Was ist **Risikomanagement** und wie funktioniert es?

Dr. Alexander Jaecklin, SNV Vorsitzender INB/NK 198 Risikomanagement

Die Entwicklung des Risikomanagements

"Risikomanagement" ist in den letzten Jahren ein viel gebrauchter Begriff geworden: Um dieses Schlagwort drehen sich sehr grosse Erwartungen aber auch viele Missverständnisse. Es ist daher an der Zeit, das Modewort "Risikomanagement" klar zu definieren und die Prozesse, die dahinter stecken zu normieren. Diese Aufgabe hat die Internationale Standardization Organization (ISO) angenommen und arbeitet eine neue Norm "ISO 31000:2009 Risk management – Guidelines on principles and implementation of risk management" als einen generischen Leitfaden für das Risikomanagement aus. Die Norm wird durch den ebenfalls in Überarbeitung stehenden "ISO Guide 73 Risk management – Vocabulary" begleitet.

Risikomanagement ist in keiner Weise neu und findet sich bereits in alten chinesischen Quellen. Der Begriff hat aber in den letzten Jahrzehnten zunehmend an Bedeutung gewonnen. Erste normative Ansätze können bei den Amerikanern ausgemacht werden, die für ihre Nasa-Projekte in den sechziger Jahren den US-MIL-STD 882 schufen. Eine ganze Reihe weiterer Normen wurden für die Durchführung von Risikoanalysen geschaffen wie beispielsweise FMEA (Fehler-Möglichkeits-Einfluss-Analyse), Fehlerbaumanalyse (FTA Fault tree analysis), Ereignisbaumanalyse (ETA Event tree analysis), HAZOP (Hazard & Operability) und viele mehr.

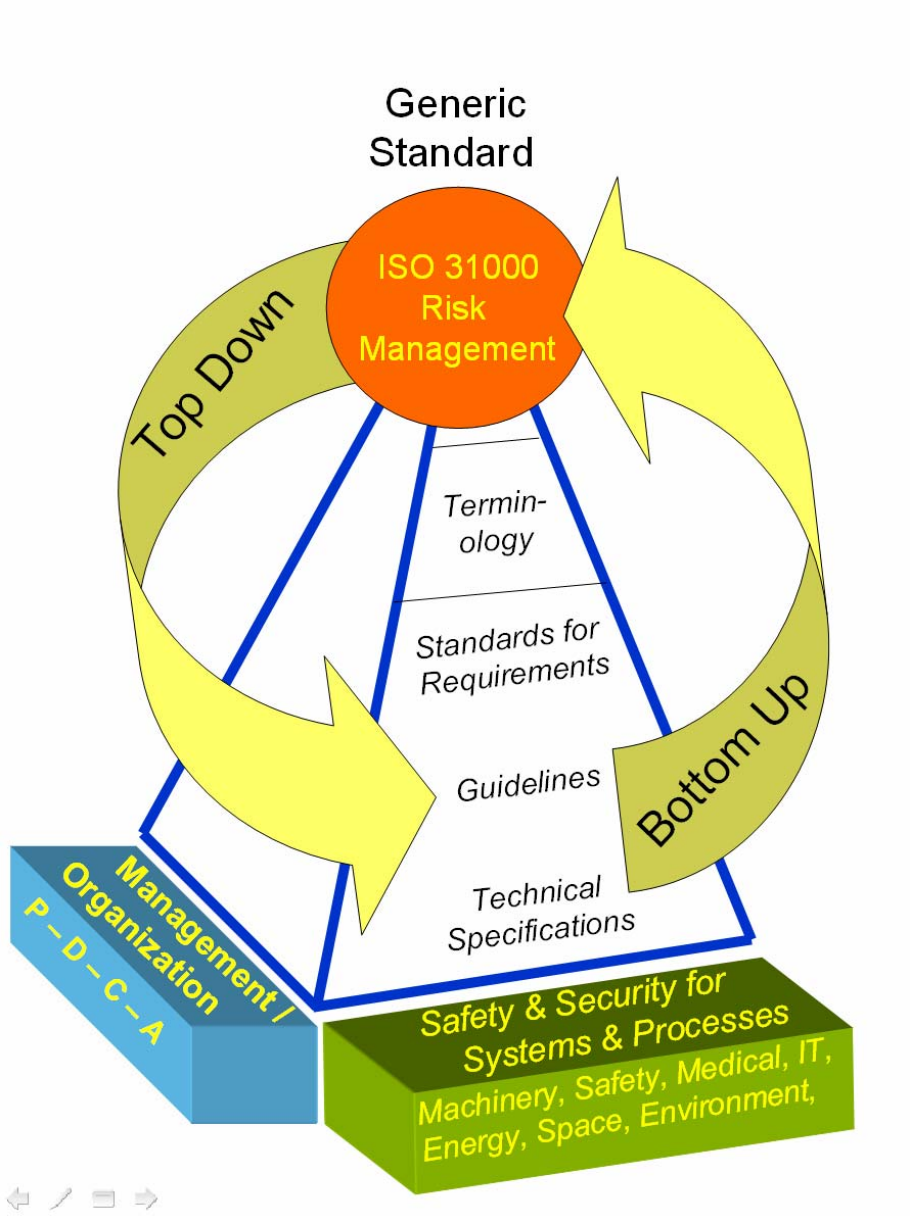
Im vergangenen Jahrzehnt dominierten zunehmend die Krisen in der Finanzwirtschaft und in der Grossindustrie. Insbesondere die Finanzwirtschaft hat Risikomanagement-Systeme aufgebaut, um die Risiken bei der Vergabe von Krediten und Hypotheken zu bewerten und durch Massnahmen Ausfälle zu minimieren. Das Ergebnis waren internationale Empfehlungen für die Kreditvergabe, beispielsweise Basel I und Basel II oder die Sicherstellung genügender Reserven bei den Versicherungen (Solvency I und II). Grosse Betrugsskandale und Bilanzfälschungen führten zur Schaffung neuer Gesetze für börsenkotierte Unternehmen. Darunter fallen die Sarbanes Oxley Act (SOX) oder das Kontroll- und Transparenzgesetz (KonTraG).

Schon früh wurde erkannt, dass die im Risikomanagement verwendeten Begriffe definiert und die Methodiken festgelegt werden sollten. So entstanden in verschiedenen Ländern, aber auch in der ISO-Organisation, eine ganze Anzahl von normativen Vorgaben. Diese waren sektorspezifisch auf bestimmte Technikbereiche ausgerichtet (Automobil, Medizinprodukte, Elektronik etc.). Heute wird Risikomanagement als systemischer und operativer Ansatz verstanden.

Der systemische Ansatz des Risikomanagements

Risikomanagement kann nur wirksam sein, wenn es in alle Unternehmensprozesse integriert wird. Risikomanagement kann und darf nicht als eine getrennte Führungsebene wie beispielsweise das Qualitätsmanagement, Umweltmanagement oder das Arbeitssicherheitsmanagement betrachtet werden. Risikomanagement ist in erster Linie eine Verantwortung der obersten Leitung, die die Risikostrategie und die Risikopolitik zu bestimmen hat. Es liegt auch in ihrer Verantwortung, im Rahmen des unternehmerischen Plan-Do-Check-Act-Zyklus die erforderlichen Vorgaben für die Durchführung der notwendigen Analysen zu machen.

Diesem Grundsatz tragen die Ausarbeitungen zu einer neuen generischen Norm zum Risikomanagement Rechnung. Dieses Vorgehen wird auch als systemischer Ansatz bezeichnet und beinhaltet die Integration der Risikoprozesse in die bestehenden Führungsprozesse. Risikomanagement ist eine Frage der Unternehmenskultur und muss auf allen Ebenen und allen Funktionen organisch integriert werden. In der Figur 1 ist dies mit dem Pfeil "Top Down" symbolisiert.

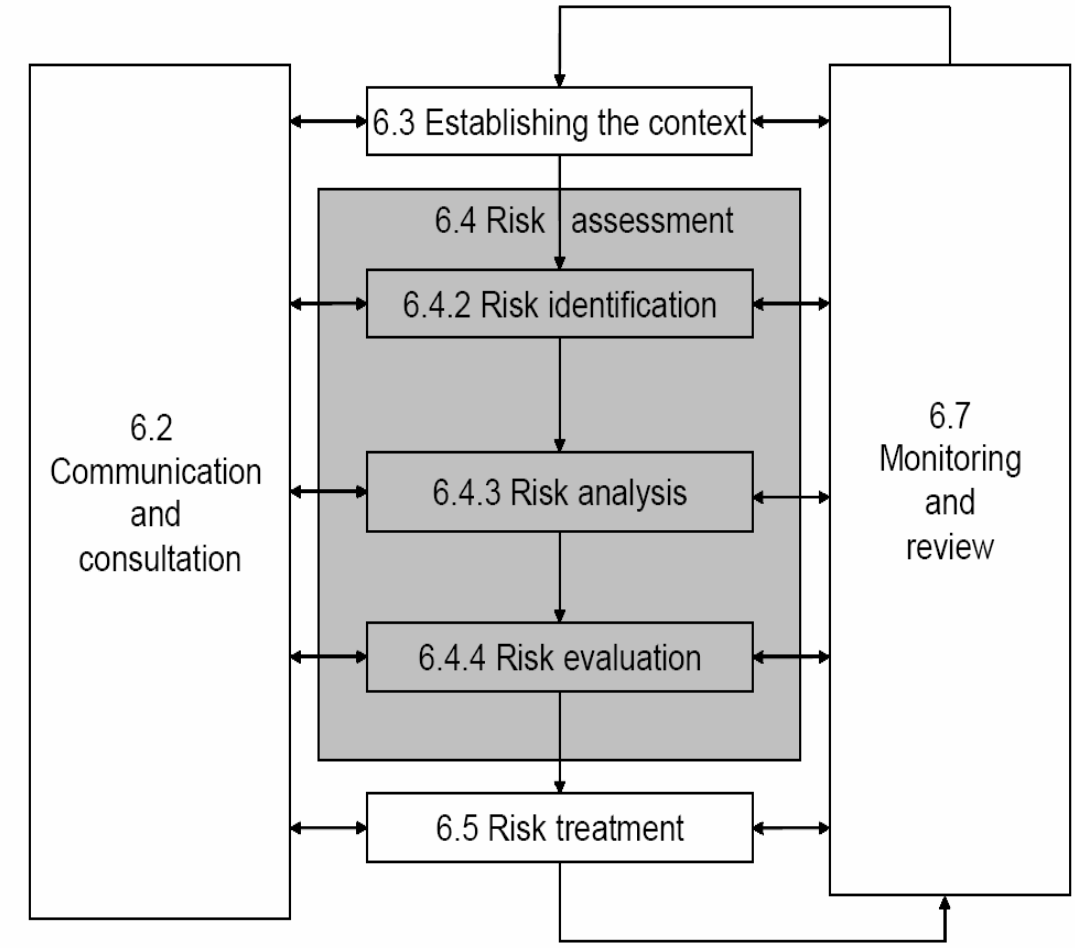


Figur 1: Risikomanagement beinhaltet einen starken systemischen Ansatz (Top Down) mit der Integration in die unternehmerischen Plan-Do-Check-Act-Entscheidungsabläufe. Der operative Ansatz des Risikomanagements beinhaltet den Risikomanagementprozess mit den Risikoanalysen (Bottom Up) in allen Aktivitätsbereichen eines Unternehmens.

Der systemische Ansatz des Risikomanagements erfasst alle Leistungserstellungsprozesse des Unternehmens oder der Organisation. Die entsprechende Integration in alle Teilbereiche der Aktivitäten eines Unternehmens erfordert eine sorgfältige Planung und Überwachung. Es wird daher erforderlich sein, die Risikomanagement-Aktivitäten zentral von der obersten Leitung zu steuern und zu überwachen. In der Praxis hat es sich gezeigt, dass das unternehmerische Risikomanagement weit über das Versicherungswesen oder das Finanzcontrolling hinaus geht und besonders ausgebildete Risikomanager erfordert.

Der operative Ansatz des Risikomanagements

Auf Grund der unternehmerischen und möglicherweise auch regulatorischen Vorgaben muss das Risikomanagement auf allen Ebenen und Funktionen integriert und umgesetzt werden. Dazu dient der operative Ansatz des Risikomanagements mit dem Risikomanagementprozess. Dieser Prozess wurde bereits in verschiedenen sektorspezifischen Normen umschrieben und die Anforderungen zu seiner Durchführung formuliert. Der grundsätzliche Ablauf des Risikomanagementprozesses ist in der Figur 2 dargestellt.



Figur 2: Der Risikomanagementprozess der im Rahmen des unternehmerischen Risikomanagement auf allen Ebenen und Funktionen durchgeführt werden muss. Die Schritte "Risiken identifizieren", "Risiken analysieren" und "Risiken bewerten" werden als "Risikoanalyse" (Risk assessment) bezeichnet. Die Ziffern bezeichnen die Normabschnitte in ISO/CD 31000.

Die Implementierung des Risikomanagementprozesses und die Durchführung der Risikoanalyse erfordern immer eine sorgfältige Definition des Kontextes, das heisst des Rahmens oder des Geltungsbereichs sowie der Zielsetzung einer Risikoanalyse. Es ist auch nicht möglich und auch nicht notwendig, alle Risiken zu analysieren, sondern das Risikomanagement muss sich an der Relevanz oder Wesentlichkeit der Risiken orientieren. Die Risikoidentifikation erfolgt daher am sinnvollsten auf Grund von Gefahrenlisten. Gefahrenlisten oder Checklisten finden sich heute bereits in vielen Normen oder beispielsweise im Arzneimittel- oder Gesundheitsbereich in Richtlinien. Hinweise auf kritische Risikoaspekte können aber auch aus den Unternehmens- oder Finanzkennzahlen abgeleitet werden. Es lohnt sich, eigentliche Gefahrenlisten im Sinne einer Erfahrungs- und Wissensbasis im Unternehmen aufzubauen. Es ist gerade das Risikomanagement, wo das Wissensmanagement eine wertvolle Unterstützung sein kann.

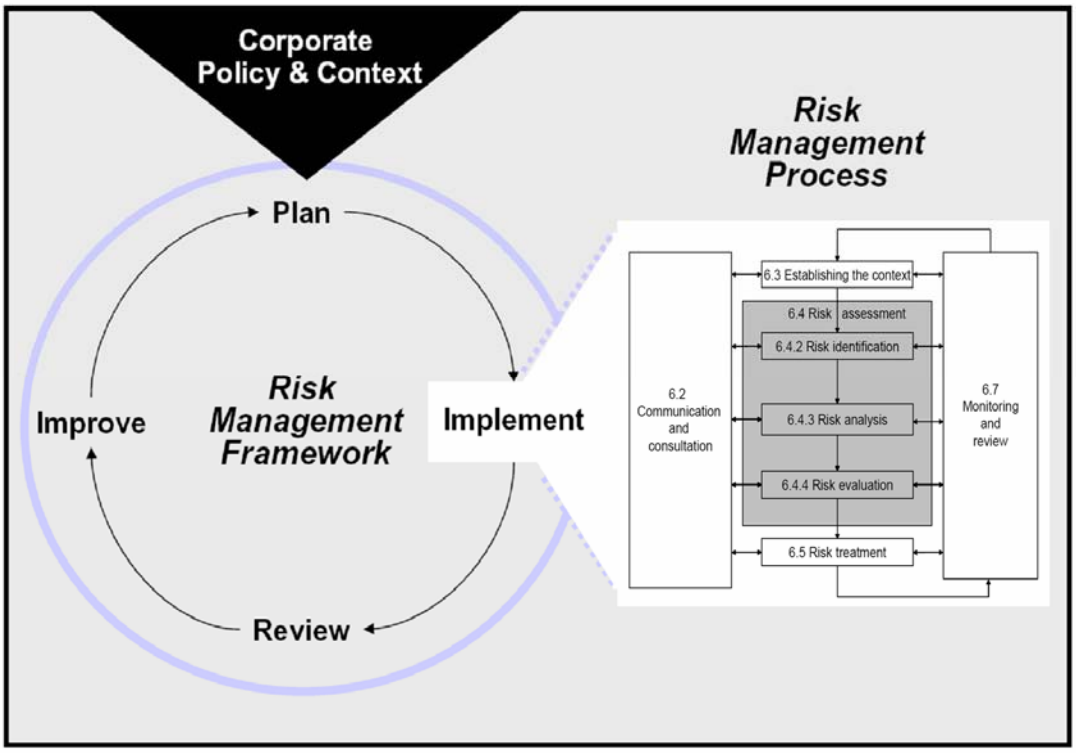
Identifizierte Risiken werden in der Regel in Form von Szenarien nach ihrem Ausmass und ihrer Wahrscheinlichkeit oder Häufigkeit analysiert. Der wichtigste Schritt ist aber die Bewertung. Dazu müssen Kriterienkataloge für das Ausmass, beispielsweise von unbedeutend bis kritisch, und die Wahrscheinlichkeit, beispielsweise von häufig bis unwahrscheinlich, vorhanden sein. Diese Kriterienkataloge orientieren sich an den unternehmerischen Vorgaben wie der Risikopolitik oder an ethischen und regulatorischen Vorgaben. Die Praxis zeigt, dass die Analysenteams jeweils einen grossen Kalibrierungsbedarf haben, damit die Bewertungen kongruent ausfallen. In jedem Fall geht es aber darum, die Grundlage für den unternehmerischen Entscheid zu schaffen, ob ein Risiko tragbar oder nicht akzeptierbar ist.

Die zukünftige Norm ISO 31000:2009

Die Normenentwürfe zur geplanten Norm ISO 31000 liegen bereits in einer ausgereiften Form vor. Es ist geplant, diese nach der endgültigen Bereinigung rund Anfang 2009 zu publizieren. Der vorliegende Normenentwurf gliedert sich in vier wesentliche Teile:

- Begriffe und Definitionen
- Prinzipen und Grundsätze des Risikomanagements
- Das Risikomanagement-Framework
- Der Risikomanagementprozess

Die Begriffe und Definitionen stützen sich auf den ebenfalls in Überarbeitung begriffenen ISO Guide 73 ab. ISO 31000 ist eine generische Norm und regelt nur die Grundsätze und die generellen Anforderungen an den Risikomanagementprozess. Die Anleitungen für die Umsetzung und Implementierung sowie die Anwendung verschiedener Risikoanalysenmethoden ist den sektorspezifischen Normen, beispielsweise für Medizinprodukte, Sicherheit etc. vorbehalten. ISO 31000 wird daher nur durch eine Bibliography mit den Verweisen auf diese sektorspezifischen Normen ergänzt.



Figur 3: Zusammenhang des systemischen Ansatzes mit der unternehmerischen Entscheidungsfindung und dem Risikomanagementprozess, wie er in der Norm ISO 31000 umschrieben wird.

Es versteht sich von selbst, dass die Umsetzung und die Implementierung des Risikomanagements in den Unternehmen und Organisationen sehr spezifisch ausfallen muss. Mit den Anstrengungen zur Harmonisierung des Risikomanagements, der Begriffe und der Prozesse fallen die gesetzgeberischen Anforderungen in der Schweiz zusammen: Ab einer bestimmten Unternehmensgrösse fordert neu revOR Art. 663b[12] den Nachweis eines Risikomanagements. Nachdem die ISO 31000 einen hohen Reifegrad erreicht hat und die regulatorischen Anforderungen verschärft werden, erscheint der Zeitpunkt gekommen, dass die Norm und deren Grundsätze einer breiteren Öffentlichkeit vorgestellt wird. Die Schweizerische Normen-Vereinigung (SNV) führt daher in Zusammenarbeit mit dem Normen-Komitee Risikomanagement ein Seminar durch, indem Exponenten des Risikomanagements aus der Wirtschaft und Industrie sowie öffentlichen Organisationen ihre Sichtweise und Vorgehensweisen erläutern. Das Seminar ist so aufgebaut, dass die Teilnehmer möglichst interaktiv mit den Experten einen Erfahrungs- und Gedankenaustausch führen können.

Seminar zum Thema:
Was ist Risikomanagement und wie funktioniert es?
Die heutigen Anforderungen und der Standard von morgen
Dienstag, 22. November 2007, Olten
Veranstalter: SNV Schweizerische Normen-Vereinigung, Bürglistrasse 29, CH-8400 Winterthur,
Tel. +41 (0)52 224 54 06, www.snv.ch/seminare