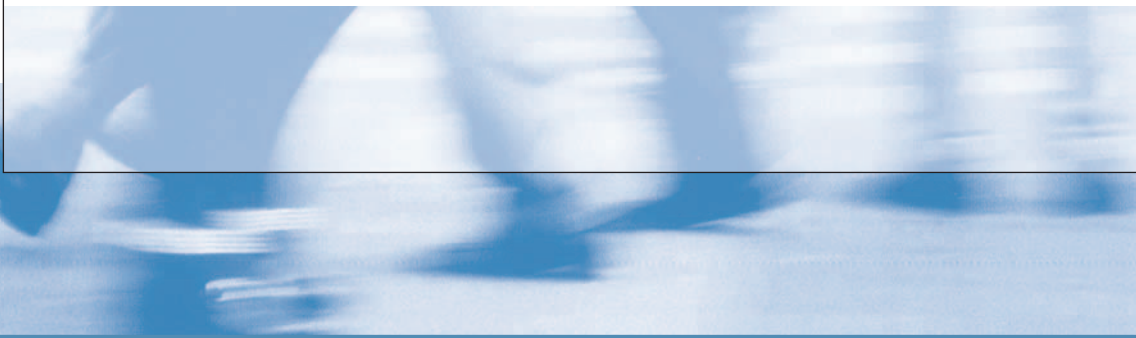




FEDERATION OF  
EUROPEAN RISK  
MANAGEMENT  
ASSOCIATIONS

# DER RISIKOMANAGEMENT-STANDARD





## Einführung

Der Risikomanagement-Standard wurde von einem Team aus den größten Organisationen für Risikomanagement im Vereinigten Königreich - dem Institut für Risikomanagement (IRM), dem Verband der Versicherungs- und Risikomanager (AIRMIC) und ALARM Nationales Forum für Risikomanagement im Öffentlichen Dienst - erstellt.

Darüber hinaus holte das Team während eines umfassenden Konsultationszeitraums die Meinungen und Ansichten einer breiten Palette anderer Berufsverbände, die sich mit Risikomanagement auseinandersetzen, ein.

Risikomanagement ist eine schnell wachsende Disziplin mit zahlreichen und unterschiedlichen Auffassungen und Beschreibungen hinsichtlich Bedeutung, empfohlener Durchführung und Zielsetzung von Risikomanagement. Nötig ist ein gewisser Standard, um Übereinstimmung zu folgenden Punkten zu gewährleisten:

- *Terminologie bezüglich der verwendeten Begriffe*
- *Prozess zur Durchführung des Risikomanagements*
- *Organisationsstruktur für das Risikomanagement*
- *Zielsetzung des Risikomanagements*

Dabei ist wesentlich, dass der Standard das Upside- und Downsidepotential (positive und negative Auswirkungen) von Risiko anerkennt.

Risikomanagement betrifft nicht nur Unternehmen und den öffentlichen Dienst, sondern alle Tätigkeiten, ob kurz- oder langfristig. Nutzen und Möglichkeiten sollten nicht nur im Rahmen der Tätigkeit selbst, sondern in Bezug auf die zahlreichen und unterschiedlichen, möglicherweise betroffenen Stakeholder eingeschätzt werden.

Da sehr viele Wege zur Verwirklichung des Ziels Risikomanagement führen, können diese nicht alle in einem einzigen Dokument dargestellt werden. Daher war man nie um die Ausarbeitung einer Vorschriftsnorm, deren Ergebnis im Abhaken von Kästchen bestehen würde, oder um die Erstellung eines sicher feststellbaren Prozesses bemüht. Wenn die Organisationen die verschiedenen Bestandteile dieser Norm, wenn auch auf unterschiedliche Art, erfüllen, können sie einen Zustand von Compliance signalisieren. Der Standard stellt die beste Praxis dar, an der sich die Organisationen messen können.

Soweit wie möglich hielt sich der Standard an die von der Internationalen Normenorganisation (ISO) in ihrem kürzlich ausgearbeiteten Dokument ISO/IEC Guide 73 Risiko Management - Vokabular - Richtlinien zur Verwendung bei Normen - festgelegte Risikoterminologie.

Angesichts der rasanten Entwicklungen in diesem Bereich bitten die Autoren bei der Verwendung der Norm um Rückmeldungen von den Organisationen (die Anschriften befinden sich auf der Rückseite des Leitfadens). Regelmäßige Abänderungen der Norm im Lichte der besten Praxis sind geplant.



## 1. Risiko

Risiko kann als Kombination der Wahrscheinlichkeit eines Ereignisses und seiner Folgen definiert werden (ISO/IEC Guide 73).

Jede Unternehmung beinhaltet ein Potential an Ereignissen und Folgen, die Gewinnmöglichkeiten (Upside) oder Erfolgsbedrohungen (Downside) darstellen.

Immer mehr beschäftigt sich das Risikomanagement mit den positiven und negativen Risikoaspekten. Daher untersucht diese Norm das Risiko aus beiden Perspektiven.

Im Bereich Sicherheit geht man im allgemeinen davon aus, dass es nur negative Folgen gibt, weshalb die Steuerung des Sicherheitsrisikos Schadensvermeidung und -eindämmung fokussiert.

## 2. Risikomanagement

Risikomanagement ist zentraler Bestandteil der Managementstrategie jedes Unternehmens. Dieser Prozess dient den Organisationen zur methodischen Behandlung von Risiken im Rahmen ihrer unternehmerischen Tätigkeit, mit dem Ziel der Verwirklichung einer anhaltenden Leistung innerhalb jeder Tätigkeit und im gesamten Portfolio aller Tätigkeiten.

Im Brennpunkt eines guten Risikomanagements stehen Identifizierung und Behandlung dieser Risiken. Ziel ist die höchstmögliche dauerhafte Wertschöpfung in allen Tätigkeitsbereichen der Organisation. Es mobilisiert das Verständnis des Upside- und Downsidepotentials aller die Organisation möglicherweise betreffenden Faktoren. Es

erhöht die Erfolgswahrscheinlichkeit und senkt sowohl die Fehlerwahrscheinlichkeit wie auch die Ungewissheit bei der Realisierung der allgemeinen Organisationsziele.

Risikomanagement sollte ein ständiger und sich fortentwickelnder Prozess sein, der die gesamte Organisationsstrategie und die Durchführung dieser Strategie durchläuft. Es sollte alle Risiken im Zusammenhang mit den vergangenen, gegenwärtigen und insbesondere zukünftigen Tätigkeiten der Organisation methodisch in Angriff nehmen.

Es muss durch eine wirksame Politik und mittels eines auf höchster Managementebene geführten Programms in die Unternehmenskultur eingebettet werden. Es muss die Strategie in taktische und betriebliche Zielsetzungen umsetzen, wobei im gesamten Unternehmen jedem Manager und Mitarbeiter, dessen Arbeitsplatzbeschreibung Risikomanagement umfasst, Verantwortung zugeordnet wird. Es unterstützt Rechenschaftspflicht, Performance-Messung und Belohnung, was zur Rentabilitätsförderung auf allen Ebenen beiträgt.

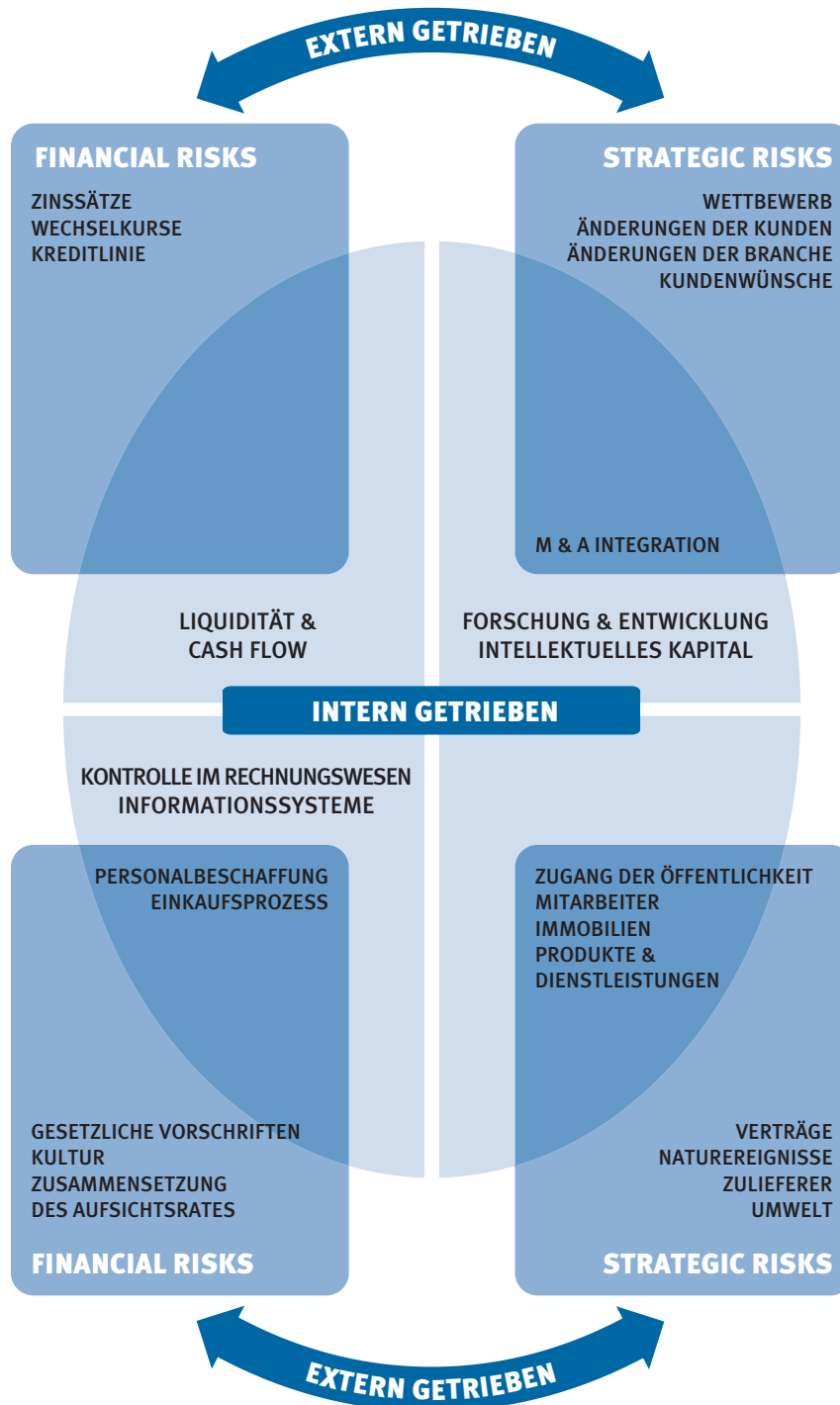
### 2.1 Externe und Interne Faktoren

Die Risiken, denen eine Organisation und ihr Betrieb ausgesetzt sind, können sowohl aus betriebsinternen, wie auch betriebsexternen Faktoren entstehen.

Das umseitige Diagramm resümiert Beispiele von Schlüsselrisiken in diesen Bereichen und zeigt, dass einige spezifische Risiken sowohl externe wie auch interne Treiber aufweisen können und daher auf beide Bereiche übergreifen. Sie können weiter nach Risikoarten wie strategisch, finanziell, betrieblich, Hazard (Unfallgefahr) usw. eingestuft werden.

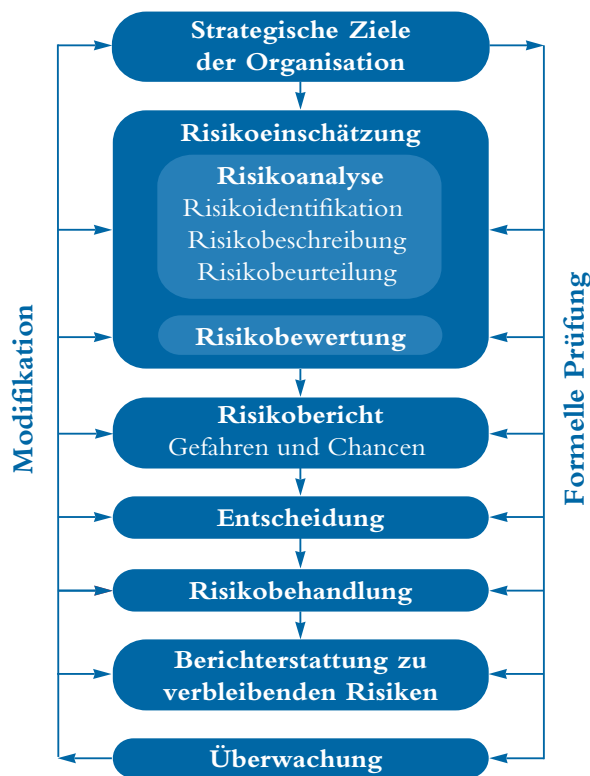


2.1 Beispiele für Treiber von Schlüsselrisiken





## 2.2 Risikomanagement - Verfahren



Risikomanagement bedeutet Schutz und Wertzuwachs für die Organisation und ihre Stakeholder, indem es die Zielsetzungen der Organisation folgendermaßen fördert:

- *Aufstellung eines Rahmens für eine Organisation, mittels der zukünftige Aktivitäten konsequent und geregelt ablaufen*
- *verbesserte Entscheidungsfassung, Planung und Prioritätenfestlegung durch ein umfassendes und strukturiertes Verständnis hinsichtlich Geschäftsablauf, Volatilität und Projektchance/Bedrohung*
- *Förderung einer effizienteren Verwendung/Zuteilung von Kapital und Ressourcen innerhalb der Organisation*
- *Volatilitätssenkung in nicht wesentlichen Geschäftsbereichen*
- *Schutz und Steigerung der Aktiva und des Unternehmensimage*
- *Entwicklung und Unterstützung der Menschen und der betrieblichen Wissensgrundlage*
- *Rentabilitätsoptimierung*



### 3. Risikoeinschätzung

ISO/IEC Guide 73 definiert Risikoschätzung als das gesamte Verfahren von Risikoanalyse und Risikobewertung.  
(Siehe Anlage)

### 4. Risikoanalyse

#### 4.1 Risikoidentifikation

Durch Risikoidentifizierung soll die Belastung einer Organisation durch Ungewissheit identifiziert werden. Voraussetzung dafür ist eine genaue Kenntnis der Organisation, des Marktes, in dem sie tätig ist, des rechtlichen, sozialen, politischen und kulturellen Umfeldes, in dem sie besteht, wie auch die Entwicklung eines soliden Verständnisses ihrer strategischen und operativen Zielsetzungen, einschließlich der für ihren Erfolg maßgeblichen Faktoren und der Bedrohungen und Möglichkeiten in Zusammenhang mit der Erreichung dieser Zielsetzungen.

Risikoidentifizierung sollte methodisch erfolgen, um sicher zu gehen, dass alle bedeutsamen Tätigkeiten innerhalb der Organisation identifiziert und alle aus diesen Tätigkeiten entstehenden Risiken definiert wurden. Jede in Zusammenhang mit diesen Tätigkeiten anfallende Volatilität sollte identifiziert und kategorisiert werden.

**Unternehmerische Tätigkeiten und Entscheidungen können auf verschiedene Weise eingeordnet werden, beispielsweise wie folgt:**

- *Strategisch - Diese betreffen die langfristigen strategischen Ziele der Organisation. Sie können durch solche Bereiche wie Kapitalverfügbarkeit, souveräne und politische Risiken, rechtliche und vorschriftsmäßige Veränderungen, guter Ruf und Veränderungen in der physischen Umgebung berührt werden.*
- *Operativ - Diese betreffen laufende Fragen, mit denen sich die Organisation bei ihrem Streben nach Erreichung der strategischen Ziele konfrontiert sieht.*

- *Finanziell - Diese betreffen wirksames Management und Kontrolle der Organisationsfinanzen und die Auswirkungen externer Faktoren wie Kreditverfügbarkeit, Devisenkurse, Zinskursschwankungen und andere Marktbelastungen.*
- *Wissensmanagement - Diese betreffen wirksames Management und Kontrolle der Wissensressourcen, wie auch deren Produktion, Schutz und Kommunikation. Zu externen Faktoren gehören möglicherweise die unerlaubte Verwendung oder der Missbrauch geistigen Eigentums, örtlicher Stromausfall und Wettbewerbstechnologie. Interne Faktoren sind vielleicht Systemstörungen oder Verlust wichtiger Mitarbeiter.*
- *Compliance - Diese betreffen Bereiche wie Gesundheit & Sicherheit, Umwelt, Handelsbezeichnungen, Verbraucherschutz, Datenschutz, Beschäftigungspraktiken und Vorschriftenfragen.*

Während die Risikoidentifizierung durch externe Berater erfolgen kann, ist ein betriebsinternes Vorgehen mit gut verständlichen, konsequenten und koordinierten Prozessen und Werkzeugen (vgl. Anlage Seite 14) wahrscheinlich wirksamer. Wesentlich ist der betriebsinterne 'Besitz' des Risikomanagementverfahrens.

#### 4.2 Risikobeschreibung

Ziel der Risikobeschreibung ist die Anzeige der identifizierten Risiken in einem strukturierten Format, beispielsweise durch Verwendung einer Tabelle. Die umseitige Tabelle zur Risikobeschreibung kann zur einfacheren Beschreibung und Schätzung von Risiken dienen. Der Einsatz einer gut durchdachten Struktur ist zur Gewährleistung eines umfassenden Verfahrens für Risikoidentifizierung, -beschreibung und -schätzung erforderlich. Durch Erwägung der Folgen und Wahrscheinlichkeit jedes in der Tabelle dargestellten Risikos sollte es möglich sein, den Stellenwert der Schlüsselrisiken, die eine genauere Analyse erfordern, zu ermitteln. Die Identifizierung der mit der unternehmerischen Tätigkeit und



Entscheidungsfassung verbundenen Risiken kann als strategisch, Projekt-/taktisch, operativ kategorisiert werden. Wichtig ist die Eingliederung des

Risikomanagements in die Projektplanungsphase wie auch in die gesamte Lebenszeit eines spezifischen Projekts.

#### 4.2.1 Tabelle - Risikobeschreibung

1. Name des Risikos	
2. Tragweite des Risikos	Qualitative Beschreibung der Ereignisse, ihres Umfangs, ihrer Art, Anzahl und Abhängigkeiten
3. Beschaffenheit des Risikos	Bsp. strategisch, operativ, finanziell, Wissen oder Compliance
4. Stakeholder	Stakeholder und deren Erwartungen
5. Quantifizierung des Risikos	Signifikanz und Wahrscheinlichkeit
6. Risikotoleranz/Appetit	Verlustpotential und finanzieller Durchdringungsgrad des Risikos Riskierter Wert Wahrscheinlichkeit und Umfang potentieller Verluste/Gewinne Ziel(e) zur Risikokontrolle und erwünschtes Leistungsniveau
7. Risikobehandlungs- & Kontrollmechanismen	Primäre Mittel zur gegenwärtigen Risikosteuerung Vertrauensgrad in die bestehende Kontrolle Identifizierung von Überwachungs- und Revisionsprotokollen
8. Potentielle Verbesserungsaktion	Empfehlungen zur Risikoreduzierung
9. Strategische und politische Entwicklungen	Identifizierung der für strategische und politische Entwicklung zuständigen Funktion.

#### 4.3 Risikobeurteilung

Die Risikobeurteilung kann hinsichtlich der Wahrscheinlichkeit des Eintretens und der möglichen Folgen quantitativ, halbquantitativ oder qualitativ sein.

Beispielsweise können die Folgen sowohl hinsichtlich der Gefahren (Downside-Risiken) und Möglichkeiten (Upside-Risiken) hoch, mittel oder niedrig sein (vgl. Tabelle 4.3.1). Die Wahrscheinlichkeit kann hoch, mittel oder niedrig liegen, erfordert allerdings andere Definitionen bezüglich Gefahren und Möglichkeiten (vgl. Tabellen 4.3.2 und 4.3.3).

Umseitig finden Sie Tabellen mit Beispielen. Verschiedene Organisationen werden feststellen, dass verschiedene Maßstäbe für Folgen und Wahrscheinlichkeit ihren Bedürfnissen am besten entsprechen.

Viele Organisationen stellen beispielsweise fest, dass die Schätzung von Folgen und Wahrscheinlichkeit nach hoch, mittel oder niedrig ihren Bedürfnissen durchaus entspricht und als 3 x 3 Matrize dargestellt werden kann.

Andere Organisationen sind der Meinung, dass ihnen die Schätzung von Folgen und Wahrscheinlichkeit mittels einer 5 x 5 Matrize eine bessere Bewertung ermöglicht.

**Tabelle 4.3.1 Folgen - Sowohl Gefahren wie auch Möglichkeiten**

Hoch	Finanzielle Auswirkungen auf die Organisation wahrscheinlich über €x Bedeutsame Auswirkungen auf die Strategie oder operativen Tätigkeiten der Organisation Bedeutsames Interesse der Stakeholder
Mittel	Finanzielle Auswirkungen auf die Organisation wahrscheinlich zwischen €x und €y Mäßige Auswirkungen auf die Strategie oder operativen Tätigkeiten der Organisation Mäßiges Interesse der Stakeholder
Niedrig	Finanzielle Auswirkungen auf die Organisation wahrscheinlich unter €y Niedrige Auswirkungen auf die Strategie oder operativen Tätigkeiten der Organisation Niedriges Interesse der Stakeholder

**Tabelle 4.3.2 Wahrscheinlichkeit des Eintretens - Gefahren**

Schätzung	Beschreibung	Indikatoren
Hoch (Wahrscheinlich)	Tritt wahrscheinlich jedes Jahr ein oder Eintrittschance über 25%.	Potential für mehrfaches Eintreten innerhalb des Zeitraums (zum Beispiel - zehn Jahre). Kürzlich eingetreten.
Mittel (Möglich)	Tritt wahrscheinlich in einem Zeitraum von zehn Jahren ein oder Eintrittschance unter 25%.	Könnte mehr als einmal innerhalb des Zeitraums (zum Beispiel - zehn Jahre) eintreten. Möglicherweise aufgrund einiger externer Einflussfaktoren schwer zu bewältigen. Gibt es eine Vorgeschichte für das Eintreten?
Niedrig (Unwahrscheinlich)	Tritt wahrscheinlich nicht in einem Zeitraum von zehn Jahren ein oder Eintrittschance unter 2%.	Nicht eingetreten. Eintreten unwahrscheinlich.



**Tabelle 4.3.3 Wahrscheinlichkeit des Eintretens - Möglichkeiten**

Schätzung	Beschreibung	Indikatoren
Hoch (Wahrscheinlich)	Günstiges Ergebnis wird wahrscheinlich in einem Jahr erzielt oder Eintrittschance über 75%.	Eindeutige Möglichkeit, die mit begründeter Gewissheit auf Grundlage laufender Management-verfahren kurzfristig erreichbar ist.
Mittel (Möglich)	Begründete Aussichten auf günstige Ergebnisse in einem Jahr oder Eintrittschance zwischen 25% und 75%.	Vielleicht erreichbare Möglichkeiten, die allerdings umsichtiges Management erfordern. Möglichkeiten, die sich über den Plan hinaus ergeben können.
Niedrig (Unwahrscheinlich)	Mittelfristig gewisse Aussichten auf ein günstiges Ergebnis oder Eintrittschance unter 25%.	Denkbare Möglichkeit, die vom Management noch voll erforscht werden muss. Möglichkeit mit geringer Erfolgswahrscheinlichkeit ausgehend von gegenwärtig eingesetzten Managementressourcen.

#### 4.4 Risikoanalyseverfahren und -techniken

Zur Risikoanalyse stehen eine Reihe von Techniken zur Verfügung. Diese sind manchmal spezifisch für Upside- oder Downsiderisiken geeignet, manchmal auch für beide. *(Beispiele).*

#### 4.5 Risikoprofil

Mit dem Ergebnis des Risikoanalyseverfahrens kann ein Risikoprofil erstellt werden, das jedem Risiko einen Bedeutsamkeitsgrad zuweist und ein Werkzeug zur Schwerpunktsetzung bei den Bemühungen zur Risikobehandlung liefert. Jedes identifizierte Risiko wird hierarchisch

eingestuft, wodurch die relative Bedeutung hervortritt.

Dieses Verfahrens sorgt für die Eintragung des Risikos auf der Karte des betroffenen Geschäftsbereichs, beschreibt die bestehenden primären Kontrollverfahren und gibt an, wo das Niveau der Risikokontrollinvestition erhöht, verringert oder neu zugeteilt werden könnte.

Die Rechenschaftspflicht sorgt für Anerkennung des Risiko'besitzes' und Zuweisung der angemessenen Managementressource.



## 5. Risikobewertung

Nach Abschluss des Risikoanalyseverfahrens sind die beurteilten Risiken mit den von der Organisation ausgearbeiteten Risikokriterien zu vergleichen. Zu den Risikokriterien gehören möglicherweise anfallende Kosten und Leistungen, rechtliche Auflagen, sozioökonomische und umweltmäßige Faktoren, Anliegen der Stakeholder usw. Daher dient die Risikobewertung zur Entscheidung über Risikosignifikanz für die Organisation und Akzeptanz oder Behandlung jedes spezifischen Risikos.

## 6. Risikobehandlung

Risikobehandlung ist der Prozess der Auswahl und Durchführung von Maßnahmen zur Risikoveränderung. Zu den Hauptelementen der Risikobehandlung gehören Risikokontrolle/-eindämmung, wobei aber beispielsweise Risikovermeidung, Risikotransfer, Risikofinanzierung usw. ebenfalls umfasst sind.

**ANMERKUNG:** *In dieser Norm bezieht sich Risikofinanzierung auf die Mechanismen (z.B. Versicherungsprogramme) zur Deckung der finanziellen Folgen des Risikos. Im allgemeinen versteht man unter Risikofinanzierung nicht die Bereitstellung von Mitteln zur Deckung der Durchführungskosten einer Risikobehandlung (gemäß ISO/IEC Guide 73; vgl. Seite 17).*

Jedes Risikobehandlungssystem sollte mindestens Folgendes enthalten:

- wirksame und leistungsfähige Arbeitsweise der Organisation
- wirksame interne Kontrollen
- Einhalten von Gesetzen und Vorschriften

Das Risikoanalyseverfahren unterstützt die wirksame und leistungsfähige Arbeitsweise der Organisation durch Identifikation derjenigen Risiken, mit denen sich das Management beschäftigen sollte. Erforderlich ist dabei die

Schwerpunktsetzung bei der Auswahl von Risikokontrollaktionen je nach ihrem potentiellen Nutzen für die Organisation.

Wirksamkeit der internen Kontrolle ist der Grad, um den das Risiko durch die geplanten Kontrollmaßnahmen entweder ausgeräumt oder verringert wird.

Die Kostenrentabilität der internen Kontrolle bezieht sich auf die Kontrolldurchführungskosten im Vergleich zum erwarteten Risikosenkungsnutzen.

Die geplanten Kontrollen sollten an ihren potentiellen wirtschaftlichen Auswirkungen, falls keine Aktion erfolgt, im Vergleich zu den Kosten der geplanten Aktion(en) gemessen werden, was ausnahmslos genauere Informationen und Annahmen erfordert, als sofort verfügbar sind.

Zuerst gilt es, die Durchführungskosten festzulegen. Diese müssen ziemlich genau berechnet werden, da sie schnell die Grundlage zum Messen der Kostenrentabilität abgeben. Auch ist der erwartete Verlust bei Unterlassen der Aktion abzuschätzen, wobei das Management die Ergebnisse vergleichen und eine Entscheidung bezüglich Durchführung oder Nichtdurchführung der Risikokontrollmaßnahmen treffen kann.

Die Einhaltung von Gesetzen und Vorschriften ist zwingend. Eine Organisation muss die geltenden Gesetze kennen und ein Kontrollsystem zur Gewährleistung von Compliance einsetzen. Nur gelegentlich zeigt sich eine gewisse Flexibilität, wenn die Kosten für eine Risikoreduzierung in keinem Verhältnis zu diesem Risiko stehen.

Eine Methode zum Aufbau von finanziellem Schutz gegen Risikoauswirkungen besteht in der Risikofinanzierung, einschließlich Versicherung. Dabei ist allerdings einzuräumen, dass gewisse Verluste oder Verlustelemente nicht versicherungsfähig sind, z.B. die nicht versicherten Kosten in Verbindung mit Gesundheit am Arbeitsplatz, Sicherheit oder Umweltereignissen, die auch das Arbeitsklima und den guten Ruf der Organisation beeinträchtigen können.



## 7. Risikoberichterstattung

### 7.1 Interne Berichterstattung

Die verschiedenen Organisationsniveaus benötigen unterschiedliche Informationen aus dem Risikomanagementverfahren.

#### Der Vorstand sollte:

- die bedeutsamsten Risiken für die Organisation kennen
- die möglichen Auswirkungen von Abweichungen bei den erwarteten Leistungsspannen auf den Aktionärswert kennen
- für angemessene Sensibilisierung in der gesamten Organisation sorgen
- wissen, wie die Organisation eine Krise bewältigen wird
- wissen, wie wichtig das Vertrauen der Akteure/Shareholder in die Organisation ist
- falls erforderlich wissen, wie die Kommunikation mit der Investitionsgemeinschaft zu gestalten ist
- überzeugt sein, dass der Risikomanagementprozess wirksam funktioniert
- eine klare Risikomanagementpolitik einschließlich Philosophie und Verantwortungen im Bereich Risikomanagement veröffentlichen

#### Die Unternehmenseinheiten sollten:

- sich der in ihren Verantwortungsbereich fallenden Risiken, ihrer etwaigen Auswirkungen auf andere Bereiche und der möglichen Auswirkungen anderer Bereiche auf sich selbst bewusst sein
- über Leistungsindikatoren verfügen, mit Hilfe derer sie die wichtigsten geschäftlichen und finanziellen Tätigkeiten überwachen, die Zielverwirklichung verfolgen und Entwicklungen identifizieren können, die ein Eingreifen erfordern (z. B. Prognosen und Haushalte).

- Systeme haben, die prognostische und budgetäre Abweichungen mit angemessener Häufigkeit melden, um ein Eingreifen zu ermöglichen.
- die oberste Unternehmensleitung systematisch und umgehend über alle wahrgenommenen neuen Risiken oder Fehler der bestehenden Kontrollmaßnahmen unterrichten

#### Einzelpersonen sollten:

- ihre Rechenschaftspflicht für Einzelrisiken kennen
- verstehen, wie sie zu einer ständigen Verbesserung des Risikomanagementverhaltens beitragen können
- wissen, dass Risikomanagement und Risikosensibilisierung Kernstück der Organisationskultur sind
- die oberste Unternehmensleitung systematisch und umgehend über alle wahrgenommenen neuen Risiken oder Fehler der bestehenden Kontrollmaßnahmen unterrichten

### 7.2 Externe Berichterstattung

Ein Unternehmen muss seinen Stakeholdern regelmäßig über die Risikomanagementpolitik und die Wirksamkeit bei der Erreichung seiner Zielsetzungen Bericht erstatten.

Die Stakeholder erwarten von den Organisationen in steigendem Maße einen Nachweis für wirksames Management der nichtfinanziellen Organisationsleistungen, und zwar in Bereichen wie Gemeinschaftsangelegenheiten, Menschenrechte, Beschäftigungspraxis, Gesundheit und Sicherheit und Umwelt.

**Gute Corporate Governance setzt voraus, dass die Unternehmen ein methodisches Verfahren im Bereich Risikomanagement einsetzen, welches:**



- *die Interessen ihrer Stakeholder schützt*
- *gewährleistet, dass der Vorstand seinen Aufgaben der Strategieleitung,, Wertschöpfung und Überwachung der Organisationsleistung erfüllt*
- *gewährleistet, dass Managementkontrollen bestehen und angemessen funktionieren*

Die Verfügungen hinsichtlich der formellen Berichterstattung des Risikomanagements sollten klar formuliert und den Stakeholdern zugänglich sein.

#### **Die formelle Berichterstattung sollte folgende Bereiche erfassen:**

- *Kontrollmethoden - insbesondere Zuständigkeiten des Managements für Risikomanagement*
- *Verfahren zur Risikoidentifikation und wie diese von den Risikomanagementsystemen gehandhabt werden*
- *bestehende primäre Kontrollsysteme zur Bewältigung von bedeutsamen Risiken.*
- *bestehendes Überwachungs- und Revisionssystem*

Alle vom System oder im System selbst ermittelten bedeutsamen Mängel sollten, zusammen mit den ergriffenen Abhilfemaßnahmen, gemeldet werden.

## **8. Struktur und Verwaltung von Risikomanagement.**

### **8.1 Risikomanagementpolitik**

Die Risikomanagementpolitik einer Organisation sollte den Risikoansatz, den Risikoappetit und das Vorgehen im Bereich Risikomanagement darlegen. Auch sollte die Politik die Verantwortungen für Risikomanagement organisationsweit abstecken.

Darüber hinaus sollte sie auf alle rechtlichen Auflagen für politische Erklärungen, z. B. Gesundheit und Sicherheit, Bezug nehmen.

Dem Risikomanagementprozess ist ein integriertes Paket von Werkzeugen und Techniken zur Verwendung in den verschiedenen Geschäftsablaufphasen angeschlossen.

#### **Zur wirksamen Arbeitsweise setzt der Risikomanagementprozess Folgendes voraus:**

- *Zusage des Aufsichtsratsvorsitzenden und der Organisationsleitung*
- *Verantwortungszuordnung innerhalb der Organisation*
- *Bereitstellung angemessener Ressourcen zur Ausbildung und Entwicklung einer gesteigerten Risikosensibilisierung seitens aller Stakeholder*

### **8.2 Rolle des Vorstands**

Der Vorstand trägt die Verantwortung für die Festlegung der strategischen Richtung der Organisation und für die Schaffung eines Umfeldes und von Strukturen, die eine wirksame Arbeitsweise des Risikomanagements ermöglichen.

Dies kann durch eine Gruppe von Führungskräften, einen nichtleitenden Ausschuss, ein Gremium von Rechnungsprüfern oder irgendeine andere Funktion geschehen, die der Betriebsweise der Organisation angepasst ist und als 'Sponsor' für Risikomanagement auftreten kann.

#### **Bei der Bewertung seines internen Kontrollsystems sollte der Vorstand mindestens erwägen:**

- *Beschaffenheit und Umfang der Downside-Risiken, die für das Unternehmen innerhalb ihrer bestimmten geschäftlichen Tätigkeit tragbar sind*
- *die Wahrscheinlichkeit, dass solche Risiken Realität werden*



- *Behandlung nicht akzeptabler Risiken*
- *Fähigkeit des Unternehmens, die Wahrscheinlichkeit und die Auswirkungen auf den Betrieb möglichst gering zu halten.*
- *Kosten und Nutzen des Risikos und der erfolgten Kontrollmaßnahme*
- *Wirksamkeit des Risikomanagementprozesses*
- *Risikoimplikationen von Vorstandsentscheidungen*

### **8.3 Rolle der Unternehmenseinheiten**

Diese beinhaltet Folgendes:

- *den Unternehmenseinheiten kommt die primäre Verantwortung für das laufende Risikomanagement zu*
- *das Management der Unternehmenseinheiten ist für die Förderung der Risikosensibilisierung innerhalb ihrer geschäftlichen Tätigkeiten verantwortlich; sie sollten Risikomanagementziele in ihre Tätigkeit aufnehmen*
- *Risikomanagement sollte regelmäßig bei Managementsitzungen zur Sprache kommen, um die Gesamtrisikoposition zu untersuchen und den Arbeiten im Lichte einer wirksamen Risikoanalyse neue Schwerpunkte zu setzen*
- *das Management der Unternehmenseinheiten sollte gewährleisten, dass Risikomanagement in die Projektplanungsphase wie auch in das gesamte Projekt eingegliedert wird*

### **8.4 Rolle der Funktion Risikomanagement**

Je nach Organisationsgröße kann die Funktion Risikomanagement von einem einzigen "Risiko Champion" bis zu einem Teilzeitriskomanager oder einer ganzen Risikomanagementabteilung reichen. Die Rolle der Funktion.

Risikomanagement sollte Folgendes beinhalten:

- *Festlegung von Politik und Strategie für Risikomanagement*
- *Hauptverfechter von Risikomanagement auf strategischer und operativer Ebene*
- *Aufbau einer risikosensiblen Kultur innerhalb der Organisation einschließlich angemessener Aufklärung*
- *Aufstellung einer internen Risikopolitik und von Strukturen für die Unternehmenseinheiten*
- *Entwurf und Revision von Risikomanagementprozessen*
- *Koordinierung der verschiedenen dienstlichen Tätigkeiten, die innerhalb der Organisation zu Risikomanagementfragen Rat geben*
- *Entwicklung von Risikoreaktionsprozessen, einschließlich Programme für unvorhergesehene Ereignisse und Unternehmenskontinuität*
- *Ausarbeitung von Risikoberichten für Vorstand und Stakeholder*

### **8.5 Rolle der Innenrevision**

Die Rolle der Innenrevision gestaltet sich wahrscheinlich in jeder Organisation anders.

In der Praxis nimmt die Innenrevision wohl einige der oder alle der folgenden Aufgaben wahr:

- *Fokussierung der Innenrevisionsarbeit auf die vom Management identifizierten bedeutsamen Risiken und Rechnungsprüfung der Risikomanagementprozesse in der gesamten Organisation*
- *Gewissheit bezüglich Risikomanagement bieten*



- *Bereitstellung aktiver Unterstützung und Mitarbeit im Risikomanagementprozess*
- *Erleichterung von Risikoidentifizierung/-schätzung und Unterrichtung des Linienpersonals im Bereich Risikomanagement und interne Kontrolle*
- *Koordinierung der Risikoberichterstattung an den Vorstand, das Gremium der Rechnungsprüfer usw.*

Bei der Festlegung der geeignetsten Rolle für eine bestimmte Organisation sollte die Innenrevision die Einhaltung der beruflich erforderlichen Unabhängigkeit und Objektivität gewährleisten.

### 8.6 Ressourcen und Durchführung

Die zur Durchführung der Risikomanagementpolitik der Organisation erforderlichen Ressourcen sollten auf jedem Managementniveau und innerhalb jeder Unternehmenseinheit eindeutig festgelegt werden.

Die Aufgaben der im Bereich Risikomanagement tätigen Personen bei der Koordinierung der Risikomanagementpolitik/-strategie sollten neben ihren etwaigen anderen operativen Funktionen klar definiert sein. Dieselbe klare Definition ist auch für diejenigen erforderlich, die im Bereich Rechnungsprüfung und Revision interner Kontrollen oder in der Förderung des Risikomanagementprozesses tätig sind.

Risikomanagement sollte mittels der Strategie- und Haushaltsprozesse in die Organisation eingebettet sein. Es sollte bei der Induktion und in allen anderen Ausbildungs- und Entwicklungsbereichen wie auch innerhalb operativer Prozesse, z.B. Entwicklungsprojekte für Produkt/Dienstleistung, hervorstechen.

## 9. Überwachung und Revision des Risikomanagementprozesses.

Zum wirksamen Risikomanagement gehört eine Berichts- und Revisionsstruktur zur Gewährleistung einer wirksamen Risikoidentifikation und -schätzung und des Bestehens angemessener Kontrollen und Reaktionen. Um Verbesserungsmöglichkeiten zu identifizieren, sollte eine regelmäßige Überprüfung der Einhaltung von Politik und Normen und der Standardleistung erfolgen. Dabei ist nicht zu vergessen, dass Organisationen dynamisch sind und in dynamischen Umfeldern agieren. Veränderungen in der Organisation und ihrem Arbeitsumfeld müssen identifiziert und die Systeme in angemessener Weise abgeändert werden.

Der Überwachungsprozess sollte dafür sorgen, dass für die Tätigkeiten der Organisation geeignete Kontrollen bestehen und dass die Verfahren verstanden und eingehalten werden. Veränderungen in der Organisation und ihrem Arbeitsumfeld müssen identifiziert und die Systeme in angemessener Weise abgeändert werden.

### Jeder Überwachungs- und Revisionsprozess sollte auch ermitteln, ob:

- *die durchgeführten Maßnahmen den angestrebten Zweck erfüllten*
- *die zur Durchführung der Schätzung eingesetzten Prozesse und eingeholten Informationen angemessen waren*
- *bessere Kenntnisse zu besseren Entscheidungen beigetragen hätten und welche Lektionen man für zukünftige Risikoschätzungen und -management ziehen könnte*



## 10. Anlage

### Techniken zur Risikoidentifizierung - Beispiele

- *Brainstorming*
- *Fragebögen*
- *Unternehmensstudien zur Untersuchung jedes Unternehmensprozesses und Beschreibung der internen Prozesse wie auch der externen Faktoren, die einen Einfluss auf diese Prozesse ausüben können*
- *Branchenleistungsvergleich (Benchmarking)*
- *Analyse des Einsatzortes*
- *Workshops zur Risikoschätzung*
- *Vorfallermittlung*
- *Rechnungsprüfung und Inspektion*
- *HAZOP (Hazard & Operability Studies) Gefahren- und Durchführbarkeitsstudien*

### Risikoanalyseverfahren und -techniken - Beispiele

#### Upside risk

- *Markterhebung*
- *Untersuchungen*
- *Vermarktungstest*
- *Forschung und Entwicklung*
- *Unternehmenswirkungsanalyse*

#### Beides

- *Modellierung einer Abhängigkeit*
- *SWOT -Analyse (Stärken, Schwächen, Möglichkeiten, Gefahren)*
- *Ereignisbaumanalyse*
- *Planung für zur Unternehmenskontinuität*
- *BPEST (uUnternehmerische, ppolitische, wWirtschaftliche, ssoziale, tTechnologische) Analyse*
- *Modellierung einer wirklichen Entscheidung*
- *Entscheidungsfassung unter Risiko- und Ungewissheitsbedingungen*
- *Statistische Rückschlüsse*
- *Maßnahmen zentraler Tendenz und Streuung*
- *PESTLE (Politisch, Wirtschaftlich, Sozial, Technisch, Rechtlich, Umweltmäßig)*

#### Downside-Risiko

- *Bedrohungsanalyse*
- *Fehlerbaumanalyse*
- *FMEA (Failure Mode & Effect Analysis) (Analyse von Fehlerarten und den daraus resultierenden Folgen)*



**AGERS** - Asociación Española de Gerencia de Riesgos y Seguros  
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.- 28006 Madrid - SPAIN  
Tel: + 34-91-562.84.25- Fax: + 34-91-561.54.05- Email: gerencia@agers.es



**AIRMIC** - The association of Insurance and Risk Managers  
Lloyd's Avenue, 6 – London EC3N3AX - UK  
Tel: + 44-207-480.76.10 – Fax: + 44-207-702.37.52 – Email: enquiries@airmic.co.uk  
Web: www.airmic.com



**AMRAE** - Association pour le Management des Risques et des Assurances de l'Entreprise  
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE  
Tel: + 33-1-42.89.33.16 – Fax: + 33-1-42.89.33.14 – Email: amrae@amrae.asso.fr  
Web: www.amrae.asso.fr



**ANRA** - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali  
Viale Coni Zugna, 53 – 20144 Milano - ITALY  
Tel: + 39-02-58.10.33.00 – Fax: + 39-02-58.10.32.33 – Email: anra@betam.it – Web: www.anra.it



**APOGERIS** - Associação Portuguesa de Gestão de Riscos e Seguros  
Avenida da Boavista, 1245, 3a Esq. – 4100-130 Porto – Portugal  
Tel. (+351) 22 608 24 62 – Fax (+351) 22 608 24 73 – E-mail: anfernandes@sonae.pt



**BELRIM** - Belgian Risk Management Association  
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM  
Tel: + 32-2-380.03.94 – Fax: + 32-2-370.34.93 – Email: info@belrim.com – Web: www.belrim.com



**bfV** - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften E. V.  
Hattenbergstrasse 10, 55122 Mainz - D  
Tel. + 49 - 6131 – 662226 - Fax. + 49 - 6131 – 662059 - Email. johannes.fischer@schott.com  
Web: www.bfv-fvv.de



**DARIM** - Dansk Industris Risk Management Forening  
DK-1787 Copenhagen – DENMARK  
Tel: + 45-33-77.33.77 – Fax: + 45-33-77.33.00 – Email: bg@di.dk



**DVS** - Deutscher Versicherungs-Schutzverband e.V.  
Breite Strasse 98 - D 53111 Bonn - Germany  
Tel: + 49-228-98.22.30 - Fax: + 49-228-63.16.51- Email: info@dvs-schutzverband.de  
Web: www.dvs-schutzverband.de



**NARIM** - Nederlandse Associatie van Risk en Insurance Managers  
Postbus 65707 – 2506 EA Den Haag – THE NETHERLANDS  
Tel: + 31-70-345.74.26 – Fax: + 31-70-427.32.63 – Email: info@narim.com – Web: www.narim.com



**SIRM** - Swiss Association of Insurance and Risk Managers  
Route du Jura, 37- Case Postale, 74 – 1706 Fribourg - SWITZERLAND  
Tel: + 41-26-347.12.20 – Fax: + 41-26-347.12.39 – Email: sirm@cfcis.ch – Web: www.sirm.ch

**ALARM** - The National Forum for Risk Management in the Public Sector  
Queens Drive, Exmouth - Devon, EX8 2AY  
Tel: 01395 223399 - Fax: 01395 223304 - Email admin@alarm.uk.com - www.alarm-uk.com



**IRM** - The Institute of Risk Management  
6 Lloyd's Avenue - London EC3N 3AX  
Tel: 020 7709 9808 - Facsimile 020 7709 0716 - Email enquiries@theIRM.org - www.theirm.org