nahezu sicher, dass der Fehler auftreten wird.

Risikoauswirkung/Fehlerauswirkung (Bedeutungszahl der Risikoauswirkung)

- 1 = Es ist unwahrscheinlich, dass der Fehler irgendeine wahrnehmbare Auswirkung haben könnte.
- 10 = Der Fehler ist so schwerwiegend, dass die Schadensfolgen den Menschen betreffen können.

Risikofeststellung (Entdeckungszahl der Risikoursache)

- 1 = Es ist sicher, dass die Risikoursache entdeckt wird, da der nachfolgende Tätigkeitsschritt nicht ausgeführt werden kann, wenn das Risiko eintritt oder es ist eine 100%-Prüfung nachgeschaltet.
- 10 = Die Risikoursache kann aus technischen und / oder wirtschaftlichen Gründen nicht festgestellt werden.

Jede andere Zahlenreihe zwischen 1 und x kann den gleichen Zweck erfüllen.

Aus Addition, Multiplikation oder ähnlichen Rechenverfahren dieser Risikohöhen wird eine **Risikozahl** ermittelt, aus der eine Risikorangfolge abgeleitet werden kann. Diese Rangfolge sollte Grundlage sein für die nächste Phase, in der Korrekturmaßnahmen geplant und umgesetzt werden.

Allerdings sollten auch Grenzwerte festgelegt werden, aus denen entnommen werden kann, bis zu welcher Risikohöhe und/oder Risikozahl ein Risiko akzeptiert werden kann. Damit sind Untergrenzen festgelegt, mit denen verhindert wird, dass zu jeder Form eines Risikos auch Korrekturmaßnahmen beschlossen werden müssen.

5.2 Maßnahmenphase: Geplante Maßnahme bis Umsetzungsverantwortung

In dieser Phase werden mindestens zu den nicht akzeptierbaren Risiken Korrektur-, Vorbeugungs- und/oder Verbesserungsmaßnahme (im Folgenden Maßnahmen genannt) geplant, entschieden und umgesetzt. Dazu können der ISO 31000 folgende Methodenschritte entnommen werden:

Geplante Maßnahmen und Ressourcen:

Erarbeiten von Maßnahmen, die geeignet sind, das festgestellte Risiko zu beseitigen oder zu minimieren. Hier sollten immer dann auch Alternativvorschläge erarbeitet werden, wenn es deutlich unterschiedliche Wege zum Ziel gibt. Diese Vorschläge müssen auch die für die spätere Umsetzung erforderlichen Ressourcenangaben enthalten, ohne deren Kenntnis die Entscheider ggf. zu falschen Schlüssen veranlasst werden.



Risikomanagement nach ISO 31000

Umsetzung in der Organisation

Genehmigung:

Zunächst muss die Organisation auch eine Regelung besitzen (z. B. Stellenbeschreibung, Kompetenzliste), wer die Kompetenz besitzt, über Maßnahmen entscheiden zu dürfen, damit keine unnötigen Verzögerungen durch Kompetenzgerangel entstehen. Im konkreten Risikofall muss dann in der Software eine Zuordnung zu diesem Entscheidungsträger (Risikoverantwortlicher) möglich sein.

Ist-Maßnahmen und Begründung:

Der jeweilige Entscheidungsträger legt fest, welche der Maßnahmenvorschläge realisiert werden soll und dokumentiert seine Entscheidungsgründe.

Termin und Verantwortung:

Um die Maßnahme durchführen zu können, muss der verantwortliche Entscheidungsträger der jeweiligen Aufgabe noch den Ausführungstermin und den Ausführungsverantwortlichen zuordnen.

5.3 Überwachungsphase: Maßnahmenkontrolle bis Abschluss

Diese Phase beinhaltet alle Maßnahmen zur Überwachung der Maßnahmendurchführung bis zum formalen Abschluss der jeweiligen Risikobetrachtung.

Maßnahmenkontrolle:

Mit Hilfe eines geeigneten Maßnahmenüberwachungsmoduls (Maßnahmenmanager) wird durch die benannte Person (Name sollte der jeweiligen Maßnahme zugeordnet werden können) überwacht, dass die beschlossenen Maßnahmen auch tatsächlich umgesetzt werden.

Maßnahmenwirksamkeit, Restrisiko und Abschluss:

Je nach Aufgabenfestlegung wird durch diese benannte Person (hier könnte es sich um den Risikoverantwortlichen handeln) oder eine übergeordnete Instanz auch geprüft, ob die tatsächlich durchgeführte Maßnahme wirksam war. Diese Prüfung umfasst, ob das Risiko in dem geplanten Umfang gesenkt werden konnte, ob ein Restrisiko verbleibt und ob der Vorgang abgeschlossen werden kann. Das Ergebnis dieser Prüfung ist zu dokumentieren.



Risikomanagement nach ISO 31000 Umsetzung in der Organisation

6 Zusammenfassung

Risikomanagement betrifft alle Bereiche und Geschäftsprozesse einer Organisation. In anderen Systemnormen, aber auch in Gesetzen und Verordnungen, wird ebenfalls auf die Anwendung von Risikomanagementmethoden verwiesen bzw. wird deren Anwendung gefordert. Mit der ISO 31000 ist ein übergreifender Leitfaden vorhanden, der sehr gut in die bestehenden Managementstrukturen integrierbar ist. So können zum Beispiel die in Systemnormen, Gesetzen oder Verordnungen geforderten Notfallpläne und daraus resultierende Aktivitäten eine Konsequenz aus der Risikobewertung sein.

Organisationen sind deshalb gut beraten, sich mit dieser Norm ernsthaft zu beschäftigen. Der damit verbundene Nutzen liegt im Wesentlichen in

- der Sicherung der Zielerreichung,
- der Senkung von Haftungsrisiken (Produkthaftung; aber auch persönliche Haftung der Geschäftsführer, Führungskräfte oder des ausführenden Personals),
- Steigerung des Vertrauens in die Fähigkeiten der Organisation,
- besserem Schutz vor Gefahren für Mensch und Umwelt,
- einer einheitlichen Methodenstruktur für alle Risikofälle.