

INTOSAI



*Richtlinien für
Normen zur internen
Kontrolle im
öffentlichen Sektor*

*Weitere
Informationen zum
Thema „umfassendes
Risikomanagement“*

INTOSAI GOV 9130

INTOSAI-

*Unterausschuss für
die interne Kontrolle
2007*

INTOSAI Unterausschuss für die interne Kontrolle

F. VANSTAPEL
Erster Vorsitzender des Belgischen Rechnungshofes

Regentschapsstraat 2 – Rue de la Régence 2
B-1000 BRUSSEL
BELGIEN

Tel : + 32 2 551 8111
Fax : + 32 2 551 8629
E-mail : international@ccek.be

*R*ichtlinien für *Normen zur internen Kontrolle im öffentlichen Sektor – Weitere Informationen zum Thema ,,umfassendes Risikomanagement*

Vorwort

Die INTOSAI-Richtlinien für *Interne Kontrollnormen* aus dem Jahr 1992 sind ein lebendes Dokument, das von der Vision einer stetigen Weiterentwicklung der Normen für die Konzeption, Durchführung und Bewertung interner Kontrollen getragen wird. Teil dieser Zielsetzung sind Bemühungen um die laufende Aktualisierung der Richtlinien.

Der XVII. INCOSAI (Seoul, 2001) erkannte die dringende Notwendigkeit einer Aktualisierung der aus dem Jahr 1992 stammenden Richtlinien und fasste den Beschluss, die

Revision an dem vom Committee of Sponsoring Organisations of the Treadway Commission (COSO) vorgeschlagenen Rahmen für die Gestaltung eines internen Kontrollsystems zu orientieren. Nachfolgende Beratungen führten zu einer zusätzlichen Erweiterung, um ethische Werte einzubeziehen und mehr Informationen zu den allgemeinen Grundsätzen der Kontrolle im Bereich der Informationsverarbeitung zu liefern.

Die Richtlinien für die interne Kontrolle wurden 2004 aktualisiert und sollten ebenfalls als lebendes Dokument betrachtet werden, das im Zeitablauf weiter entwickelt und verfeinert werden muss, um neue Entwicklungen wie das COSO's *Enterprise Risk Management framework*¹ zu berücksichtigen. Dementsprechend wurde die vorliegende Ergänzung der Richtlinien erstellt, um die aktuellen fachlichen Konzepte zum Risikomanagement, wie sie im COSO ERM Framework niedergelegt sind, zu berücksichtigen. Da sich dieses Dokument hauptsächlich an Leser aus dem öffentlichen Sektor richtet, wurde der Ausdruck „Unternehmen“, der ganz überwiegend mit dem Privatsektor assoziiert wird, durch „Organisation“ ersetzt.

Die hier zusätzlich gegebenen Informationen sind Ergebnis der gemeinsamen Arbeit der Mitglieder des INTOSAI-Unterausschusses für die interne Kontrolle. Die vorliegende Aktualisierung wurde von einer aus Mitgliedern des Unterausschusses bestehenden Task Force koordiniert, der Vertreter der Rechnungshöfe der Staaten Frankreich, Ungarn, Bangladesch, Litauen, Niederlande, Oman, Ukraine, Rumänien, Vereinigtes Königreichs, USA und Belgien (Vorsitz) angehörten.

¹ Enterprise Risk Management - Integrated Framework (COSO – September 2004)

Franki VANSTAPEL
Erster Vorsitzender des Belgischen
RechnungshofesPräsident des INTOSAI-Unterausschusses
für die interne Kontrolle

Einleitung

Grundlegende Prämisse des COSO ERM Framework ist, dass jede Organisation bestimmte Leistungen zugunsten verschiedener Interessenträger erbringen soll. Vom öffentlichen Sektor wird allgemein erwartet, dass dessen Bedienstete nach dem Grundsatz der Fairness dem öffentlichen Interesse dienen und die öffentlichen Mittel sachgemäß bewirtschaften. Träger berechtigter Interessen, sind die Bürger und ihre gewählten Vertreter.

Alle Organisationen sind mit Ungewissheit konfrontiert und es ist die Aufgabe der Leitung, zu bestimmen, welches Maß an Ungewissheit sie bei den Bemühungen, für die Interessenträger optimalen Nutzen zu schaffen, in Kauf zu nehmen bereit ist. Wichtig ist auch die Erkenntnis, dass Ungewissheit sowohl Risiken als auch Chancen beinhaltet. Es besteht sowohl die Möglichkeit, dass der Nutzen sich verringert als auch, dass er sich erhöht. Im Kontext der öffentlichen Hand heißt dies, dem öffentlichen Interesse wird entweder besser oder schlechter gedient. Ziel des Risikomanagements ist es, der Organisationsleitung die Möglichkeit zu geben, mit Ungewissheit und den zugehörigen Risiken und Chancen zweckmäßig umzugehen, die Fähigkeit zur Nutzensteigerung zu stärken, wirksamere Dienstleistungen wirtschaftlicher und sparsamer sowie zielgerichteter zu erbringen und dabei Werte wie den Gleichbehandlungsgrundsatz und Gerechtigkeit im Allgemeinen zu berücksichtigen.

Die INTOSAI-Richtlinien für Normen der internen Kontrolle im öffentlichen Sektor sehen die interne Kontrolle als übergreifendes Konzept, mittels dessen eine Organisation so geführt werden kann, dass sie ihre Ziele erreicht. Das COSO ERM Framework und andere ähnliche Modelle gehen hier noch einen Schritt weiter mit der Aussage, dass die Organisation durch das Erkennen künftiger Chancen und Risiken so geleitet werden kann,

dass es möglich ist, die Ziele noch sachgerechter zu formulieren und die internen Kontrollmechanismen so zu gestalten, dass die Risiken minimiert und die Chancen maximiert werden.

Neben einer Erweiterung der vom Begriff „Corporate Governance“ erfassten Funktionen erforderte das Konzept des Risikomanagements ein Umdenken hinsichtlich der Formulierung von Zielen. Dies ist so, weil ein wirksames Risikomanagement einen auf die Strategieplanung angewandten, auf allen Ebenen sowie bei allen Untereinheiten einer Organisation wirksamen kontinuierlichen Prozess voraussetzt. Dieser ist so zu gestalten, dass alle Vorgänge, die die Fähigkeit der Organisation zur Erreichung ihrer Ziele beeinflussen, erkannt werden.

Das vorliegende Dokument skizziert einen empfohlenen Rahmen für die Anwendung der Grundsätze des Risikomanagements im Bereich der öffentlichen Hand und liefert eine Grundlage für die Bewertung des Risikomanagements einer Organisation. Es soll jedoch die Richtlinien für Normen der internen Kontrolle im öffentlichen Sektor nicht ersetzen, sondern ergänzende Zusatzinformationen liefern, die in den Fällen, in denen Mitgliedstaaten dies für angemessen halten, neben den genannten Normen genutzt werden. Weiterhin sollen die vorliegenden Richtlinien die Geltung einschlägiger gesetzlicher Regelungen, Verwaltungsvorschriften oder anderer im Ermessen der Organisationsleitung liegender Vorgaben in keiner Weise beschränken oder außer Kraft setzen.

Alles in allem soll hier klar gestellt werden, dass das vorliegende Dokument zusätzliche Richtlinien für Normen der Corporate Governance enthält. Die Richtlinien sollen nicht als ins Einzelne gehende Vorgaben für die Umsetzung eines Systems optimaler Unternehmensführung

verstanden werden. Es kann auch nicht erwartet werden, dass sie sich für alle Organisationen unabhängig vom jeweiligen rechtlichen Rahmen eignen. Die vorliegende Ergänzung soll jedoch weitere Elemente des breit gefassten Rahmens liefern, innerhalb dessen Organisationen ihre Grundsätze und Verfahren so weiterentwickeln können, dass ihre Leistungen für die Interessenträger soweit wie möglich optimiert werden.

Gliederung des vorliegenden Dokuments

Die Ergänzung ist ähnlich gegliedert wie die INTOSAI-*Richtlinie für Normen der internen Kontrolle im öffentlichen Sektor*. Im ersten Kapitel wird das Konzept des Risikomanagements definiert und sein Umfang beschrieben. Im zweiten Kapitel werden die Komponenten des Verfahrens vorgestellt und die Erweiterungen der Normen der internen Kontrolle beleuchtet.

Abschnitt 1: Was bedeutet umfassendes Risikomanagement?

1.1 Definition

1.1.1 Das COSO *ERM Framework* besagt, dass sich das Risikomanagement in folgender Weise mit den Risiken und Möglichkeiten befasst, die Einfluss auf die Schaffung und Bewahrung von Werten haben:

„Umfassendes Risikomanagement ist ein von Überwachungs- und Leitungsorganen, Führungskräften und Mitarbeitern einer Organisation bei der Strategiefestlegung innerhalb der Gesamtorganisation angewandtes Verfahren zum Erkennen der die Organisation möglicherweise beeinflussenden Ereignisse und zur Gewährleistung hinreichender Sicherheit bezüglich des Erreichens der Ziele der Organisation“. (COSO-ERM-Modell 2004)

1.1.2 Im öffentlichen Sektor haben die Ausdrücke „Schaffung von Werten (bzw. Nutzen)“ nicht die unmittelbare Bedeutung wie im Privatsektor. Die Definition ist jedoch absichtlich sehr weit, um so viele Sektoren und Arten von Organisationen wie möglich einzubeziehen. Insoweit ist es möglich,

die Ausdrücke „Erbringung von Dienstleistungen“ und „Bewahrung der Fähigkeit zur Erbringung von Dienstleistungen“ an die Stelle der Ausdrücke „Schaffung von Werten (bzw. Nutzen)“ und „Bewahrung von Werten (bzw. Nutzen)“ zu setzen.

1.2 Bestimmung der Aufgabenstellung

1.2.1 Ausgangspunkt für das Risikomanagement ist die festgelegte Aufgabenstellung oder das Leitbild der Organisation. Im Rahmen dieser Aufgabenstellung sollte die Leitung strategische Ziele setzen, Strategien zur Erreichung dieser Ziele auswählen und Unterziele für alle Ebenen der Organisation formulieren.

1.3 Festlegung der Ziele

1.3.1 Den INTOSAI-Richtlinien für Normen der internen Kontrolle zufolge können Ziele in vier Kategorien unterteilt werden (wobei allerdings die meisten Ziele unter mehrere Kategorien fallen). Die Kategorien sind folgende:

- **Strategische Ziele** – übergeordnete Ziele, die auf die Aufgabenstellung abgestimmt sind und die Aufgabenerfüllung unterstützen
- **Operative Ziele** – ordnungsmäßige, ethisch einwandfreie, sparsame, wirtschaftliche und wirksame Aufgabenerfüllung sowie Schutz der vorhandenen Mittel gegen Verlust, Missbrauch und Beschädigung

-
- **Berichterstattung** – Zuverlässigkeit der Berichterstattung einschließlich Einhaltung der Verpflichtungen zur Rechnungslegung
 - **Einhaltung von Vorgaben** – Beachtung der einschlägigen Rechts- und Verwaltungsvorschriften sowie der politischen Vorgaben der Regierung

1.3.2 Über die Ziele in den ersten beiden Kategorien hat die betreffende Organisation keine vollständige Kontrolle, so dass ein Risikomanagementsystem nur einen angemessenen Grad von Gewissheit darüber erzeugen kann, ob die Risiken befriedigend gemanagt werden. Das System sollte allerdings sicherstellen, dass die Leitung rechtzeitig erkennen kann, inwieweit diese Ziele erreicht werden. Über die Ziele zur Zuverlässigkeit der Berichterstattung und der Einhaltung von Vorgaben hat die betreffende Organisation jedoch die Kontrolle, so dass ein wirksames Risikomanagement in der Regel der Organisationsleitung Gewissheit darüber gibt, dass diese Ziele erreicht werden.

1.4 Risiken und Chancen von Ereignissen erkennen

1.4.1 Sind die Ziele gesetzt, ist das Risikomanagement organisatorisch so umzusetzen, dass Ereignisse erkannt werden, die sich auf die Erreichung der gesetzten Ziele auswirken können. Ereignisse können sich negativ, positiv oder sowohl negativ als auch positiv auswirken. Ereignisse mit negativer Auswirkung stellen Risiken dar, die die Fähigkeit der Organisation zur Erreichung ihrer Ziele beeinträchtigen können. Diese Risiken

können sich aus internen und externen Faktoren ergeben. Abb. 1 stellt viele der Risiken dar, denen staatliche Stellen ausgesetzt sind – bestimmte Dienststellen können durchaus noch anderen Risiken ausgesetzt sein.

- 1.4.2 Ereignisse mit positiver Auswirkung können negative Auswirkungen ausgleichen oder Chancen eröffnen. Unter Chancen ist die Möglichkeit des Eintritts eines Ereignisses zu verstehen, das die Fähigkeit der Organisation zur Erreichung ihrer Ziele verbessert oder sie in die Lage versetzt, ihre Ziele wirtschaftlicher zu erreichen. Die Organisationsleitung sollte sich nicht nur um die Abmilderung von Risiken bemühen, sondern auch Pläne für das Ergreifen von Chancen formulieren.

1.5 Kommunikation und Lernprozesse

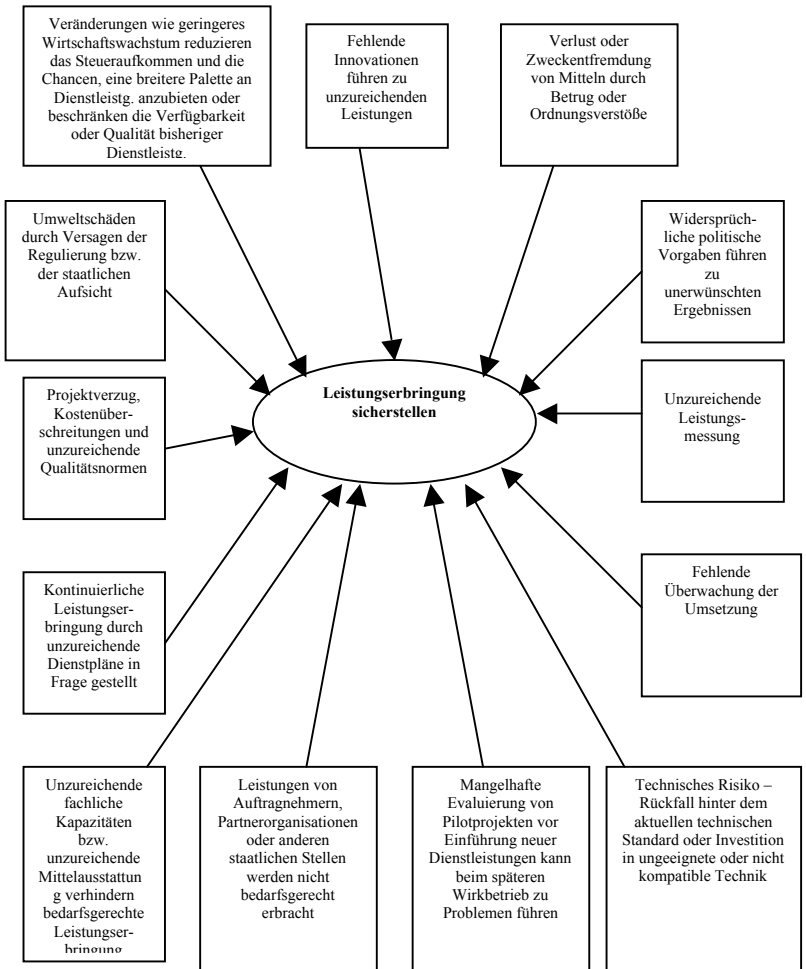
- 1.5.1 Die Beurteilung, ob das Risikomanagement einer Organisation „wirksam“ ist, bildet einen grundlegenden Teil des Prozesses. Die Organisationsleitung muss beurteilen, ob die Komponenten des Risikomanagements vorhanden sind und wirksam funktionieren; d.h. keine erheblichen Schwachstellen bestehen und alle Risiken unter Berücksichtigung der Risikobereitschaft der Organisation auf akzeptable Parameter zurückgeführt worden sind. Ist es wirksam, hat die Organisationsleitung Klarheit darüber, in welchem Ausmaß die Ziele aller Kategorien mit der Aufgabenstellung der Organisation in Einklang stehen und erreicht werden. Um diesen Prozess zu fördern, ist eine Kommunikation zwischen allen Ebenen

wesentlich („von oben nach unten und umgekehrt“).

1.6 Einschränkungen

- 1.6.1 Unabhängig davon, wie gut das System gestaltet und betrieben wird, kann das Verfahren der Organisationsleitung keine absolute Gewissheit über die Erreichung der allgemeinen Ziele liefern. Die vorliegende Ergänzung erkennt viel mehr an, dass nur ein angemessener Grad an Gewissheit erreichbar ist.
- 1.6.2 Angemessene Gewissheit ist gleichzusetzen mit einem zufriedenstellenden Vertrauen, dass die Ziele erreicht werden oder dass - wenn die Erreichung der Ziele unwahrscheinlich ist - die Organisationsleitung rechtzeitig davon erfährt. Die Bestimmung des notwendigen Grades an Gewissheit ist Ermessenssache. Bei Ausübung des Ermessens muss die Organisationsleitung die Risikobereitschaft der Organisation und die Ereignisse berücksichtigen, die sich auf die Zielerreichung auswirken können.
- 1.6.3 Das Konzept der angemessenen Gewissheit beruht auf dem Gedanken, dass Ungewissheit und Risiko sich auf die Zukunft beziehen, die niemand mit Gewissheit voraussagen kann. Außerdem können Faktoren, die außerhalb der Einwirkungsmöglichkeiten einer Organisation liegen, z.B. politische Faktoren, sich auf ihre Fähigkeit zur Erreichung ihrer Ziele auswirken.

Abb. 1: Einige typische Risiken, denen staatliche Stellen ausgesetzt sind



1.7 Verbindung zwischen interner Kontrolle und umfassendem Risikomanagement

1.7.1 Das Verfahren kann in vieler Hinsicht als natürliche Weiterentwicklung des Modells der internen Kontrolle betrachtet werden. Die meisten Organisationen werden zunächst das Modell der internen Kontrolle vollständig anwenden wollen, bevor sie die Konzepte des Risikomanagements anwenden. Die interne Kontrolle ist integraler Bestandteil des umfassenden Risikomanagements. Sie fällt in den Rahmen des Risikomanagements, stellt aber gleichzeitig ein Konzept für die Entscheidungsfindung auf der Grundlage der Kernaufgabe und damit verbundenen Zielen dar und dient als Instrument für die Organisationsleitung, mit dessen Hilfe diese bestimmen kann, welches die richtige Reaktion auf ein bestimmtes Ereignis ist. Das Modell des Risikomanagements geht in einer Anzahl von Bereichen über die INTOSAI-Richtlinien für die interne Kontrolle hinaus. Insbesondere:

- sind die Kategorien von Zielen weiter gefasst und erstrecken sich auch auf weitere Berichterstattung, nicht finanzielle Informationen und strategische Ziele;
- erweitert das Modell die Komponente „Risikoabschätzung“ und führt verschiedene Risikokonzepte ein, z.B. Risikobereitschaft, Risikotoleranz, Reaktion auf Risiken und
- betont es die Wichtigkeit unabhängiger Mitglieder in Verwaltungs- oder

Aufsichtsorganen und führt deren Rollen und
Zuständigkeit genauer aus.

Abschnitt 2 -

Komponenten des Risikomanagements

Das Verfahren besteht aus acht untereinander verbundenen Komponenten. Diese leiten sich daraus ab, wie Führungskräfte ein Unternehmen steuern und orientieren sich am Führungsprozess:

- Internes Umfeld
- Zielfestlegung
- Erkennen von Ereignissen
- Risikobewertung
- Risikobewältigung
- Steuerungsaktivitäten
- Information und Kommunikation
- Überwachung

Bei der Anwendung des Risikomanagements sollte eine Organisation den gesamten Umfang ihrer Tätigkeit auf allen Ebenen berücksichtigen. Außerdem sollte die Leitung neue Initiativen und Projekte unter Nutzung des Rahmens für das Risikomanagement prüfen.

Anwendung des umfassenden Risikomanagements

Die Leitung muss die Risiken im Sinne einer Aufgabenanalyse betrachten. Tatsächlich müssen die Führungskräfte auf allen Ebenen die Ereignisse in Betracht ziehen, die sich auf ihren Tätigkeitsbereich auswirken können und die oberste Leitungsebene davon unterrichten. Die Bewertung kann qualitativ oder quantitativ erfolgen. Die oberste Leitungsebene sollte die Teilbewertungen aller hierarchischen Ebenen und Geschäftsbereiche der Organisation nutzen, um für die Organisation insgesamt eine Bewertung des Gesamtrisikos vorzunehmen.

Bedeutung des menschlichen Faktors

Risikomanagement obliegt den Führungskräften und anderen Mitarbeitern und wird von diesen umgesetzt. Dies geschieht durch individuelles Handeln und Sprechen und beeinflusst das Risikomanagement des menschlichen Handelns. Jeder Mitarbeiter ist ein Individuum mit jeweils eigenen Kenntnissen und Fähigkeiten. Das Verfahren soll den Mitarbeitern das Verständnis des Risikos im Hinblick auf die Ziele der Organisation vermitteln.

Die Mitarbeiter sollten ihren jeweiligen Verantwortungsbereich und dessen Grenzen kennen. Dementsprechend muss eine klare und einfache Verknüpfung zwischen den Pflichten der einzelnen Mitarbeiter und der Aufgabenwahrnehmung bestehen. Die Leitungsebene hat hauptsächlich Aufsichtsfunktionen, aber auch Leitungsfunktionen, muss bestimmte Strategien, Vorgehensweisen sowie Grundsätze billigen und spielt damit eine wesentliche Rolle bei der Durchsetzung der Organisationskultur.

2.1 Risikoumfeld/Kontext

2.1.1 Das Risikoumfeld bzw. der Risikokontext umfasst das Klima einer Organisation, beeinflusst das Risikobewusstsein aller Mitarbeiter, ist Grundlage für alle anderen Komponenten des Risikomanagements und gibt dem System Disziplin und Struktur. Zu den Faktoren des internen Umfelds gehören die Risikomanagementphilosophie einer Organisation, ihre Risikobereitschaft, die Überwachung durch das Aufsichtsorgan, Integrität und ethische Werte, die Qualifikation der Mitarbeiter sowie die Art und Weise, in der die Leitung Befugnisse erteilt, Verantwortung festlegt, das Personal organisiert und weiterentwickelt.

2.1.2 Die Risikomanagementphilosophie einer Organisation ist die Gesamtheit der gemeinsamen Überzeugungen und Einstellungen, die darüber bestimmen, wie die Organisation bei allen ihren Tätigkeiten von der Festlegung der Strategie bis zum laufenden Tagesgeschäft Risiken berücksichtigt. Sie beeinflusst die Organisationskultur und die Aufgabenwahrnehmung einschließlich des Erkennens von Risiken, der Art von Risiken, die akzeptiert werden und die Risikosteuerung. Die Risikomanagement-philosophie einer Organisation sollte sich in „unternehmenspolitischen“ Erklärungen, mündlichen und schriftlichen Mitteilungen an die Interessenträger und Mitarbeiter sowie in den Entscheidungsprozessen niederschlagen. Unabhängig von der Kommunikationsmethode ist es wesentlich, dass die obere Leitungsebene die Philosophie nicht nur

durch die Übermittlung von Grundsätzen, sondern auch durch ihr tägliches Handeln bekräftigt.

- 2.1.3 Maßstab der Risikobereitschaft ist allgemein das Ausmaß des Risikos, das eine Organisation zur Erreichung ihrer Ziele einzugehen bereit ist. In der Risikobereitschaft schlägt sich die Risikomanagementphilosophie nieder. Andererseits beeinflusst sie die Organisationskultur und die Aufgabenerfüllung. Die Risikobereitschaft kann quantitativ oder qualitativ betrachtet werden. Sie sollte bei Festlegung der Strategie berücksichtigt werden, wobei der gewünschte Nutzen einer Strategie an der Risikobereitschaft gemessen werden sollte, d.h. mit der Bereitschaft, Risiken einzugehen oder zu tolerieren.
- 2.1.4 Die öffentliche Verwaltung hat bei der Bestandsaufnahme des Risikoumfeldes und des Ausmaßes der Risikobereitschaft auch ihre Einbindung in den Staatsaufbau zu berücksichtigen. Die Meinungen und Erwartungen der über- und nachgeordneten Stellen im Bereich der Exekutive oder Legislative und die Meinungen von Partnerorganisationen können klare Hinweise für eine angemessene Risikomanagementphilosophie und Risikobereitschaft liefern.
- 2.1.5 Die oberste Leitungsebene ist maßgeblicher Bestandteil des internen Umfeldes und beeinflusst dessen Elemente erheblich. Es ist eine Binsenweisheit, dass die Organisationskultur vom „Umgangston an der Spitze“ bestimmt oder entscheidend unterminiert werden kann. Dabei spielen die Unabhängigkeit der obersten Leitungs- bzw. Aufsichtsebene von der für den

Aufgabenvollzug zuständigen Leitungsebene, die Erfahrung und das Format der Angehörigen der obersten Leitungsebene, ihre Einbindung in die praktische Aufgabenwahrnehmung sowie die Aufsichtsaufgaben und die Angemessenheit ihrer Tätigkeit eine Rolle. Die Leiter der Vollzugsebene können auch dem obersten Leitungsebene- bzw. Aufsichtsorgan angehören; jedoch ist ratsam, dass diesem Organ auch einige unabhängige externe Mitglieder angehören wie im amerikanischen Verwaltungsrat. Denn das oberste Leitungs- bzw. Aufsichtsorgan muss bereit sein, sowohl das Vollzugsmanagement durch Befragung und Überwachung der Tätigkeit zu kontrollieren als auch die eigene Sicht der Dinge einzubringen.

- 2.1.6 Die Integrität und die ethischen Werte der Leitung beeinflussen die Umsetzung von Strategien und Zielen. Da der gute Ruf einer Organisation so wertvoll ist, müssen die Verhaltensnormen über die Einhaltung eines Mindeststandards der Rechtmäßigkeit hinausgehen. Ethisches Verhalten und die Integrität der Leitung sind Nebenprodukte der Organisationskultur, zu der neben ethischen und Verhaltensnormen auch die Art und Weise ihrer Umsetzung und Durchsetzung gehören. Die oberste Leitungsebene spielt eine wesentliche Rolle bei der Bestimmung der Organisationskultur. Eine unangemessene Schwerpunktsetzung bei kurzfristigen Ergebnissen anstatt der Ausrichtung an der langfristigen Aufgabenerfüllung kann zu einem unangemessenen Organisationsklima führen.
- 2.1.7 Förmliche Verhaltensnormen sind wichtige, ja grundlegende Faktoren für die Förderung eines angemessenen ethischen Klimas. Außerdem wichtig sind Kanäle für die Kommunikation nach

oben (oder förmliche Verfahren für Hinweise auf Missstände), durch die die Mitarbeiter ermutigt werden, der obersten Leitungs- bzw. Aufsichtsebene wichtige Hinweise zu geben. Ein schriftlicher Verhaltenskodex allein stellt jedoch nicht sicher, dass die vorgeschriebenen Verfahren eingehalten werden. Dies gilt selbst dann wenn alle Mitarbeiter die Kenntnisnahme der von ihnen einzuhaltenden Verhaltensregeln bestätigen müssen. Für die Durchsetzung der Regeln sind Sanktionen gegen Mitarbeiter, die Verstöße begehen, ebenso wichtig. Die von der obersten Leitungs- bzw. Aufsichtsebene übermittelten Botschaften werden schnell Bestandteil der Organisationskultur. Der Grundsatz, auch bei schwierigen geschäftlichen Entscheidungen „das Rechte zu tun“, setzt sich dann in der gesamten Organisation schnell durch.

- 2.1.8 Die Fachkompetenz ist die Gesamtheit der Kenntnisse und Fähigkeiten, die für die Durchführung der zugewiesenen Aufgaben benötigt werden. Um sie sicherzustellen, bedarf es einer Personalpolitik, die die Einstellung und Beförderung geeigneter Mitarbeiter, deren Einarbeitung und Fortbildung gewährleistet und über Instrumente für den Umgang mit Leistungsschwächen verfügt. Die Leitung hat die für die einzelnen Aufgaben benötigten Kenntnisse und Fähigkeiten genau festzulegen und sie in angemessene Stellenbeschreibungen umzusetzen. Wichtig ist dabei die Anerkennung der Tatsache, dass zwischen Qualifikation und Kosten ggf. ein Kompromiss gefunden werden muss.
- 2.1.9 Die Aufbauorganisation bildet den Rahmen für die Planung, Durchführung, Steuerung und Überwachung der Tätigkeiten. Sie ist den

Notwendigkeiten der Aufgabenerfüllung anzupassen. Der Aufbau kann zentralisiert, dezentralisiert, nach Standorten oder Funktionen gegliedert sein. Unabhängig von der Organisationsstruktur im Einzelnen sollte diese jedenfalls ein wirksames Risikomanagement und eine Aufgabenerfüllung ermöglichen, bei denen die Ziele der Gesamtorganisation erreicht werden.

- 2.1.10 Die Erteilung von Befugnissen und Übertragung von Verantwortung beinhaltet das Ausmaß, in dem Einzelne und Teams zur Eigeninitiative ermächtigt und ermutigt werden, um Aufgaben anzugehen und Probleme zu lösen. Es gehören dazu aber auch die Grenzen der Befugnisse. Die wesentlichen Herausforderungen bestehen darin zu gewährleisten, dass alle Mitarbeiter die Ziele der Organisation verstehen und sich außerdem darüber klar sind, wie ihre Handlungen zur Erreichung dieser Ziele beitragen, sowie darin, nur soweit zu delegieren, wie es für die Erreichung der Ziele notwendig ist. Verantwortung ist ebenso wichtig wie Befugnisse. Das Organisationsklima wird stark davon beeinflusst, in welchem Ausmaß Einzelpersonen erkennen, dass sie verantwortlich gemacht werden. Dies gilt bis hinauf zum Vorstandsvorsitzenden oder zum Präsidenten einer Behörde.

2.2 Zielfestlegung

- 2.2.1 Ziele werden auf der strategischen Ebene gesetzt und bilden die Grundlage für die Tätigkeit auf den nachgeordneten Ebenen, die Berichterstattung und die Durchsetzung von Vorgaben. Jede Organisation ist Risiken aus externen und internen Quellen ausgesetzt und die Festlegung von Zielen ist eine Voraussetzung für wirksames Erkennen

von Ereignissen, für die Risikobewertung und –steuerung. Erst nach der Festlegung der Ziele können Risiken erkannt und bewertet werden, die der Zielerreichung entgegenstehen können, und Maßnahmen zur Abmilderung dieser Risiken getroffen werden. Die Ziele müssen der Risikobereitschaft der Organisation entsprechen, von der wiederum die Risikotoleranzen für die Organisation abhängen.

- 2.2.2 Die Aufgabenbeschreibung („Mission“) einer Organisation legt in allgemeiner Form fest, was die Organisation erreichen will. Die Leitung setzt strategische Ziele, formuliert die Strategie und bestimmt die zugehörigen Einzelmaßnahmen. Strategische Ziele sind Oberziele, die der Aufgabenstellung der Organisation entsprechen und diese unterstützen. Die zur Aufgabenerfüllung umgesetzte Strategie und die zugehörigen Ziele unterliegen tendenziell einer stärkeren Dynamik als die „Mission“ und sind an sich verändernde Bedingungen anzupassen.
- 2.2.3 Trotz der Verschiedenheit der Ziele verschiedener Organisationen können einige allgemeine Kategorien angewandt werden. Alle Ziele fallen in eine oder mehrere der folgenden Kategorien:
- *Operative Ziele* – Diese beziehen sich auf die Wirksamkeit und Wirtschaftlichkeit der Aufgabenerfüllung einschließlich der Erreichung von Leistungs- bzw. Wirtschaftlichkeitszielen und den Schutz der vorhandenen Mittel gegen Verlust. Wird das Konzept des Schutzes der vorhandenen Mittel gegen Verlust im Zusammenhang mit öffentlicher Berichterstattung benutzt, kann eine erweiterte Definition dieses Begriffes

verwendet werden, nämlich im Sinne der Prävention, Aufdeckung und Korrektur der Zweckentfremdung öffentlicher Mittel. In den operativen Zielen müssen sich die Rahmenbedingungen, unter denen die Organisation tätig ist, niederschlagen. Da die operativen Ziele das wesentliche Kriterium für die Zuteilung von Mitteln sind, kann es zur Fehlallokation von Mitteln kommen, wenn diese Ziele unklar oder nicht gut durchdacht sind.

- *Berichterstattungsziele* – Diese beziehen sich auf die Zuverlässigkeit der Berichterstattung und können sich sowohl auf finanzielle als auch nichtfinanzielle Daten erstrecken. Zwar beziehen sich die Berichterstattungsziele auch auf für externe Adressaten erstellte Informationen; der Hauptzweck einer zuverlässigen Berichterstattung besteht jedoch darin, der Leitung genaue und vollständige sowie für den beabsichtigten Zweck geeignete Informationen zu liefern. Ohne genaue und vollständige Informationen ist es für die Leitungsebene sehr schwer, gute Entscheidungen zu treffen.
- *Ziele für die Regeleinhaltung* – Dazu gehört die Einhaltung der einschlägigen Rechts- und Verwaltungsvorschriften. Die Vorschriften können sich u.a. auf Märkte, die Umwelt, die Fürsorge für die Bediensteten beziehen. Einige Organisationen müssen auch internationale Vorschriften einhalten.

2.2.4 Durch ein wirksames Risikomanagement wird in angemessenem Umfang sichergestellt, dass die operativen sowie die auf die Berichterstattung und

die Regeleinhaltung bezogenen Ziele erreicht werden.

2.2.5 Die von der Leitung und dem Aufsichtsgremium festgelegte Risikobereitschaft ist ein Wegweiser für die Bestimmung der Strategie und die Priorisierung der Ziele. Die Risikobereitschaft bemisst sich nach dem Grad des Risikos, das einzugehen eine Organisation bereit ist, um einen Nutzen (in Form öffentlicher Dienstleistungen) für die Interessenträger zu erbringen. In der Regel steht eine Anzahl verschiedener Strategien für die Erfüllung der gewünschten Aufgabe zur Verfügung. Bei jeder Strategie sind die Risiken unterschiedlich. Die Leitung sollte eine Strategie und Ziele auswählen, die mit der jeweiligen Risikobereitschaft in Einklang stehen.

2.2.6 Risikotoleranz ist die hinnehmbare Abweichung von der vorgegebenen Zielerreichung. Sie kann mittels Leistungsvorgaben gemessen werden. Diese Messung erfolgt am besten in Organisationseinheiten, die auch für die Beurteilung der Zielerreichung zuständig sind. Sind Risikotoleranzen festgelegt, gibt dies der Leitung größere Sicherheit, dass die Organisation im Rahmen ihrer Risikobereitschaft bleibt und ihre Ziele erreicht.

2.3 Ereigniserkennung

2.3.1 Die Leitung erkennt mögliche Ereignisse, deren Eintreten sich auf die Organisation auswirkt. Die Ereignisse sind danach zu klassifizieren, inwieweit sie die Fähigkeit der Organisation fördern oder

beeinträchtigen, ihre Strategie erfolgreich umzusetzen und ihre Ziele zu erreichen (Risiken). Zur Erkennung von Ereignissen berücksichtigt die Leitung verschiedene interne und externe positive oder Risikofaktoren. Dies geschieht für den gesamten Bereich der Organisation.

- 2.3.2 Ein Ereignis ist ein Vor- oder Zwischenfall, der sich aus internen oder externen Faktoren ergibt und die Umsetzung der Strategie oder die Erreichung der Ziele beeinflusst. Ereignisse können sowohl negative als auch positive Auswirkungen haben. Die mögliche Bandbreite der Ereignisse reicht vom Offensichtlichen bis zum Obskuren und das Maß der Auswirkungen vom Wirkungslosen bis zum Hochbedeutsamen. Um das Übersehen von Ereignissen zu vermeiden, sollte die Ereigniserkennung gesondert von der Abschätzung der Wahrscheinlichkeit des Ereigniseintritts und seiner Wirkungen erfolgen.
- 2.3.3 Die Leitung muss die wichtigsten Arten interner und externer Ereignisauslöser kennen. Zu den externen Faktoren gehören u.a. Veränderungen der politischen, gesellschaftlichen und technischen Rahmenbedingungen sowie wirtschaftliche Entwicklungen, die entweder die Organisation selbst oder deren Vertragspartner beeinflussen. Die internen Faktoren ergeben sich aus Entscheidungen der Leitung zur Aufgabenerfüllung. Diese umfassen die Infrastruktur der Organisation, Zahl ihrer Standorte, Fachkenntnisse und Fähigkeiten der Mitarbeiter und Arbeitsweise der Managementinformationssysteme.
- 2.3.4 Ereigniserkennungsmethoden sind sowohl vergangenheits- als auch zukunftsorientiert. Bei

vergangenheitsorientierten Methoden werden u.a. die Jahresberichte und -abschlüsse, das bisherige Zahlungsverhalten und interne Berichte ausgewertet. Bei zukunftsorientierten Methoden können der demographische Wandel, neue Marktverhältnisse und zu erwartende Veränderungen der politischen Rahmenbedingungen berücksichtigt werden. Die Detailliertheit und Automatisierung können sich stark unterscheiden und die Methode kann entweder „von unten nach oben“ oder „von oben nach unten“ ansetzen.

- 2.3.5 Ereignisse treten oft nicht isoliert auf. Ein Ereignis kann ein anderes auslösen, und sie können gleichzeitig auftreten. Es ist nötig, zu verstehen, in welchem Zusammenhang Ereignisse miteinander stehen. Durch Bewertung dieser Beziehungen ist es ggf. möglich zu bestimmen, worauf sich das Risikomanagement konzentrieren sollte.
- 2.3.6 Auch ist es nützlich, potentielle Ereignisse in Kategorien einzuordnen. Der Zusammenhang zwischen Ereignissen kann durch eine horizontale Betrachtung im Rahmen der Gesamtorganisation oder durch eine vertikale Betrachtung innerhalb der operativen Organisationseinheiten ermittelt werden. Die Klassifizierung von Ereignissen kann auch Anhaltspunkte für kostengünstige Lösungen liefern. Zwar wird jede Organisation ihre eigene Methode der Klassifizierung von Ereignissen entwickeln; es gibt aber Standardinstrumente wie PEST Market Analysis², die als Grundlage dafür dienen können.

² Die PEST Analyse ist ein nützliches Instrument für das Verständnis und die Bewertung des Einflusses externer

2.4 Risikoabschätzung

- 2.4.1 Die Risikoabschätzung ermöglicht einer Organisation eine Bewertung des Ausmaßes, in dem sich potentielle Ereignisse auf die Zielerreichung auswirken. Die Leitung sollte Ereignisse mittels quantitativer und qualitativer Techniken unter zwei Gesichtspunkten bewerten, nämlich deren Auswirkung und Eintrittswahrscheinlichkeit. Die positiven und negativen Auswirkungen von Ereignissen können entweder einzeln oder nach Kategorien aus der Perspektive der Gesamtorganisation bewertet werden. Die Risikoabschätzung sollte sowohl im Hinblick auf das inhärente Risiko als auch das Restrisiko erfolgen.
- 2.4.2 Der Ausdruck „Risikoabschätzung“ wird gelegentlich für einen einmaligen Vorgang genutzt. Im Kontext des Risikomanagements ist die Risikoabschätzung ein kontinuierliches und sich wiederholendes Zusammenspiel verschiedener Maßnahmen innerhalb einer Organisation. Die Risikoabschätzung bezweckt die Erkennung von Ereignissen, die so wichtig und bedeutsam sind, dass sich die Leitungsebene damit beschäftigt.
- 2.4.3 Die Ungewissheit möglicher Ereignisse ist unter den Gesichtspunkten der Wahrscheinlichkeit und der Auswirkungen zu bewerten. Wahrscheinlichkeit ist dabei die Möglichkeit des Eintretens eines Ereignisses innerhalb eines

Faktoren auf die Zielerreichung einer Organisation. PEST steht als Abkürzung für „Political, Economic, Social and Technological factors“

bestimmten Zeitraums, während die Auswirkungen sich auf das Ausmaß des Einflusses beziehen, den das Ereignis auf die Zielerreichungsmöglichkeiten der Organisation hat. Der Zeitraum, für den die Leitung die Wahrscheinlichkeit abschätzt, sollte dem Zeithorizont der jeweiligen Strategie und Ziele entsprechen. Am wichtigsten sind Risiken mit hoher Eintrittswahrscheinlichkeit und starker Auswirkung. Am unbedeutendsten sind Risiken mit geringer Eintrittswahrscheinlichkeit und schwacher Auswirkung. Die Leitung sollte sich bei der Risikoabschätzung auf die Risiken mit hoher Eintrittswahrscheinlichkeit und starken Auswirkungen konzentrieren. Angestrebt wird eine Priorisierung sowohl nach Wahrscheinlichkeit als auch Stärke der Auswirkungen. Zum Teil wird dazu eine Bewertungsskala von hoch / stark bis niedrig / schwach verwendet, zum Teil ein Ampelsystem mit den Farben rot, gelb und grün oder ein prozentuales Risikoverteilungssystem.

Abbildung 2: Einfache Matrix für Risikoabschätzung und Risikosteuerung



2.4.4 Die Methodik der Risikoabschätzung kann quantitativ oder qualitativ sein. Sie kann sich auf objektive oder subjektive Methoden stützen. Es ist auch nicht zwangsläufig so, dass eine Organisation in allen ihren Geschäftsbereichen dieselben Techniken der Risikoabschätzung einsetzt. Die Leitung sollte sich jedoch der Subjektivität jeder menschlichen Risikoabschätzung bewusst sein und hat sicherzustellen, dass alle betreffenden Mitarbeiter ein einheitliches Verständnis der Priorisierung bei der Risikoabschätzung haben. Ist dies nicht der Fall, kann die oberste Leitungs- bzw. Aufsichtsebene die relative Bedeutung verschiedener Risiken nur schwer richtig einschätzen.

2.4.5 Nach Durchführung der Risikoabschätzung sollten die Risikoprioritäten der Organisation zu Tage treten. Ist nach Maßgabe der Risikobereitschaft der Organisation die Risikoexposition nicht

akzeptabel, sollte das Risiko als solches mit hoher Priorität oder als „wesentliches Risiko“ eingestuft werden. Die wesentlichen Risiken bedürfen der regelmäßigen Betrachtung durch die höchste Instanz innerhalb der Organisation. Die konkreten Risikoprioritäten ändern sich im Zeitablauf mit der Änderung der Ziele der Organisation, des Risikoumfeldes und infolge der getroffenen Maßnahmen zur Risikosteuerung.

- 2.4.6 Die oben skizzierte Risikoabschätzung bezieht sich auf das „inhärente Risiko“. Darunter ist dasjenige Risiko zu verstehen, dem die Organisation ohne Maßnahmen der Leitung zur Verringerung der Wahrscheinlichkeit seines Eintretens bzw. der Auswirkungen ausgesetzt wäre. Unter Restrisiko ist das Risiko zu verstehen, das unter Berücksichtigung der Risikosteuerungsmaßnahmen der Leitung noch besteht. Diese Maßnahmen werden im nächsten Absatz skizziert. Der Vorteil dieser Methode besteht darin, dass sie es Organisationen ermöglicht, Risiken zu erkennen, die Zeit auf Leitungsebene beanspruchen, die besser auf andere Angelegenheiten verwendet würde (z.B. weil beim inhärenten Risiko die Wahrscheinlichkeit seines Eintritts gering ist).

2.5 Risikosteuerung

- 2.5.1 Nach Abschätzung des jeweiligen Risikos hat die Leitung über die Maßnahmen der Risikosteuerung zu entscheiden. Mögliche Maßnahmen zur Steuerung erkannter Risiken sind die Risikoübertragung, die Risikobehandlung, die Einstellung von Tätigkeiten und die Tolerierung des Risikos. Bei den Überlegungen zu den Risikosteuerungsmaßnahmen bewertet die Leitung

deren Einfluss auf die Wahrscheinlichkeit des Eintretens und die Stärke der Auswirkungen, außerdem die Kosten und den Nutzen jeder Risikosteuerungsmaßnahme, um diejenige Maßnahme auszuwählen, die das Restrisiko so verringert, dass es innerhalb der Risikotoleranz liegt. Die Leitung sollte auch die verfügbaren Möglichkeiten prüfen und die Risiken organisationsweit und aufgabenbezogen betrachten.

2.5.2 Die Risikosteuerungsmaßnahmen lassen sich in folgende Kategorien unterteilen:

- *Risikoaufteilung bzw. -übertragung* - Verringerung der Wahrscheinlichkeit des Eintretens oder der Auswirkungen des Risikos durch seine Übertragung oder teilweise Verlagerung. Dies kann in Form einer herkömmlichen Versicherung geschehen oder dadurch, dass man eine dritte Stelle für die Risikoübernahme in anderer Form bezahlt. Diese Möglichkeit ist besonders nützlich, wenn es um die Verringerung finanzieller oder Vermögensrisiken oder um die Absicherung ausgelagerter Tätigkeiten geht. Jedoch lassen sich die meisten Risiken nicht vollständig übertragen. Selbst bei Outsourcing einer Dienstleistung kann das Risiko für den guten Ruf nicht übertragen werden.
- *Risikoverringern bzw. -behandlung* – Die weitaus meisten Risiken werden mit dieser Methode gesteuert. Es werden Maßnahmen ergriffen, um die Wahrscheinlichkeit des Eintritts oder die Auswirkungen zu verringern. Typischerweise umfasst dieser Ansatz eine große Zahl täglicher

Geschäftsentscheidungen einschließlich Kontrollverfahren, die ausführlicher in Abschnitt 2.6 und im „Rahmen für umfassendes Risikomanagement“ beschrieben sind.

- *Risikovermeidung / Beendigung der Tätigkeit* – Einstellung der vom Risiko betroffenen Tätigkeiten. Zwar dürften Stellen im Bereich der öffentlichen Hand selten in der Lage sein, die Erbringung von Kernleistungen einzustellen; jedoch kann Risikovermeidung eine nützliche Maßnahme sein, wenn es um die Entscheidung darüber geht, ob eine neue Methode der Leistungserbringung geeignet ist oder ob ein bestimmtes Projekt fortgesetzt werden soll.
- *Akzeptanz / Tolerierung* – In diesem Fall werden keine Maßnahmen ergriffen, um die Wahrscheinlichkeit des Eintritts oder die Auswirkungen zu verringern. Die Wahl dieser Alternative legt den Schluss nahe, dass entweder keine Möglichkeit gefunden wurde, mit der sich die Auswirkungen und die Wahrscheinlichkeit des Eintritts des Risikos wirksam auf ein akzeptables Niveau verringern lassen oder dass das inhärente Risiko im Bereich der Risikotoleranz liegt. Die Tolerierung des Risikos kann natürlich durch eine Notfallplanung ergänzt werden, um bei Eintritt des Risikos die Auswirkungen abzumildern.

2.5.3 Der Schwerpunkt des Modells liegt nicht ausschließlich auf der Risikovorschau oder -steuerung, sondern auch auf der Chancenerkennung im Rahmen desselben

Ansatzes. Die Leitungsebene sollte in jeder Situation die Aufmerksamkeit auch auf Chancen oder Ereignisse mit positiven Wirkungen richten, nicht nur auf Risiken oder Ereignisse mit negativen Auswirkungen. Hierbei sind zwei Gesichtspunkte zu berücksichtigen: zum einen, ob sich nicht gleichzeitig mit der Abmilderung von Gefahren Möglichkeiten zur Ausnutzung positiver Auswirkungen ergeben und zum anderen, ob Umstände eingetreten sind, die nicht zu Gefahren führen, aber positive Möglichkeiten eröffnen.

- 2.5.4 Die Leitungsebene sollte die Wirkungen der verschiedenen Methoden der Risikosteuerung bewerten und sich dann für die beste Alternative entscheiden. Dabei sind Maßnahmen oder Maßnahmenbündel zu wählen, die dazu beitragen, sowohl die Wahrscheinlichkeit des Risikoeintritts als auch die möglichen Auswirkungen auf das Risikotoleranzniveau zu verringern. Die gewählte Maßnahme muss nicht notwendigerweise zum geringstmöglichen Restrisiko führen. Wenn sie jedoch zu einem Restrisiko führt, das die Schwelle der Risikotoleranz übersteigt, ist entweder die gewählte Maßnahme oder die Höhe der Risikotoleranz nochmals von der Leitung zu überdenken.
- 2.5.5 Die Bewertung der Maßnahmen zur Steuerung inhärenter Risiken erfordert die Berücksichtigung von Zusatzrisiken, die sich aus einer Risikosteuerungsmaßnahme ergeben können. Die oberste Leitungs- bzw. Aufsichtsebene prüft Handlungsalternativen aus der Perspektive einer Aufgabenanalyse, da sie so einen Überblick über das Gesamtprofil der Risikosteuerungsmaßnahmen erhält und sie abschätzen kann inwieweit Restrisiken mit dem

Gesamtauftrag der Organisation und ihrer Risikobereitschaft in Einklang stehen.

- 2.5.6 Nach Auswahl der bevorzugten Methode der Risikosteuerung ist von der Leitung ein Plan für die Umsetzung zu erarbeiten. Wesentlicher Bestandteil jedes Umsetzungsplans sind Kontrollaktivitäten, die gewährleisten sollen, dass die Risikosteuerungsmaßnahme wirksam durchgeführt wird.

2.6 Kontrollmechanismen

- 2.6.1 Hierunter versteht man die Grundsatz- und Verfahrensregelungen, mit denen die Umsetzung der Risikosteuerungsmaßnahmen der Leitung gewährleistet werden soll. Kontrollmechanismen bestehen in allen Bereichen der Organisation, auf allen Ebenen und für alle Funktionen. Da die Richtlinien für Normen der internen Kontrolle im Bereich der öffentlichen Hand ausführliche Informationen zur Einrichtung wirksamer Kontrollmechanismen enthalten, soll dieser Nachtrag lediglich die internen Kontrollmechanismen in den Gesamtzusammenhang des umfassenden Risikomanagements stellen.
- 2.6.2 Bei diesem Verfahren werden die Kontrollaktivitäten als wesentlicher Bestandteil des Prozesses zur Zielerreichung der Organisation ihre Ziele angesehen. Kontrollaktivitäten erfolgen nicht um ihrer selbst willen oder weil sie als angemessen betrachtet werden, sondern weil sie die Steuerung der Zielerreichung ermöglichen.

-
- 2.6.3 Zwar werden Kontrollmechanismen im Allgemeinen eingerichtet, um zu gewährleisten, dass Risikosteuerungsmaßnahmen im Hinblick auf bestimmte Ziele angemessen durchgeführt werden, jedoch sind die Kontrollmechanismen selbst Maßnahmen der Risikosteuerung. Bei ihrer Auswahl oder Überprüfung müssen ihre Relevanz und Angemessenheit und die mit ihnen zusammenhängenden Ziele berücksichtigt werden.
- 2.6.4 Da jede Organisation ihre eigene Zielstruktur und Vorgehensweise bei der Umsetzung hat, gibt es Unterschiede bei den Risikosteuerungsmaßnahmen und den jeweiligen Kontrollmechanismen. Selbst wenn zwei Organisationen dieselben Ziele und Entscheidungen über die Vorgehensweise bei der Zielerreichung hätten, wären die sich daraus ergebenden Kontrollmechanismen wahrscheinlich unterschiedlich. Dies ist darauf zurückzuführen, dass verschiedene Organisationseinheiten jeweils eine unterschiedliche Risikobereitschaft und Risikotoleranz besitzen.
- 2.6.5 Jedoch lassen sich im Rahmen des Risikomanagements alle Kontrollverfahren in vier weitgefaste Kategorien einordnen:
- **Präventive Kontrollmechanismen** sollen die Möglichkeit des Eintritts eines Risikos und dessen unerwünschte Folgen beschränken. Je stärker die Auswirkungen des Risikos auf die Fähigkeit der Organisation zur Erreichung ihrer Ziele sind, desto wichtiger ist die Einrichtung geeigneter präventiver Kontrollvorkehrungen.

-
- **Direktive Kontrollmechanismen** sollen gewährleisten, dass ein bestimmtes Ergebnis erreicht wird. Solche Kontrollvorkehrungen sind besonders wichtig, wenn es um die Vermeidung eines unerwünschten Ereignisses (z.B. Sicherheitsverstoß) geht. Sie werden deshalb oft eingesetzt, um zur Erreichung von auf die Regeleinhaltung bezogenen Zielen beizutragen.
 - **Nachgelagerte Kontrollmechanismen** sollen eingetretene unerwünschte Ergebnisse erkennen lassen. Das Bestehen geeigneter nachgelagerter Kontrollmechanismen kann auch auf Grund der abschreckenden Wirkung das Risiko des Eintritts unerwünschter Ergebnisse vermindern.
 - **Korrektive Kontrollmechanismen** sollen eingetretene unerwünschte Ergebnisse korrigieren. Sie können auch als Notfallmaßnahmen fungieren, um nach Verlusten oder Schäden entweder verlorene Mittel oder die Funktionsfähigkeit zurückzuerlangen.

2.7 Information und Kommunikation

- 2.7.1 Zwischen den Qualitätsanforderungen an die Daten für Zwecke der internen Kontrolle und denjenigen zur Unterstützung des Risikomanagements bestehen kaum Unterschiede. Da die Richtlinien für Normen der internen Kontrolle im Bereich der öffentlichen Hand ausführliche Angaben zu den Qualitätsanforderungen an Information und Kommunikation enthalten, sollen mit dem

vorliegenden Nachtrag diese Anforderungen lediglich in den Kontext des Risikomanagements gestellt werden. .

Information

- 2.7.2 Das umfassende Risikomanagement verlangt insbesondere, dass eine Organisation eine größere Menge an Informationen gewinnt, als sie für die Erreichung der Ziele der internen Kontrolle braucht. Liegt z. B. der Schwerpunkt auf den strategischen Zielen, werden mehr Informationen über die Ergebnisse und Produkte benötigt. Außerdem werden diese Daten anders genutzt. Vergangenheitsbezogene Daten ermöglichen der Organisation einen laufenden Soll-Ist-Vergleich gemessen an den Zielen, Planungen und Erwartungen und können ein Frühwarnsystem für potentielle Ereignisse sein, denen die Leitung Beachtung schenken muss. Aktuelle Daten ermöglichen der Leitung eine Echtzeitbetrachtung vorhandener Risiken innerhalb einer Organisationseinheit oder eines Geschäftsprozesses sowie das Erkennen von Abweichungen gegenüber den Erwartungen. Damit kann die Organisation feststellen, ob sich ihre Tätigkeit im Bereich der Risikotoleranz bewegt.
- 2.7.3 Benötigte Informationen sollten fristgerecht erkannt, erfasst und so übermittelt werden, dass die jeweiligen Mitarbeiter, ihre Aufgaben erfüllen können. Wirksame Kommunikation umfasst sowohl den horizontalen als auch den vertikalen Informationsfluss in beide Richtungen innerhalb der Organisation ein. Alle Mitarbeiter sollten von

der obersten Leitungs- bzw. Aufsichtsebene die klare Vorgabe erhalten, dass die Aufgaben des Risikomanagements ernst zu nehmen sind. Sie müssen sich über ihre eigene Rolle innerhalb des Verfahrenablaufes sowie dessen Verknüpfung zur Arbeit anderer im Klaren sein. Mitarbeiter müssen über Möglichkeiten zur Übermittlung bedeutsamer Informationen an die jeweils geeignete Leitungsebene verfügen. Auch mit den externen Trägern berechtigter Interessen muss eine wirksame Kommunikation bestehen.

- 2.7.4 Die Umsetzung des Risikomanagements hängt im Wesentlichen davon ab, dass die richtigen Informationen zeitgerecht und adressatengerecht vermittelt werden.

Kommunikation

- 2.7.5 Kommunikation gehört zu jedem Informationssystem. Außer zur Übermittlung von Informationen, die die Mitarbeiter für ihre Aufgabenerfüllung brauchen, hat Kommunikation auch in einem breiteren Sinne stattzufinden, u.a. zur Verbreitung der Organisationskultur, zum Umgang mit Erwartungen, zur Festlegung von Zuständigkeiten einzelner Mitarbeiter und Mitarbeitergruppen.
- 2.7.6 Die Leitung kommuniziert organisationsintern konkret und direkt ihre Erwartungen zum Verhalten der Mitarbeiter und Informationen zur Klarstellung der Zuständigkeiten. Kommuniziert werden sollte auch eine klare Aussage zur Risikomanagementphilosophie der Organisation und den Umsetzungsmethoden'. Die Kommunikation über Geschäftsprozesse und Verfahren sollte mit der gewünschten

Organisationskultur in Einklang stehen und diese stützen. Kommuniziert werden sollten dabei

- die Bedeutung und Relevanz des umfassenden Risikomanagements
- die Ziele der Organisation
- die Risikobereitschaft und Risikotoleranz der Organisation
- eine einheitliche Ausdrucksweise für die Risikoerkennung und -abschätzung
- die Aufgaben und Pflichten der Mitarbeiter bei der Risikomanagementumsetzung und -unterstützung.

2.7.7 Außerdem muss es Methoden geben, mittels derer Mitarbeiter risikobezogene Informationen an ihre jeweiligen Fachvorgesetzten bzw. innerhalb der Gesamtorganisation weitergeben können. Die Mitarbeiter, die Publikumsverkehr bzw. Kontakte nach außen pflegen und täglich mit den Aufgaben des operativen Geschäfts zu tun haben, sind oft am besten in der Lage, Probleme schon im Stadium ihrer Entstehung zu erkennen. Für die Übermittlung einschlägiger Informationen müssen offene Kommunikationswege und eine klare Bereitschaft zum Zuhören vorhanden sein. Ist die Organisationskultur so angelegt, dass der Überbringer schlechter mit Sanktionen rechnen muss, werden die Mitarbeiter ihre Vorgesetzten nicht über Probleme unterrichten, so dass Risiken möglicherweise nicht rechtzeitig erkannt werden.

2.7.8 In den meisten Fällen gilt für die Unterrichtung der Vorgesetzten der normale Dienstweg. Es gibt jedoch einige Umstände, unter denen alternative Kommunikationskanäle (z. B. eine besondere Hotline für Hinweisgeber) notwendig sind. Wegen

seiner Bedeutung bedarf ein wirksames Risikomanagement eines alternativen direkten Kommunikationsweges zur höchsten Leitungs- bzw. Aufsichtsebene, den alle Mitarbeiter nutzen können, ohne Nachteile befürchten zu müssen.

- 2.7.9 Eine angemessene Kommunikation muss nicht nur innerhalb der Organisation, sondern auch mit der Außenwelt stattfinden. Es ist wichtig, nach außen mit den Interessenträgern darüber zu kommunizieren, wie die Organisation Risikomanagement betreibt, um ihnen Gewissheit darüber zu verschaffen, dass sie die erwartete Leistung erbringt. Auch die von außen an die Organisation herangetragenen Erwartungen müssen in gewisser Weise gesteuert werden. Dies ist besonders wichtig bei Risiken, die die Allgemeinheit betreffen und bei denen die Bürger erwarten, dass der Staat für sie Risikomanagement betreibt. Die Ernsthaftigkeit, mit der die Kommunikation mit Außenstehenden betrieben wird und die Aufrichtigkeit dieser Kommunikation vermitteln wichtige Botschaften an alle Teile der Organisation und können sich stark auf die Organisationskultur aufwirken.

2.8 Überwachung

- 2.8.1 Das Risikomanagement sollte überwacht werden, um das Funktionieren seiner Komponenten im Zeitablauf bewerten zu können. Dies kann durch kontinuierliche Überwachung, gesonderte Evaluierungen oder eine Kombination dieser beiden Verfahren erreicht werden. Mängel im System des Risikomanagements müssen an die richtige Leitungsebene gemeldet werden. Wenn es sich um schwerwiegende Angelegenheiten handelt, an die oberste Leitungsebene oder das

Aufsichtsorgan, damit die Organisation ihre Geschäftsprozesse verbessern kann.

- 2.8.2 Die Ziele einer Organisation können sich im Zeitablauf ändern. Der Bestand an vorhandenen Risiken und ihr relatives Gewicht dürfte sich ebenfalls im Zeitablauf ändern. Maßnahmen der Risikosteuerung, die in der Vergangenheit wirksam waren können irrelevant oder nicht mehr durchführbar werden und Kontrollmechanismen können an Wirksamkeit verlieren oder ganz entfallen.
- 2.8.3 Je nach Bedeutung der Risikogruppen, der Risikosteuerungsmaßnahmen und der Kontrollmechanismen unterscheiden sich Evaluierungen der Wirksamkeit des Risikomanagements in Umfang und Häufigkeit. Beschließt die Leitung eine umfassende Evaluierung des Risikomanagementsystems, sollte jeder Aspekt des Risikomanagementprozesses einschließlich der Festlegung einer Strategie betrachtet werden. Jedoch gehören auch wiederkehrende Tätigkeiten wie die Aktualisierung von Risikokatastern und organisatorische oder funktionale Überprüfungen zur Überwachung des Risikomanagementprozesses dazu.

Bibliographie

Australian Standard[®] for risk management (Standards Australia, 2004)

Entity Risk Management - Integrated Framework (COSO, 2004)

Integrated Risk Management Framework (Treasury Board of Canada Secretariat, 2001)

Internal Control - Integrated Framework (COSO, 1992)

Risk Management Standard (ARMIC, IRM & ALARM, 2002)

The Orange Book: Management of Risk - Principles and Concepts (HM Treasury, 2004)