

**INTOSAI**



RICHTLINIENKOMITEE FÜR DIE INTERNE  
KONTROLLE

**INTOSAI RICHTLINIEN  
FÜR DIE  
INTERNEN KONTROLLNORMEN  
IM ÖFFENTLICHEN SEKTOR**

# INHALTSVERZEICHNIS

|  |           |
|--|-----------|
| <a href="#">Vorwort</a> .....  | 2         |
| <a href="#">Einleitung</a> .....   | 4         |
| <b><a href="#">1 Interne Kontrolle</a></b> .....                           | <b>7</b>  |
| <a href="#">1.1 Definition</a> .....                                       | 7         |
| <a href="#">1.2 Grenzen der Wirksamkeit interner Kontrollsysteme</a> ..... | 13        |
| <b><a href="#">2 Eckpfeiler des internen Kontrollsystems</a></b> .....     | <b>15</b> |
| <a href="#">2.1 Kontrollumfeld</a> .....                                   | 19        |
| <a href="#">2.2 Risikobeurteilung</a> .....                                | 24        |
| <a href="#">2.3 Kontrolltätigkeiten</a> .....                              | 30        |
| <a href="#">2.4 Information und Kommunikation</a> .....                    | 39        |
| <a href="#">2.5 Überwachung</a> .....                                      | 43        |
| <b><a href="#">3 Aufgaben und Zuständigkeiten</a></b> .....                | <b>47</b> |
| <a href="#">Anlage 1 Beispiele</a> .....                                   | 53        |
| <a href="#">Anlage 2 Glossar</a> .....                                     | 61        |

# INTOSAI RICHTLINIEN FÜR INTERNE KONTROLLNORMEN IM ÖFFENTLICHEN SEKTOR

## Vorwort

Die INTOSAI Richtlinien für Interne Kontrollnormen aus dem Jahr 1992 sind ein lebendes Dokument, das von der Vision einer laufenden Weiterentwicklung der Normen für die Konzeption, Durchführung und Beurteilung 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. Aus der weiteren Auseinandersetzung mit der Thematik entwickelten sich zusätzliche Empfehlungen, welche die Einbindung des Konzepts einer ethischen Werterhaltung und die Erweiterung der allgemeinen Grundsätze für Kontrollen im Bereich der Informationsverarbeitung forderten. In der überarbeiteten Fassung der Richtlinien wird diesen Empfehlungen bereits Rechnung getragen. Dies sollte zu einer Vertiefung des Verständnisses neuer Konzepte über die interne Kontrolle beitragen.

Die überarbeiteten Richtlinien sollten ebenfalls als lebendes Dokument gesehen werden, das im Lauf der Zeit weiterentwickelt und verfeinert werden wird, um neuen Entwicklungen wie etwa dem COSO Rahmenwerk zum Enterprise Risk Management<sup>1</sup> Rechnung zu tragen.

Die vorliegende aktualisierte Fassung ist das Ergebnis der Bemühungen der Mitglieder des INTOSAI Richtlinienkomitees für die interne Kontrolle. Die Aktualisierung erfolgte durch eine von Mitgliedern des Komitees gebildete Task Force bestehend aus Vertretern der ORKB Boliviens, Frankreichs, Ungarns, Litauens, der Niederlande, Rumäniens, des Vereinigten Königreichs, der USA und Belgiens (Vorsitz).

Anlässlich der 50. Präsidialtagung (im Oktober 2002 in Wien) wurde dem Präsidium ein Aktionsplan für die Aktualisierung der Richtlinien unterbreitet und von diesem angenommen. Ein Bericht über den Fortschritt der Arbeit wurde dem Präsidium anlässlich der 51.

---

<sup>1</sup> COSO, Enterprise Risk Management Framework, Exposure Draft for Public Comment, [www.erm.coso.org](http://www.erm.coso.org), 2004.

Präsidialtagung (im Oktober 2003 in Budapest) vorgelegt. Bei einer Komiteesitzung im Februar 2004 in Brüssel wurde der Entwurf schließlich im Detail diskutiert und generell angenommen. Nach der Komiteesitzung wurde der Entwurf an alle INTOSAI-Mitglieder für eine abschließende Stellungnahme weitergeleitet.

Der Komiteepäsident hat die eingereichten Stellungnahmen analysiert und die geeigneten Abänderungen vorgenommen.

Ich möchte allen Mitgliedern des INTOSAI Richtlinienkomitees für die internen Kontrollnormen danken für deren Bemühungen und Mitarbeit an diesem Projekt. Besonderen Dank sage ich den Mitgliedern der Task Force.

Die Richtlinien für die internen Kontrollnormen im öffentlichen Sektor werden dem XVIII. INCOSAI in Budapest 2004 zur Genehmigung unterbreitet.

Franki VANSTAPEL  
Erster Vorsitzender des Rechnungshofes von Belgien  
Präsident des INTOSAI Richtlinienkomitees für die internen  
Kontrollnormen

## Einleitung

Im Jahr 2001 fasste der INCOSAI den Beschluss zur Aktualisierung der 1992 erlassenen INTOSAI Richtlinien für die internen Kontrollnormen. Damit soll allen wesentlichen aktuellen Entwicklungen im Bereich interne Kontrollsysteme Rechnung getragen und das dem COSO-Bericht „Internal Control – Integrated Framework“ zu Grunde liegende Konzept in die INTOSAI-Normen integriert werden.

Mit der Umsetzung des von der COSO vorgeschlagenen Modells in den neuen Richtlinien soll nicht nur das Konzept der internen Kontrolle auf den letzten Stand gebracht werden, vielmehr geht es dem Komitee auch darum, das allgemeine Verständnis interner Kontrolle bei den ORKB zu fördern. Es liegt auf der Hand, dass die besonderen Merkmale öffentlicher Verwaltungseinrichtungen in diesem Dokument speziell berücksichtigt werden. Dieser Umstand veranlasste das Komitee, eine Anzahl zusätzlicher Themen und aktueller Entwicklungen mit in Betracht zu ziehen.

Daher finden über das COSO-Rahmenwerk und das Konzept der Richtlinien aus dem Jahr 1992 hinausgehend auch die ethischen Aspekte der Arbeits- und Betriebsabläufe in der öffentlichen Verwaltung Berücksichtigung. Die Erweiterung der internen Kontrollziele um diesen Aspekt ist erforderlich, da die Bedeutung ethischen Verhaltens ebenso wie die Verhinderung und Aufdeckung von Betrug und Korruption im öffentlichen Sektor seit den Neunzigerjahren stärker in den Vordergrund getreten sind.<sup>2</sup> Grundsätzlich darf von öffentlich Bediensteten erwartet werden, dass sie dem Gemeinwohl zuverlässig dienen, öffentliche Mittel ordnungsgemäß verwalten und die Bürger nach dem Grundsatz von Rechtmäßigkeit und Gerechtigkeit unparteiisch behandeln. Ethische Grundsätze und Normen sind daher ein Eckpfeiler von Good Governance und eine wesentliche Voraussetzung, um das Vertrauen der Bevölkerung zu gewinnen und zu festigen.

Da es sich bei den vom öffentlichen Sektor verwalteten Ressourcen in der Regel um öffentliche Mittel handelt und deren Einsatz im Interesse der Allgemeinheit generell einer besonderen Sorgfalt bedarf, muss die Bedeutung, die einer ordnungsgemäßen Sicherung dieser Vermögenswerte zukommt, stärker betont werden. Außerdem verschafft die im öffentlichen Sektor noch vielfach übliche einfache Einnahmen- und Ausgabenrechnung keinen ausreichenden Einblick in Bezug auf die Beschaffung und den Einsatz der Ressourcen und deren weitere Verwendung. Die öffentlichen Verwaltungseinrichtungen verfügen daher nicht durchwegs über aktualisierte Aufzeichnungen über alle ihre Vermögenswerte, wodurch wiederum Schwachstellen entstehen. Die Sicherstellung der Ressourcen wurde daher als ein wesentliches Ziel interner Kontrollen erkannt.

Wie sich auch die Richtlinien für interne Kontrollnormen aus dem Jahr 1992 nicht auf das herkömmliche Konzept der Finanzkontrolle und der damit verbundenen Verwaltungskontrolle beschränkten und das breiter

---

<sup>2</sup> XVI INCOSAI, Montevideo, Uruguay, 1998.

gefasste Konzept der Managementkontrolle aufgegriffen, wird in diesem Dokument die Bedeutung von allgemeineren, über Finanzdaten hinausgehenden Informationen zusätzlich betont.

Durch den umfassenden Einsatz von Informationssystemen in allen öffentlichen Verwaltungseinrichtungen rückt die Bedeutung von Kontrollen im Bereich Informationstechnologie (IT-Kontrollen) in den Vordergrund. Diesem Erfordernis ist in den vorliegenden Richtlinien daher ein eigener Abschnitt gewidmet. Die IT-Kontrollen stehen in unmittelbarem Zusammenhang mit allen Teilbereichen des internen Kontrollsystems wie Kontrollumfeld, Risikobeurteilung, Information und Kommunikation sowie der laufende Überwachung der Wirksamkeit der Verfahren. Aus Gründen der einfacheren Darstellung werden sie im Abschnitt „Kontrolltätigkeiten“ zusammenfassend erörtert.

Die Zielsetzung des Komitees bestand in der Bereitstellung eines Leitfadens für die Entwicklung und Durchführung wirksamer interner Kontrollen im öffentlichen Sektor. Die Richtlinien richten sich daher zuallererst an die Führungsgremien öffentlicher Einrichtungen, für die sie als Leitfaden für die Umsetzung und Durchführung interner Kontrollen innerhalb der jeweiligen Körperschaften dienen können.

Da die Bewertung der Wirksamkeit interner Kontrollsysteme in der öffentlichen Verwaltung<sup>3</sup> einem allgemein anerkannten Normenstandard unterliegt, können die Richtlinien von Revisoren und Prüfern als Prüfinstrument eingesetzt werden. Einerseits dienen die unter Berücksichtigung des COSO-Rahmenwerks erstellten Richtlinien für interne Kontrollnormen Führungskräften in der öffentlichen Verwaltung<sup>4</sup> als Rahmenvorgabe zur Konzeption eines tragfähigen internen Kontrollsystems für die jeweilige Körperschaft, andererseits geben sie internen Revisoren und externen Prüfern einen Maßstab zur Beurteilung der internen Kontrollen an die Hand. Diese Richtlinien sind jedoch nicht als Ersatz für die INTOSAI Richtlinien für die Finanzkontrolle oder andere relevante Prüfungsnormen gedacht.

Mit dem vorliegenden Dokument wurde eine Rahmenempfehlung für ein internes Kontrollsystem für öffentliche Verwaltungseinrichtungen erarbeitet und eine Grundlage für die Evaluierung interner Kontrollsysteme geschaffen. Der hier vorgeschlagene Ansatz ist auf alle Teilbereiche der Arbeits- und Betriebsabläufe einer Körperschaft anwendbar. Die Richtlinien sind jedoch nicht dazu gedacht, rechtmäßige Kompetenzen einer Körperschaft in Bezug auf die Ausarbeitung von Gesetzen, den Erlass von Vorschriften oder die unabhängige Formulierung von strategischen Zielsetzungen einzuschränken oder zu behindern.

---

<sup>3</sup> INTOSAI Richtlinien für die Finanzkontrolle

<sup>4</sup> Das Verwaltungspersonal im Allgemeinen ist als Adressatengruppe nicht speziell genannt. Diese Gruppe ist zwar mit den Auswirkungen interner Kontrollen unmittelbar konfrontiert und spielt auch bei deren Durchführung eine wichtige Rolle, ist aber im Gegensatz zur Führungsebene nicht in letzter Instanz für die im Zusammenhang mit internen Kontrollen innerhalb einer Organisation ergriffenen Maßnahmen verantwortlich. Die Aufgaben und Zuständigkeiten werden in Abschnitt 3 im Einzelnen beschrieben.

Die internen Kontrollsysteme öffentlicher Verwaltungseinrichtungen müssen vor dem Hintergrund der speziellen Merkmale dieser Körperschaften erfasst werden, nämlich ihrer Ausrichtung auf soziale und politische Zielsetzungen, der Verwaltung öffentlicher Mittel, ihrer Abhängigkeit vom Haushaltszyklus, ihrer komplexen Leistungsstruktur (die einen Interessensausgleich zwischen traditionellen Werten wie Rechtmäßigkeit, Integrität und Transparenz und modernen unternehmerischen Wertmaßstäben wie Effizienz und Wirksamkeit erforderlich macht) und ihrer entsprechend umfassenden öffentlichen Rechenschaftspflicht.

Zusammenfassend sollte hervorgehoben werden, dass es in diesem Dokument um Richtlinien zur Formulierung von Normen und Standards geht. Die Richtlinien sind jedoch nicht als detaillierte Vorgaben für Strategien, Verfahren und Methoden zur Umsetzung interner Kontrollen zu sehen, sondern vielmehr als weitgefasser Leitfaden für die Entwicklung von Kontrollsystemen innerhalb der jeweiligen Körperschaften. Das Richtlinienkomitee verfügt natürlich über keinerlei Handhabe zur Durchsetzung von Normen und Vorgaben.

### **Die Struktur des Dokuments**

Im ersten Abschnitt wird das Konzept der internen Kontrolle definiert und die Reichweite der Kontrollen abgesteckt. In diesem Abschnitt wird auch auf die Grenzen interner Kontrollsysteme eingegangen. Im zweiten Abschnitt werden die einzelnen Komponenten interner Kontrollsysteme vorgestellt und erörtert. Das Dokument schließt mit der Beschreibung der Aufgaben und Zuständigkeiten im dritten Abschnitt. Jedem Abschnitt vorangestellt ist ein grau unterlegter Kasten, der eine kurze und zusammenfassende Darstellung der Hauptthemen des jeweiligen Abschnitts enthält. Daran anschließend folgt, kleiner gedruckt, die Erörterung der jeweiligen Themen, wobei auch auf im Anhang enthaltene konkrete Beispiele verwiesen wird. Ebenfalls im Anhang beigefügt ist ein Glossar mit den wichtigsten Fachbegriffen.

# 1 Interne Kontrolle

## 1.1 Definition

Die interne Kontrolle ist ein in die Arbeits- und Betriebsabläufe einer Organisation eingebetteter Prozess, der von den Führungskräften und den Mitarbeitern durchgeführt wird, um bestehende Risiken zu erfassen und zu steuern und mit ausreichender Gewähr sicherstellen zu können, dass die betreffende Körperschaft im Rahmen der Erfüllung ihrer Aufgabenstellung die folgenden allgemeinen Ziele erreicht:

- Sicherstellung ordnungsgemäßer, ethischer, wirtschaftlicher, effizienter und wirksamer Abläufe;
- Erfüllung der Rechenschaftspflicht;
- Einhaltung der Gesetze und Vorschriften;
- Sicherung der Vermögenswerte vor Verlust, Missbrauch und Schaden

Die interne Kontrolle ist ein in die Organisationsstruktur eingebetteter dynamischer Prozess, der laufend an die innerhalb der Organisation stattfindenden Veränderungen angepasst werden muss. Die Führungskräfte und die Mitarbeiter müssen auf allen Ebenen in diesen Prozess eingebunden werden, um bestehende Risiken zu erfassen und zu steuern und mit hinlänglicher Sicherheit gewährleisten zu können, dass die Körperschaft ihre Aufgabenstellung erfüllt und ihre allgemeinen Ziele erreicht.

### Ein eingebetteter Prozess

Die interne Kontrolle bezieht sich nicht auf ein Ereignis oder einen Umstand, sondern beinhaltet eine Kette von Kontrollverfahren, die auf allen Ebenen und in allen Arbeits- und Betriebsabläufen der Organisation wirksam werden. Sie ist quasi allgegenwärtig und kommt im Führungsstil des Managements zum Ausdruck. Interne Kontrolle ist im Gegensatz zur Ansicht mancher Beobachter nicht ein den Arbeits- und Betriebsabläufen einer Organisation hinzugefügter oder aufgesetzter Prozess, eine Art unausweichlicher Last, sondern ein eng mit der Gesamtorganisation verzahnter Prozess, der seine höchste Wirksamkeit entfaltet, wenn er, eingebettet in die Gesamtstruktur der Organisation, Teil ihres Wesens bildet.

Die interne Kontrolle sollte ein eingebetteter, und nicht ein aufgesetzter Prozess sein. Durch Einbettung als Bestandteil des Managementprozesses wird die interne Kontrolle zu einem Führungsinstrument im Dienste der Planung, Durchführung und laufenden Überwachung der Arbeits- und Betriebsabläufe.

Ein in die Gesamtstruktur eingebettetes internes Kontrollsystem trägt wesentlich zur Eindämmung der Kosten bei. Die Einführung neuer Kontrollverfahren neben bereits bestehenden Verfahren verursacht Kosten. Häufig lassen sich unnötige zusätzliche Verfahren und Kosten vermeiden, wenn man sich in einem ersten Schritt auf die bestehenden Abläufe und ihren möglichen Beitrag zu wirksamen internen Kontrollen durch Einbindung der Kontrollfunktionen in die eigentlichen Arbeits- und Betriebsabläufe konzentriert.

### **Umsetzung durch Führungskräfte und Mitarbeiter**

Das Funktionieren von internen Kontrollen hängt von den Menschen ab, von dem, was jeder Einzelne tut und sagt. Die Menschen müssen ihre Aufgaben und Zuständigkeiten, ebenso wie die Grenzen ihrer Kompetenzen genau kennen. Diesem Konzept ist auf Grund seiner hohen Bedeutung ein eigener Abschnitt (3) gewidmet.

Zu den in einer Organisation tätigen Menschen zählen die Führungskräfte und die übrigen Mitarbeiter. Dem Management obliegt in erster Linie die Aufsicht, es gibt jedoch auch die der Tätigkeit der Organisation zu Grunde liegenden Zielsetzungen vor und hat die Gesamtverantwortung für die Einrichtung und Führung eines wirksamen internen Kontrollsystems. Das interne Kontrollsystem umfasst jene Mechanismen, die benötigt werden, um die der Erreichung der Organisationsziele möglicherweise im Weg stehenden Risiken zu erfassen. Es ist die Aufgabe der Führungskräfte, interne Kontrollverfahren einzurichten, diese zu überwachen und zu bewerten. Die Umsetzung interner Kontrollen erfordert von den Führungskräften hohes Engagement und eine intensive Kommunikation zwischen dem Management und den übrigen Mitarbeitern. Die interne Kontrolle ist demzufolge ein Führungsinstrument, das sich unmittelbar an den Zielen der jeweiligen Organisation orientiert. Hauptverantwortlich für die interne Kontrolle ist das Management, während die Mitarbeiter eine wesentliche Rolle bei deren Durchführung spielen.

Die Wirksamkeit interner Kontrollsysteme hängt daher wesentlich vom Faktor Mensch ab. Die Richtlinien für die Einrichtung eines internen Kontrollsystems und die Durchführung der Kontrollen tragen der Tatsache Rechnung, dass nicht durchgehend sichergestellt werden kann, dass die Mitarbeiter die nötigen Informationen erhalten, die Kontrollen ausreichend verstehen und sie wirkungsvoll umsetzen. Jeder Mitarbeiter bringt seine eigene Geschichte und besonderen Fähigkeiten in die Organisation ein, hat aber auch seine speziellen Bedürfnisse und Prioritäten. Diese Gegebenheiten haben Einfluss auf die interne Kontrolle und werden von dieser beeinflusst.

### **Erfüllung der speziellen Aufgabenstellung der Organisation**

Das oberste Ziel jeder Organisation besteht in der Erfüllung ihrer Aufgabenstellung. Jede Körperschaft dient einem Zweck – der in der öffentlichen Verwaltung ganz allgemein darin besteht, gewisse Dienstleistungen zu erbringen und ein dem öffentlichen Interesse förderliches Ergebnis zu erzielen.

## Steuerung von Risiken

Worin immer die Aufgabenstellung einer Körperschaft besteht, die Erfüllung dieser Aufgabenstellung kann von vielerlei Risiken bedroht sein. Es ist die Aufgabe des Managements, diese Risiken zu identifizieren und entsprechend zu reagieren, um das bestmögliche Umfeld für die Umsetzung der Aufgabenstellung zu schaffen. Interne Kontrollsysteme tragen dazu bei, die Risiken zu erfassen, können jedoch nur hinlänglich sicherstellen, dass die Aufgabenstellung erfüllt und die Gesamtziele erreicht werden.

## Hinlängliche Sicherheit schaffen

Auch ein wohldurchdachtes und gewissenhaft eingesetztes internes Kontrollsystem bietet dem Management keine absolute Gewähr, dass die Gesamtziele erreicht werden. Die Richtlinien tragen dem Umstand Rechnung, dass nur ein „hinlängliches“ Maß an Sicherheit erreichbar ist.

Ein hinlängliches Maß an Sicherheit setzt voraus, dass – unter Berücksichtigung der Kosten, des Nutzens und der Risiken – ein zufriedenstellendes Maß an Vertrauen geschaffen wird. Um feststellen zu können, welches Maß an Sicherheit als hinlänglich betrachtet werden kann, ist eine Beurteilung der Situation erforderlich. Diese Beurteilung erfordert, dass die den Arbeits- und Betriebsabläufen inhärenten Risiken identifiziert werden und das unter wechselnden Bedingungen jeweils hinnehmbare Risiko definiert und aus qualitativer und quantitativer Sicht beurteilt wird.

Der Begriff der hinlänglichen Sicherheit basiert auf dem Konzept, dass Unsicherheit und Risiko in der Zukunft liegen, die niemand mit Sicherheit voraussagen kann. Ob die Ziele letztlich erreicht werden, hängt überdies auch von Faktoren ab, die außerhalb des Einflussbereichs der Organisation liegen. Weitere Einschränkungen resultieren aus den folgenden Umständen: Fehleinschätzungen können zu Fehlern in den Entscheidungsprozessen führen; banale Fehler oder Irrtümer können einen Systemzusammenbruch verursachen; geheime Absprachen zwischen zwei oder mehreren Beteiligten führen unter Umständen zu einer Umgehung der Kontrollen; oder das Management setzt sich über das interne Kontrollsystem hinweg. Außerdem kosten Kontrollen Geld, was zu Kompromisslösungen führen kann. Auf Grund dieser Einschränkungen kann vom Management die Erreichung der Ziele nicht mit absoluter Sicherheit gewährleistet werden.

Ein hinlängliches Maß an Sicherheit trägt der Tatsache Rechnung, dass die Kosten der internen Kontrolle den mit dem System erzielten Nutzen nicht übersteigen sollten. Entscheidungen im Hinblick auf Maßnahmen zur Risikosteuerung und die Einrichtung interner Kontrollen müssen auf Basis einer Kosten-/Nutzenrechnung getroffen werden. Die Kosten beinhalten jedoch nicht nur die für den jeweiligen Zweck aufgewendeten Finanzmittel, sondern auch die wirtschaftlichen Folgen verpasster Gelegenheiten, wie etwa Verzögerungen in Arbeits- und Betriebsabläufen, Abnahme der Servicequalität oder der Arbeitsleistung oder eine niedrige Arbeitsmoral auf Seiten der Mitarbeiter. Der Nutzen wird daran gemessen, inwieweit das Risiko verringert wird, dass ein gestecktes Ziel nicht erreicht wird. Beispiele, die hier zu nennen wären,

sind unter anderem eine Erhöhung der Wahrscheinlichkeit, dass Betrug, Verschwendung, Missbrauch oder Fehler rechtzeitig aufgedeckt, Misswirtschaft verhindert oder die Einhaltung von Vorschriften gefördert wird.

Die Konzeption von kosteneffizienten internen Kontrollsystemen, die geeignet sind, die Risiken auf ein hinnehmbares Maß zu reduzieren, setzt voraus, dass sich die Führungskräfte ein klares Bild von den zu erreichenden Gesamtzielen machen. Andernfalls droht Gefahr, dass die Führungskräfte in der öffentlichen Verwaltung in einem Bereich exzessive Kontrollen einführen, die dann negative Auswirkungen in anderen Bereichen haben. Zum Beispiel besteht Gefahr, dass Mitarbeiter aufwändige Verfahren umgehen, ineffiziente Abläufe Verzögerungen verursachen, zu komplexe Verfahren die Kreativität und Fähigkeit zur Problemlösung der Mitarbeiter einschränken oder die rechtzeitige Bereitstellung von Dienstleistungen verhindern und deren Kosten und Qualität negativ beeinflussen. Der in einem Bereich durch übermäßige Kontrollen erzielte Nutzen wird dadurch unter Umständen in anderen Bereichen durch erhöhte Kosten zunichte gemacht.

Darüber hinaus sollten auch qualitative Überlegungen angestellt werden. In Bereichen, in denen ein hohes Missbrauchsrisiko einem relativ geringen Geldwert gegenübersteht, wie etwa bei Gehältern, Reisespesen und Bewirtungsaufwendungen, erweisen sich angemessene Kontrollen unter Umständen als wichtig, auch wenn die Kosten gemessen an den betreffenden Beträgen und im Vergleich zu den Verwaltungsausgaben insgesamt überhöht erscheinen. Diese Kontrollen sind jedoch von entscheidender Bedeutung für den Erhalt des Vertrauens der Bevölkerung in die öffentliche Verwaltung und die Tätigkeit der öffentlichen Körperschaften.

### **Erreichung der Ziele**

Interne Kontrollen zielen darauf ab, das Erreichen einer Reihe von Gesamtzielen zu gewährleisten. Diese allgemeinen Ziele stehen in direkter Wechselbeziehung und werden über zahlreiche untergeordnete Ziele, Funktionen, Prozesse und Tätigkeiten umgesetzt.

Die übergeordneten allgemeinen Ziele bestehen in der:

- *Sicherstellung von ordnungsmäßigen, wirtschaftlichen, ethischen, effizienten und wirksamen Abläufen*

Die Arbeits- und Betriebsabläufe einer Organisation sollten ordnungsgemäß, ethisch, wirtschaftlich, effizient und wirksam sein. Sie müssen mit der Aufgabenstellung der Organisation im Einklang stehen.

Ordnungsgemäß bedeutet gut organisiert und methodisch.

Ethisch spricht moralische Grundsätze an. Die Bedeutung ethischen Verhaltens und der Verhinderung und Aufdeckung von Betrug und Korruption im öffentlichen Sektor ist in den Neunzigerjahren stärker in den Vordergrund getreten. Grundsätzlich wird von öffentlich Bediensteten erwartet, dass sie dem Gemeinwohl zuverlässig und fair dienen, die öffentlichen Mittel ordnungsgemäß verwalten und die Bürger

nach dem Grundsatz von Rechtmäßigkeit und Gerechtigkeit unparteiisch behandeln. Ethische Grundsätze sind daher ein Eckpfeiler von Good Governance in der öffentlichen Verwaltung und die Voraussetzung, um das Vertrauen der Öffentlichkeit zu gewinnen und zu festigen.

Wirtschaftlich bedeutet einen weder verschwenderischen noch übermäßigen Einsatz von Ressourcen. Hier geht es darum, die angemessene Menge an Ressourcen in der richtigen Qualität, zur rechten Zeit und zu geringstmöglichen Kosten bereitzustellen.

Effizient bezieht sich auf das Verhältnis der eingesetzten Ressourcen zu der zur Zielerreichung erbrachten Leistung. Dabei steht die Forderung im Vordergrund, dass eine bestimmte Menge oder Qualität einer Leistung mit dem geringstmöglichen Ressourceneinsatz produziert wird, beziehungsweise mit einer bestimmten Menge und Qualität an Ressourceneinsatz die maximale Leistung erzielt wird.

Wirksam bezieht sich auf die Erreichung von Zielen beziehungsweise das Ausmaß, in dem das Ergebnis einer Tätigkeit der Zielsetzung oder dem beabsichtigten Effekt dieser Zielsetzung entspricht.

- *Erfüllung der Rechenschaftspflicht*

Die Rechenschaftslegung ist der Prozess, durch welchen öffentliche Verwaltungseinrichtungen und deren Mitarbeiter über ihre Entscheidungen und Tätigkeiten im Rahmen ihrer Verantwortung für die Verwendung öffentlicher Mittel und deren angemessenem Einsatz sowie alle übrigen Aspekte der Arbeits- und Betriebsabläufe Rechenschaft ablegen.

Die Rechenschaftslegung erfolgt durch die Erstellung, Führung und Bereitstellung von zuverlässigen Finanz- und Managementinformationen und die angemessene Offenlegung dieser Information an intern und extern involvierte und interessierte Stellen in termingerecht vorgelegten Berichten.

Managementinformationen beziehen sich auf die Wirtschaftsentwicklung, die Effizienz und Wirksamkeit der Geschäftspolitik und der Tätigkeit der Organisation (Leistungsberichte) sowie interne Kontrollen und deren Wirksamkeit.

- *Einhaltung von Gesetzen und Vorschriften*

Die Organisationen unterliegen zahlreichen Gesetzen und Vorschriften. In Organisationen des öffentlichen Rechts ist die Aufbringung und Verwendung von öffentlichen Mitteln durch Gesetze und Verordnungen geregelt, darunter das Budgetgesetz, internationale Abkommen, Gesetze betreffend die ordnungsgemäße Verwaltung, Rechnungslegungsvorschriften und -normen, Umweltschutz- und Bürgerrechtsgesetze, Einkommenssteuerregelungen und Anti-Betrugs- und Korruptionsgesetze.

- *Sicherung der Vermögenswerte vor Zweckentfremdung und Schaden auf Grund von Verschwendung, Missbrauch, Misswirtschaft, Fehlern, Betrug und Unregelmäßigkeiten*

Das vierte dieser übergeordneten Gesamtziele könnte zwar als Unterkategorie des ersten gesehen werden (ordnungsgemäße, ethische, wirtschaftliche, effiziente und wirksame Abläufe), aber die hohe Bedeutung einer ordnungsgemäßen Sicherung der Ressourcen im öffentlichen Sektor muss speziell hervorgehoben werden. Bei den im öffentlichen Sektor verwalteten Ressourcen handelt es sich in der Regel um öffentliche Mittel, deren Einsatz im Interesse der Allgemeinheit generell einer besonderen Sorgfalt bedarf.

Außerdem verschafft die im öffentlichen Sektor noch vielfach übliche einfache Einnahmen- und Ausgabenrechnung keinen ausreichenden Einblick in Bezug auf die Beschaffung und den Einsatz der Ressourcen und deren weitere Verwendung. Die öffentlichen Verwaltungseinrichtungen verfügen nicht durchwegs über aktualisierte Aufzeichnungen über alle ihre Vermögenswerte, wodurch wiederum Schwachstellen entstehen. Aus diesem Grund sollten in allen mit der Verwaltung der Ressourcen einer Organisation verbundenen Abläufen vom Einkauf bis zu deren Ausscheiden entsprechende Kontrollen eingebaut werden.

Andere Ressourcen wie Information, Originaldokumente und Rechnungslegungsunterlagen bilden die Grundvoraussetzung für eine transparente Verwaltungstätigkeit und Rechenschaftslegung und sollten entsprechend verwahrt werden. Sie sind jedoch ebenfalls der Gefahr von Diebstahl, Zweckentfremdung oder Zerstörung ausgesetzt. Durch den Einsatz von Computersystemen kommt der Sicherstellung bestimmter Ressourcen und Aufzeichnungen erhöhte Bedeutung zu. Wenn nicht ausreichende Schutzmaßnahmen getroffen werden, besteht bei in Computermedien gespeicherten sensiblen Informationen Gefahr, dass diese zerstört oder kopiert, verbreitet oder unzulässig verwendet werden.

## 1.2 Grenzen der Wirksamkeit interner Kontrollsysteme<sup>5</sup>

Interne Kontrollsysteme gewährleisten nicht automatisch, dass die oben definierten Gesamtziele erreicht werden.

Ein wirksames internes Kontrollsystem, unabhängig davon, wie gut es konzipiert ist und betrieben wird, kann nur hinlänglich – und nicht absolut – sicherstellen, dass eine Organisation ihre Ziele erreicht bzw. dass sie überlebt. Auf dem Weg zur Zielerreichung liefern interne Kontrollen dem Management Informationen über den Erfolg der Tätigkeit der betreffenden Organisation, oder auch das Ausbleiben von Erfolg. Interne Kontrollsysteme können jedoch eine schlechte Führungskraft niemals in eine gute verwandeln. Darüber hinaus liegen Änderungen von Regierungsprogrammen und Faktoren wie demographische oder konjunkturelle Bedingungen außerhalb des Einflussbereichs des Managements einer Organisation und können eine Anpassung der Kontrollen oder des hinnehmbaren Risikos erfordern.

Ein wirksames System interner Kontrollen senkt die Wahrscheinlichkeit, dass Ziele verfehlt werden. Allerdings besteht auch immer das Risiko, dass die internen Kontrollen zu schwach ausgelegt sind oder nicht wie beabsichtigt funktionieren.

Da die Wirksamkeit interner Kontrollen auch vom *Faktor Mensch* abhängt, unterliegen die Systeme der Gefahr von Konzeptions-, Beurteilungs- und Auslegungsfehlern sowie Missverständnissen, Nachlässigkeiten, Ermüdungs- und Ablenkungserscheinungen, geheimen Absprachen, Missbrauch oder absichtlicher Umgehung.

Ein weiterer Einschränkungsfaktor bei der Einrichtung interner Kontrollsysteme sind *begrenzte Ressourcen*. Der Nutzen der Kontrollen muss daher immer gegen die Kosten abgewogen werden. Ein internes Kontrollsystem, das alle Verlustrisiken ausschließt, ist nicht realistisch und würde wahrscheinlich mehr kosten als der tatsächliche Nutzen rechtfertigen würde. Bei der Entscheidung, welche spezifischen Kontrollen eingerichtet werden sollten, müssen immer die Risikowahrscheinlichkeit und die potenziellen Auswirkungen auf die Organisation im Vergleich mit den Kosten für die Einrichtung der jeweiligen Kontrolle überlegt werden.

*Organisatorische Änderungen und die Einstellung des Managements* können die Wirksamkeit interner Kontrollen und die Einstellung der mit der Durchführung der Kontrollen betrauten Mitarbeiter entscheidend beeinflussen. Es ist daher von großer Wichtigkeit, dass das

<sup>5</sup> Die Grenzen der Wirksamkeit interner Kontrollen müssen betont werden, um übertriebenen Erwartungen durch Fehleinschätzung der Möglichkeiten vorzubeugen.

Management die Kontrollen laufend überprüft und aktualisiert, die Mitarbeiter über Veränderungen informiert und durch Einhaltung der Kontrollen mit gutem Beispiel vorangeht.

## 2 Eckpfeiler des internen Kontrollsystems

Das interne Kontrollsystem besteht aus fünf in Wechselbeziehung stehenden Komponenten:

- Kontrollumfeld
- Risikobeurteilung
- Kontrolltätigkeiten
- Information und Kommunikation
- Überwachung

Das interne Kontrollsystem ist dazu ausgelegt, mit hinreichender Sicherheit zu gewährleisten, dass die Gesamtziele der Organisation erreicht werden. Klare Ziele bilden daher die Voraussetzung für wirksame interne Kontrollen.

Das *Kontrollumfeld* ist die Basis für das gesamte interne Kontrollsystem. Es bestimmt die Disziplin und die Struktur des internen Kontrollsystems ebenso wie das Klima, das die Gesamtqualität der internen Kontrollen beeinflusst. Es ist für die Gesamtkonzeption der Strategie und der Ziele ebenso von Bedeutung wie für die Struktur der Kontrolltätigkeit.

Nach der Formulierung klarer Ziele und der Einrichtung eines wirksamen Kontrollumfeldes, wird durch *Beurteilung der Risiken*, die der Erfüllung der Aufgabenstellung der Organisation und ihrer Ziele im Weg stehen könnten, die Basis für die Entwicklung eines geeigneten Risikomanagementansatzes geschaffen.

Die wichtigste Strategie zur Beschränkung der Risiken besteht in *internen Kontrollmaßnahmen*. Kontrollmaßnahmen haben vorbeugende und/oder aufdeckende Funktion. Korrekturen und Verbesserungsmaßnahmen sind eine notwendige Ergänzung interner Kontrollmaßnahmen. Beide müssen einer Kosten-/Nutzenrechnung standhalten. Die Kosten sollten den erzielten Nutzen nicht übersteigen (Kostenwirksamkeit).

Wirksame *Information und Kommunikation* sind für funktionierende Arbeits- und Betriebsabläufe und Kontrollprozesse unerlässlich. Das Management einer Körperschaft braucht Zugang zu relevanten, vollständigen, zuverlässigen, korrekten und zeitgerechten Informationen über interne und externe Vorgänge. Auch innerhalb der Organisation ist die Verfügbarkeit von Information eine Voraussetzung, dass die jeweiligen Ziele erreicht werden können.

Schließlich bedarf das interne Kontrollsystem der ständigen *Überwachung*. Die interne Kontrolle ist ein dynamischer Prozess, der

eine laufende Anpassung an die tatsächlichen Risiken und Veränderungen in einer Organisation erforderlich macht. Durch Überwachung wird sichergestellt, dass die internen Kontrollen allfälligen Veränderungen der Zielsetzungen, des Umfeldes, der Ressourcen und der Risiken adäquat Rechnung tragen.

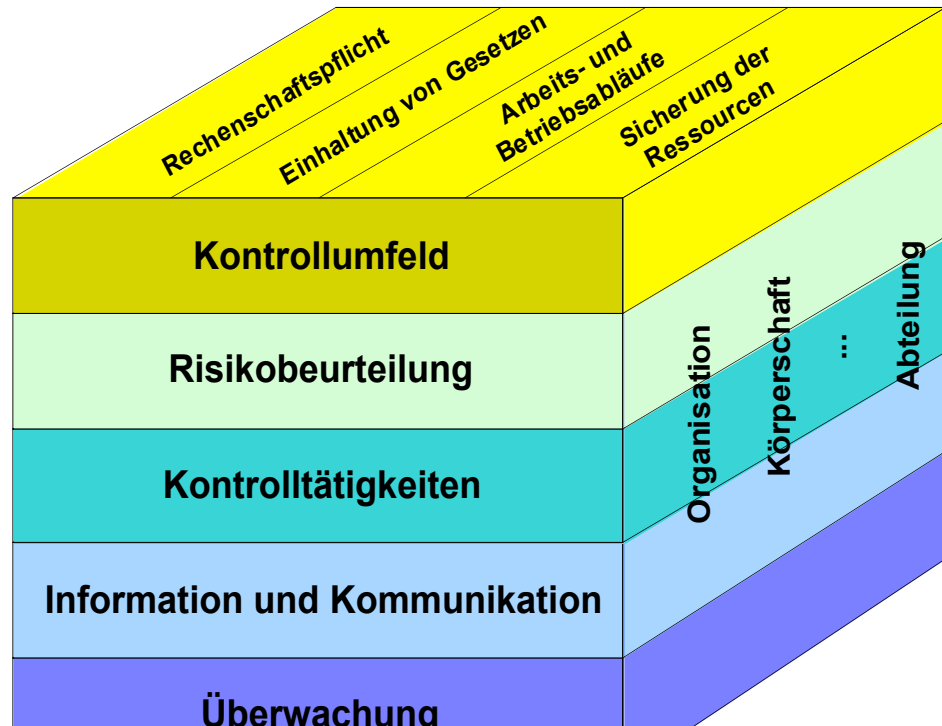
Diese Komponenten bilden die Eckpfeiler eines internen Kontrollsystems in der öffentlichen Verwaltung. Sie stecken den empfohlenen Rahmen für die Einrichtung und Führung eines internen Kontrollsystems ab und schaffen die Basis für die Evaluierung interner Kontrollen. Diese Komponenten gelten für alle Aspekte der Arbeits- und Betriebsabläufe einer Organisation.

Diese Richtlinien liefern einen allgemeinen Rahmen für interne Kontrolle. Die Umsetzung dieses Rahmens obliegt dem Management, das für die Entwicklung detaillierter und organisationsgerechter Strategien, Verfahren und Maßnahmen sowie deren Einbettung in die Arbeits- und Betriebsabläufe verantwortlich ist.

### **Wechselwirkung zwischen Zielen und Komponenten**

Die Gesamtziele, die abbilden, was eine Organisation erreichen will, und die Komponenten des internen Kontrollsystems, die darstellen, was zur Erreichung der allgemeinen Ziele erforderlich ist, stehen in direkter Wechselwirkung. Diese Wechselwirkungen werden durch ein dreidimensionales Modell in Form eines Würfels dargestellt.

In diesem Modell werden die vier übergeordneten Zielkategorien – Rechenschaftspflicht (und Berichterstattung), Einhaltung (von Gesetzen und Vorschriften), (ordnungsgemäße, ethisch einwandfreie, wirtschaftliche, effiziente und wirksame) Arbeits- und Betriebsabläufe und Sicherung der Ressourcen – durch die vertikalen Spalten abgebildet. Die fünf Komponenten der Kontrolle werden von den horizontalen Spalten dargestellt. Die dritte Dimension des Würfels verdeutlicht den Zusammenhang mit der Organisation oder Körperschaft und deren Abteilungen.



Jede der Komponenten „durchzieht“ und bezieht sich jeweils auf alle vier allgemeinen Zielkategorien und ist auf alle gleichermaßen anwendbar. So sind zum Beispiel aus internen oder externen Quellen stammende Finanz- und Managementinformationen, die in der Komponente Information und Kommunikation enthalten sind, für das Management der Arbeits- und Betriebsabläufe, die Berichterstattung und Erfüllung der Rechenschaftspflicht und die Einhaltung der gesetzlichen Vorschriften gleichermaßen erforderlich.

Ebenso gelten die vier Zielkategorien für jede der fünf Komponenten. Die Wirksamkeit und Effizienz der Abläufe kann hier als Beispiel dienen, das deutlich macht, dass jede der fünf Komponenten eine unerlässliche und wesentliche Rolle bei der Zielerreichung spielt.

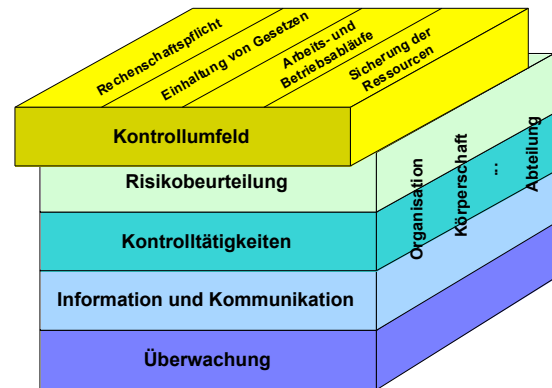
Interne Kontrollen sind nicht nur für die Gesamtorganisation von Bedeutung, sondern auch für die einzelnen Abteilungen. Dieser Zusammenhang wird durch die dritte Dimension verdeutlicht, welche die Organisation oder Körperschaft und deren Abteilungen darstellt. Jede der Einzelzellen des Würfelmodells kann separat für sich betrachtet werden.

Dieser interne Kontrollrahmen ist für jede öffentliche Verwaltungseinrichtung generell gültig und anwendbar. Die Umsetzung durch das jeweilige Management wird aber je nach dem Wesen der Körperschaft stark variieren und von einer Reihe spezifischer Faktoren abhängen. Zu diesen zählen unter anderem die Organisationsstruktur, das Risikoprofil, das operative Umfeld, die Größe, Komplexität und die Tätigkeit der Organisation sowie die jeweiligen normativen Vorgaben. Das Management muss unter Berücksichtigung der speziellen Gegebenheiten der betreffenden Organisation eine Reihe von Entscheidungen im Hinblick auf die Komplexität der Verfahren, die

eingesetzten Methoden und die Komponenten des internen Kontrollsystems treffen.

In den folgenden Abschnitten werden die obgenannten Komponenten im Überblick vorgestellt und durch zusätzliche Kommentare erläutert.

## 2.1 Kontrollumfeld



Das Kontrollumfeld bestimmt die Einstellung innerhalb einer Organisation und beeinflusst das Kontrollbewusstsein der Mitarbeiter. Es bildet die Basis aller übrigen Komponenten interner Kontrolle und gibt die Disziplin und Struktur vor.

Die Elemente des Kontrollumfelds sind:

- (1) Die persönliche und fachliche Integrität und die ethische Werterhaltung des Managements und der Mitarbeiter; dazu gehört eine in der Organisation durchgängig und konsequent fördernde Haltung gegenüber internen Kontrollen;
- (2) Engagement für Kompetenz;
- (3) „Das gute Beispiel der Führungskräfte“ (Philosophie und Führungsstil des Managements);
- (4) Organisationsstruktur;
- (5) Personalpolitik und Management.

### **Die persönliche und fachliche Integrität und die ethische Werterhaltung des Managements und der Mitarbeiter**

Die persönliche und fachliche Integrität und die ethische Werterhaltung der Führungskräfte und der Mitarbeiter bestimmen deren grundsätzliche Einstellung und Werturteile, die wiederum in Verhaltensgrundsätzen zum Ausdruck kommen. Führungskräfte und Mitarbeiter sollten zu jeder Zeit und in allen Bereichen eine unterstützende Einstellung zu internen Kontrollen zeigen.

Jede in einer Organisation tätige Person – Führungskräfte und Mitarbeiter – ist gefordert, die persönliche und fachliche Integrität und ethische Werthaltung zu jeder Zeit zu wahren, unter Beweis zu stellen und im Einklang mit den geltenden Verhaltensgrundsätzen zu handeln. Dies kann beispielsweise die Offenlegung von persönlichen finanziellen Interessen, von Funktionen in anderen Organisationen, von Geschenken (z.B. im Fall gewählter Mandatare und leitender Beamte) und von Interessenskonflikten beinhalten.

Ebenso sind die öffentlichen Verwaltungseinrichtungen gefordert, ihre Integrität und ethische Werthaltung zu wahren und unter Beweis zu stellen, und der Öffentlichkeit durch Vermittlung ihrer Aufgabenstellung und ihrer Grundwerte erkennbar machen. Darüber hinaus muss für ethische, ordnungsgemäße, wirtschaftliche, effiziente und wirksame Arbeits- und Betriebsabläufe gesorgt sein, die im Einklang mit der Aufgabenstellung der betreffenden Körperschaft stehen.

### **Engagement für Kompetenz**

Engagement für Kompetenz bezieht sich auf das Wissens- und Kompetenzniveau, das erforderlich ist, um eine ordnungsgemäße, ethische, wirtschaftliche, effiziente und wirksame Leistungserbringung gewährleisten zu können. Ebenso beinhaltet es die genaue Kenntnis der Zuständigkeiten für die internen Kontrollen.

Die Führungskräfte und Mitarbeiter müssen das erforderliche Kompetenzniveau aufweisen und bewahren, das sie befähigt, die Bedeutung der Entwicklung, Durchführung und Aufrechterhaltung leistungsfähiger interner Kontrollen zu begreifen, die allgemeinen Ziele interner Kontrollen zu erreichen und die Aufgabenstellung der Körperschaft zu erfüllen. Durch ihre jeweiligen Zuständigkeiten ist jede in einer Organisation tätige Person in den Prozess der internen Kontrolle eingebunden.

Die Führungskräfte und deren Mitarbeiter müssen daher über die notwendigen Fähigkeiten und die Fachkompetenz verfügen, um Risiken einschätzen und zu einer effizienten und wirksamen Leistungserbringung beitragen zu können sowie das Wesen der internen Kontrolle ausreichend verstehen, um ihrer Verantwortung in wirksamer Weise gerecht werden zu können.

Das Bewusstsein öffentlich Bediensteter über die Ziele der internen Kontrolle und speziell die Bedeutung ethischen Handelns kann zum Beispiel durch entsprechende Weiterbildungsmaßnahmen gefördert werden, was auch dazu beiträgt, das Verstehen der Ziele zu vertiefen und Fähigkeiten zu entwickeln, um ethische Probleme sinnvoll zu lösen.

## Das gute Beispiel der Führungskräfte

Das „gute Beispiel der Führungskräfte“ (Philosophie und Führungsstil des Managements) zeigt sich in:

- einer zu jeder Zeit unterstützenden Einstellung gegenüber internen Kontrollen, Unabhängigkeit, Kompetenz und Führung durch gutes Beispiel;
- den vom Management vorgegebenen Verhaltensgrundsätzen, und der Betonung der Bedeutung interner Kontrollziele und speziell ethischer Arbeits- und Betriebsabläufe in der Mitarbeiterberatung und in Leistungsbeurteilungen.

Die Einstellung der Führungskräfte zeigt sich in allen Aspekten der vom Management ergriffenen Maßnahmen. Engagement, Einsatz und Unterstützung der obersten Behördenleiter und der Gesetzgeber durch Vorgabe des „guten Beispiels“ fördern eine positive Einstellung und sind von entscheidender Bedeutung, um eine nachhaltig positive und unterstützende Haltung gegenüber internen Kontrollen zu gewährleisten.

Wenn die Führungsspitze die Überzeugung vertritt, dass interne Kontrollen wichtig sind, werden die übrigen Mitarbeiter diese Haltung übernehmen und die Kontrollen gewissenhaft durchführen. So wird zum Beispiel die Einrichtung einer internen Revisionsstelle in der Regel als ein starkes Signal für die hohe Bedeutung interner Kontrollen verstanden.

Wenn die Mitarbeiter umgekehrt den Eindruck gewinnen, dass das Management den internen Kontrollen keine hohe Bedeutung beimisst und das Engagement der Führungskräfte eher als Lippenbekenntnis denn als ernsthafte Unterstützung aufgefasst wird, ist mit großer Wahrscheinlichkeit damit zu rechnen, dass die Kontrollziele der Organisation nicht wirkungsvoll erreicht werden.

Es ist daher von entscheidender Bedeutung für das Erreichen der Kontrollziele, speziell der Zielsetzung „ethischer Arbeits- und Betriebsabläufe“, dass die Führungskräfte ethisches Verhalten vorleben und auf der Einhaltung hoher ethischer Standards beharren. Die Führungskräfte müssen durch ihr eigenes Verhalten eine Vorbildrolle einnehmen und ein angemessenes Leitbild schaffen, anstatt sich mit passablem und angepasstem Verhalten zu begnügen. Speziell die vom Management vorgegebenen Strategien, Verfahren und Methoden sollten auf die Förderung eines ordnungsgemäßen, ethischen, wirtschaftlichen, effizienten und wirksamen Verhaltens abzielen.

Die Integrität der Führungskräfte und ihrer Mitarbeiter wird jedoch von vielerlei Faktoren beeinflusst. Das Management sollte die Mitarbeiter daher in gewissen Abständen an die im Pflichten- und Verhaltenskodex definierten Verpflichtungen erinnern. Ein wichtiges Instrument in diesem Zusammenhang sind Beratungsgespräche und Leistungsbeurteilungen. Auch bei Gesamtleistungsbeurteilungen sollte die Durchführung der interner Kontrollnormen durch die Mitarbeiter neben zahlreichen anderen Beurteilungsfaktoren Berücksichtigung finden.

## Organisationsstruktur

In der Organisationsstruktur einer Körperschaft sind:

- die Zuweisung von Aufgaben und Verantwortungsbereichen;
- Übertragung von Befugnissen und Verantwortlichkeiten;
- die Einrichtung eines angemessenen Instanzenweges;

vorgegeben.

In der Organisationsstruktur sind die Aufgaben- und Verantwortungsbereiche einer Körperschaft festgelegt. Durch Übertragung der Befugnisse und Verantwortlichkeiten wird die Art und Weise vorgegeben, in der Aufgaben und Zuständigkeiten innerhalb der Organisation delegiert werden. Eine Übertragung von Befugnissen und Verantwortlichkeiten ist ohne Berichtswesen nicht denkbar. Daher muss ein angemessener Instanzenweg eingerichtet werden. In Sonderfällen, wie etwa einer Verwicklung des Managements in Unregelmäßigkeiten, müssen neben dem normalen Instanzenweg unter Umständen zusätzliche Wege der Berichterstattung eingerichtet werden.

Die Organisationsstruktur kann eine interne Revisionsstelle vorsehen, die unabhängig vom Management sein sollte und der obersten Managementebene in der Organisation direkt berichtet.

In Abschnitt 3 über Aufgaben und Zuständigkeiten wird ebenfalls auf die einzelnen Aspekte der Organisationsstruktur eingegangen.

## Personalpolitik und Personalmanagement

Der Bereich Personalpolitik und Personalmanagement umfasst die Personaleinstellung und Stellenbesetzung, Orientierungsmaßnahmen, Schulung (formal und praktisch) und Weiterbildung, Leistungsbeurteilung und Beratung, Förderungsmaßnahmen und Gehaltsschemen sowie Ausgleichsmaßnahmen.

Die Mitarbeiter bilden einen wichtigen Aspekt des internen Kontrollsystems. Kompetente, vertrauenswürdige Mitarbeiter sind eine Voraussetzung für wirksame Kontrollen. Einstellungs-, Schulungs- und Beurteilungsmaßnahmen sowie Gehaltsschemen und Förderungsmaßnahmen bilden einen wesentlichen Teil des Kontrollumfeldes. Bei Entscheidungen über Einstellungen und Stellenbesetzungen sollte sichergestellt sein, dass die jeweiligen Kandidaten persönliche Integrität und ausreichende Ausbildung und berufliche Erfahrung zur Durchführung der ihnen übertragenen Aufgaben aufweisen und dass sie die erforderliche formale Ausbildung, praktische Schulung und ethische Unterweisung am Arbeitsplatz erhalten. Führungskräfte und Mitarbeiter, die ein tiefgehendes Verständnis für interne Kontrollen zeigen und bereit sind, Verantwortung für diese zu übernehmen, sind für die Wirksamkeit von internen Kontrollstrukturen von ausschlaggebender Bedeutung.

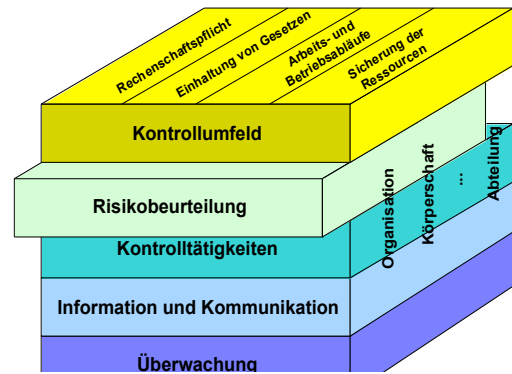
Das Personalmanagement spielt auch in der Förderung eines ethischen Umfeldes eine wichtige Rolle, indem für ein hohes professionelles Niveau und Transparenz in den täglichen Abläufen gesorgt wird. Dies

zeigt sich in der Personalbeschaffung ebenso wie bei Leistungsbeurteilungen und im Beförderungswesen, das auf einem Leistungssystem aufgebaut sein sollte. Die Sicherstellung offener Auswahlverfahren durch Veröffentlichung der Einstellungsbedingungen und die öffentliche Ausschreibung der Stellen trägt ebenfalls zur Verwirklichung eines hohen ethischen Standards im Personalmanagement bei.

### **Beispiele**

Der Leser wird auf die im Anhang enthaltenen Beispiele zu jedem der Ziele und den Komponenten eines internen Kontrollsystems verwiesen.

## 2.2 Risikobeurteilung



Die Risikobeurteilung ist ein Verfahren zur Identifizierung und Analyse von Risiken, welche die Erreichung der Ziele einer Körperschaft gefährden könnten, und dient zur Festlegung einer angemessenen Risikomanagementstrategie.

Sie umfasst:

(1) die Identifizierung von Risiken:

- in Bezug auf die Zielsetzungen der Körperschaft;
- im Gesamtzusammenhang;
- auf Grund externer und interner Faktoren, auf Ebene der Körperschaft und ihrer Tätigkeitsbereiche;

(2) die Risikoevaluierung:

- Einschätzung der Bedeutung eines Risikos;
- Abschätzung der Eintrittswahrscheinlichkeit;

(3) Einschätzung der Risikobereitschaft der Organisation;

(4) Entwicklung von Risikomanagementstrategien:

- Vier unterschiedliche Risikomanagementstrategien müssen erwogen werden: Übertragung, Tolerierung, Beschränkung oder Vermeidung; der bedeutendste Ansatz im Rahmen dieser Richtlinie ist die Beschränkung von Risiken, da wirksame interne Kontrollen die wichtigste Maßnahme zur Eindämmung von Risiken darstellen;
- Die geeigneten Kontrollmechanismen können

aufdeckender und/oder vorbeugender Natur sein.

- Das Arbeits- und Betriebsumfeld öffentlicher Verwaltungseinrichtungen befindet sich auf Grund von Veränderungen im administrativen und regulativen Umfeld und der volkswirtschaftlichen und konjunkturellen Rahmenbedingungen in ständigem Wandel. Daher sollte auch die Risikobeurteilung ein permanenter, sich ständig wiederholender Prozess sein, in dessen Rahmen geänderte Bedingungen, Chancen und Risiken erhoben und analysiert (Risikobeurteilungszyklus) und die internen Kontrollen der veränderten Risikosituation angepasst werden.

Wie schon in der Definition betont wurde, kann ein internes Kontrollsystem nur hinlänglich Gewähr bieten, dass die Ziele der Organisation erreicht werden. Die Risikobeurteilung ist eine Komponente der internen Kontrolle und spielt eine Schlüsselrolle bei der Wahl der geeigneten Kontrollmaßnahmen. Die Risikobeurteilung dient dazu, allfällige Risiken, welche die Erreichung der Ziele der jeweiligen Körperschaft gefährden könnten, zu identifizieren und zu analysieren und eine angemessene Risikostrategie zu bestimmen.

Eine Beurteilung der Risiken setzt voraus, dass die betreffende Organisation ihre Ziele definiert hat. Die Ziele müssen festgelegt werden, bevor das Management allfällige Risiken, die der Erreichung eines Zieles im Wege stehen könnten, feststellen und entsprechende Gegenmaßnahmen treffen kann. Die laufende Evaluierung der Risiken und die Entwicklung entsprechender Gegenmaßnahmen erfordert die Einrichtung eines kostengünstigen Systems und Mitarbeiter, die ausreichend qualifiziert sind, um potenzielle Risiken identifizieren und beurteilen zu können. Interne Kontrollen sind eine Maßnahme zur Risikobeschränkung, da sie dazu dienen, die Unsicherheit in Bezug auf die Wahrscheinlichkeit des Eintretens erkannter Risiken zu reduzieren.

Öffentliche Verwaltungseinrichtungen haben die Aufgabe, eine geeignete Risikomanagementstrategie zu entwickeln, um den Risiken, welche die Leistungserbringung und das Erreichen gewünschter Ergebnisse gefährden, wirksam zu begegnen.

### **Risikoidentifizierung**

Ein strategischer Ansatz zur Risikobeurteilung erfordert die Identifizierung von Risiken vor dem Hintergrund der strategischen Ziele der jeweiligen Organisation. Risiken, die diese Ziele gefährden könnten, werden dann analysiert und bewertet und die wesentlichsten Risiken herausgefiltert.

Die Identifizierung der primären Risiken ist nicht nur von Bedeutung, um die wichtigsten Bereiche zu bestimmen, denen die Ressourcen zur Risikobeurteilung zugeteilt werden sollten, sondern auch um die Verantwortung für das Management dieser Risiken entsprechend zuweisen zu können.

Die Leistungserbringung einer Körperschaft kann durch interne und externe Faktoren sowie auf der Ebene der Körperschaft und von deren Arbeits- und Betriebsabläufen gefährdet sein. Die Risikobeurteilung sollte alle potenziell bestehenden Risiken in Betracht ziehen (einschließlich des Betrugs- und Korruptionsrisikos). Von großer Bedeutung ist daher, dass die Identifizierung von Risiken aus dem Gesamtzusammenhang erfolgt. Die Identifizierung von Risiken ist ein permanenter, sich ständig wiederholender Prozess, der häufig in den Planungsprozess integriert ist. Ein von Null ausgehender Ansatz, der nicht einfach auf der zuletzt durchgeführten Prüfung aufbaut, erweist sich häufig als sinnvoll. Dieser Ansatz erleichtert das Erkennen von Änderungen im Risikoprofil<sup>6</sup> einer Organisation, die durch Veränderungen des wirtschaftlichen und regulativen Umfelds, interner und externer Bedingungen und die Einführung von neuen oder geänderten Zielsetzungen bedingt sein können.

Zur Identifizierung von Risiken müssen geeignete Instrumente eingesetzt werden. Zwei der häufigsten sind die Beauftragung von Risikoprüfungen und eine Selbstbewertung der Risiken.<sup>7</sup>

---

<sup>6</sup> Die Übersicht oder Matrix der Hauptrisiken einer Verwaltungseinrichtung oder untergeordneten Körperschaft, die auch das Ausmaß der Auswirkungen (z.B. hoch, mittel, gering) und die Wahrscheinlichkeit des Eintretens beinhaltet.

<sup>7</sup> *Beauftragung von Risikoprüfungen*

Dieses Verfahren baut auf dem Top-down Ansatz auf und besteht darin, dass ein Team zusammengestellt wird, das alle Abläufe und Tätigkeiten einer Organisation in Bezug zu deren Zielsetzungen untersucht und die bestehenden Risiken identifiziert. Das Team führt eine Reihe von Interviews mit Mitarbeitern auf allen Organisationsebenen, um für das gesamte Spektrum von Tätigkeiten ein Risikoprofil zu erstellen und Strategiebereiche, Tätigkeiten und Funktionen mit hohem Risikopotenzial (einschließlich Betrugs- und Korruptionsrisiko) zu identifizieren.

*Selbstbewertung von Risiken*

Dieses Verfahren baut auf dem Bottom-up Ansatz auf und besteht darin, dass jede Ebene und jeder Teilbereich einer Organisation aufgefordert wird, seine Tätigkeitsbereiche auf Risiken zu überprüfen und die Diagnose an die jeweils nächste Instanz zu melden. Die Durchführung erfolgt auf Basis eines übergreifenden Dokumentationsansatzes (wobei der Diagnoserahmen durch einen Fragebogen vorgegeben wird) oder durch moderierte Workshops.

Die beiden Ansätze schließen sich gegenseitig nicht aus, vielmehr ist eine Kombination der aus beiden Methoden gewonnenen Inputs wünschenswert, um die Identifizierung von organisationsweiten und auf bestimmte Tätigkeitsbereiche beschränkten Risiken zu erleichtern.

## Risikoevaluierung

Um Entscheidungen in Bezug auf eine wirkungsvolle Handhabung von Risiken treffen zu können, muss nicht nur grundsätzlich festgestellt werden, dass eine bestimmte Art von Risiko vorliegt, sondern es muss auch die Bedeutung des betreffenden Risikos und die Wahrscheinlichkeit des Eintretens beurteilt werden. Es gibt unterschiedliche Methoden zur Risikoanalyse, vor allem weil zahlreiche Risiken schwer zu quantifizieren sind (z.B. das Risiko für den Ruf), während sich andere leicht beziffern lassen (speziell finanzielle Risiken). Die erstere Gruppe lässt sich nur aus relativ subjektiver Sicht bewerten. Dies macht die Risikoevaluierung mehr zu einer Kunst als einer Wissenschaft. Allerdings lässt sich die subjektive Natur dieser Beurteilung durch die systematische und konsequente Anwendung von Risk Rating Kriterien in einem gewissen Maß einschränken.

Ein primärer Zweck der Risikoevaluierung besteht darin, dem Management Informationen über risikorelevante Bereiche, in denen Maßnahmen erforderlich sind, zu liefern, und diese Bereiche nach ihrer Priorität zu ordnen. Dazu bedarf es in der Regel eines Rahmens, in dem alle Risiken kategorisiert und, beispielsweise, als hoch, mittel oder niedrig eingestuft werden können. Generell ist zu empfehlen, die Anzahl dieser Kategorien gering zu halten, da eine zu ausgeprägte Differenzierung zu einer störenden Abgrenzung von Ebenen führen kann, die in Wirklichkeit nicht klar trennbar sind.

Eine derartige Evaluierung schafft die Grundlage für eine Reihung der Risiken, auf deren Basis das Management Prioritäten setzt, und liefert dem Management die nötige Information, um Beschlüsse fassen zu können, welchen Risiken mit Maßnahmen begegnet werden soll (z.B. den Risiken mit den potenziell gravierendsten Auswirkungen oder der höchsten Eintrittswahrscheinlichkeit).

## Beurteilung der „Risikobereitschaft“ der Organisation

Ein wichtiger Aspekt für die Entwicklung einer Risikomanagementstrategie ist die Definition der „Risikobereitschaft“ der betreffenden Körperschaft. Die Risikobereitschaft definiert das Risiko, das die Körperschaft einzugehen bereit ist, ohne Gegenmaßnahmen zu treffen. Entscheidungen in Bezug auf Risikomanagementmaßnahmen müssen im Zusammenhang mit der Feststellung des hinnehmbaren Risikos getroffen werden.

Bei der Feststellung der Risikobereitschaft müssen inhärente und Restrisiken berücksichtigt werden. Das inhärente Risiko ist jenes Risiko, dem eine Organisation ohne Maßnahmen zur Reduktion der Auswirkungen oder der Eintrittswahrscheinlichkeit ausgesetzt ist. Das Restrisiko ist das nach Ergreifung von Maßnahmen verbleibende Risiko.

Die Risikobereitschaft einer Organisation hängt von der den jeweiligen Risiken zugeordneten Bedeutung ab. Der hinnehmbare finanzielle Verlust, beispielsweise, hängt von einer Reihe von Aspekten ab, darunter auch dem Umfang des zur Verfügung stehenden Budgets, der Ursache des Verlustes, oder allfälliger Folgerisiken, wie Rufschädigung. Die Feststellung der Risikobereitschaft hängt stark von subjektiven

Faktoren ab, bildet aber in der Formulierung einer umfassenden Risikostrategie einen wichtigen Teilabschnitt.

### Entwicklung von Risikomanagementstrategien

Aus den bisher skizzierten Maßnahmen ergibt sich das Risikoprofil einer Organisation; dieses bildet die Basis für die Erarbeitung einer angemessenen Risikostrategie.

Grundsätzlich gibt es vier unterschiedliche Risikomanagementansätze. In manchen Fällen kann Risiko *übertragen*, *hingenommen* oder *vermieden* werden.<sup>8</sup> In den meisten Fällen wird es jedoch um eine *Beschränkung* des Risikos gehen. Um das Risiko auf ein akzeptables Niveau zu reduzieren, ist die Einrichtung und Führung eines wirksamen internen Kontrollsystems erforderlich.

Der Zweck des Risikomanagements besteht vor allem in der Eindämmung und nicht so sehr im Ausschluss von Risiken. Die Verfahren, die eine Organisation zur Steuerung von Risiken entwickelt, werden als interne Kontrollmaßnahmen bezeichnet. Die Risikobeurteilung sollte bei der Wahl angemessener Kontrollmaßnahmen eine wichtige Rolle spielen. Hier sei noch einmal darauf hingewiesen, dass nicht alle Risiken ausgeschlossen werden können und dass interne Kontrollen nur hinlänglich gewährleisten, dass die Ziele der Organisation kontinuierlich erreicht werden. Allerdings sind Körperschaften mit einem aktiven, auf die laufende Identifizierung und Beschränkung von Risiken abgestellten Risikomanagementansatz besser auf das mögliche Auftreten von Risiken und Veränderungen im Allgemeinen vorbereitet und auch rascher reaktionsfähig, wenn tatsächlich einmal etwas schief gehen sollte.

In der Ausgestaltung des internen Kontrollsystems ist es wichtig, darauf zu achten, dass die jeweilige Kontrolltätigkeit in einem angemessenen Verhältnis zum Nutzen steht, der durch Begrenzung des betreffenden Risiko erzielt wird. Mit Ausnahme extrem unerwünschter Folgen genügt es in der Regel Kontrollen einzurichten, die hinlänglich gewährleisten, dass ein allfälliger Verlust im Rahmen der Risikobereitschaft der Organisation bleibt. Jede Kontrolle verursacht Kosten, und der Nutzen

---

<sup>8</sup> Im Fall mancher Risiken besteht die beste Strategie in der *Übertragung* des Risikos. Dies kann durch konventionelle Versicherungen oder sonstige entgeltliche Übertragung an Dritte oder durch vertragliche Regelungen geschehen.

Für manche Risiken lassen sich keine oder nur bedingt Beschränkungsmaßnahmen treffen, oder die Kosten dieser Maßnahmen stehen in keinem realistischen Verhältnis zum möglichen Nutzen. In diesen Fällen liegt der sinnvollste Ansatz möglicherweise in der *Hinnahme* des Risikos.

Manche Risiken können nur auf ein akzeptables Niveau reduziert werden, indem die entsprechende Tätigkeit *vermieden* wird. Im öffentlichen Sektor ist die Möglichkeit zur Vermeidung von Tätigkeiten im Vergleich zum privaten Sektor möglicherweise stark eingeschränkt. Es gibt eine Reihe von Tätigkeiten, die gerade deshalb dem öffentlichen Sektor übertragen wurden, weil die inhärenten Risiken so hoch sind, dass der für das Gemeinwohl erforderliche Nutzen nur auf diese Weise erzielt werden kann.

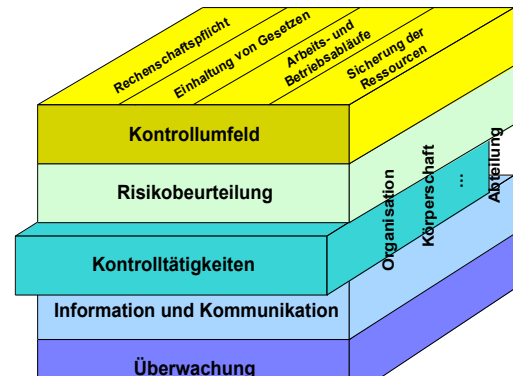
der Kontrolltätigkeit muss in einem angemessenen Verhältnis zu den Kosten der Risikoeindämmung stehen.

Das Arbeits- und Betriebsumfeld öffentlicher Verwaltungseinrichtungen befindet sich auf Grund von Veränderungen im administrativen und regulativen Umfeld und der volkswirtschaftlichen und konjunkturellen Rahmenbedingungen in ständigem Wandel. Dadurch ändert sich auch die Priorität von Zielsetzungen und das Risikoumfeld einer Organisation laufend, wodurch sich wiederum die Bedeutung der Risiken verlagert und verändert. Daher sollte die Risikobeurteilung ein permanenter, sich ständig wiederholender Prozess sein, in dessen Rahmen geänderte Bedingungen erhoben und analysiert (Risikobeurteilungszyklus) und, wo erforderlich, Maßnahmen eingeleitet werden. Die Risikoprofile und damit zusammenhängenden Kontrollen müssen regelmäßig überprüft und revidiert werden, um sicherzustellen, dass das Risikoprofil seine Gültigkeit behält, das Risikomanagement gezielt und angemessen bleibt, und die Kontrollen zur Steuerung der Risiken trotz der Veränderungen in der Risikolandschaft ihre Wirksamkeit behalten.

### **Beispiele**

Der Leser wird auf die im Anhang enthaltenen Beispiele zu jedem der Ziele und den Komponenten eines internen Kontrollsystems verwiesen.

## 2.3 Kontrolltätigkeiten



Die Kontrolltätigkeiten umfassen die von einer Körperschaft zur Risikosteuerung und zur Erreichung der Organisationsziele eingesetzten Strategien und Verfahren.

Um ihre Wirksamkeit zu gewährleisten, müssen die Kontrolltätigkeiten angemessen sein, über den gesamten Zeitraum hinweg kontinuierlich und nach Plan eingesetzt werden, weiters müssen sie kostengünstig, umfassend und sinnvoll sein und sich direkt auf die Kontrollziele beziehen.

Kontrolltätigkeiten fallen überall, auf allen Ebenen und in allen Aufgabenbereichen einer Organisation an. Sie umfassen aufdeckende und vorbeugende Kontrollmaßnahmen unterschiedlicher Natur, wie zum Beispiel:

- (1) Bevollmächtigungs- und Genehmigungsverfahren;
- (2) Aufgabentrennung (Genehmigung, Auswertung, Erfassung und Überprüfung);
- (3) Kontrolle über den Zugriff auf Ressourcen und Unterlagen;
- (4) Verifizierung;
- (5) Übereinstimmungsvergleich;
- (6) Leistungsüberprüfung;
- (7) Überprüfung der Arbeits- und Betriebsabläufe, Verfahren

und Tätigkeiten;

(8) Beaufsichtigung (Zuweisung, Überprüfung, Genehmigung, Anleitung und Training).

Die Körperschaften sollten für ein angemessenes Gleichgewicht zwischen aufdeckenden und vorbeugenden Kontrolltätigkeiten sorgen.

Korrekturen und Verbesserungsmaßnahmen sind als notwendige Ergänzung der Kontrollen erforderlich, um sicherzustellen, dass die Kontrollziele erreicht werden.

Die Kontrolltätigkeiten umfassen die für Risikomanagementzwecke eingesetzten Strategien und Verfahren, mit denen sichergestellt werden soll, dass die Organisationsziele erreicht werden.

Um wirksam zu sein müssen Kontrollmaßnahmen:

- angemessen sein (das heißt die richtige und dem Risiko angemessene Kontrolle am richtigen Ort);
- über den gesamten Zeitraum kontinuierlich und nach Plan durchgeführt werden (das heißt, sie werden von allen zuständigen Mitarbeitern sorgfältig eingehalten und in Abwesenheit von Aufsichtspersonen oder unter Arbeitsdruck nicht umgangen);
- kostengünstig sein (das heißt, die Kosten der Kontrollen sollten den Nutzen nicht übersteigen);
- umfassend und sinnvoll sein und sich direkt auf die Kontrollziele beziehen.

Die Kontrollmaßnahmen umfassen ein breites Spektrum an Strategien und Verfahren unterschiedlichster Natur wie:

### **1. Bevollmächtigungs- und Genehmigungsverfahren**

Geschäftsfälle und Vorgänge werden nur von Personen genehmigt und durchgeführt, die im Rahmen ihrer dienstlichen Befugnisse handeln. Die Genehmigung ist das wichtigste Instrument zur Sicherstellung, dass nur im Einklang mit den Absichten des Managements zulässige Maßnahmen und Vorgänge eingeleitet werden. Die Genehmigungsverfahren, die dokumentiert und den Führungskräften und Mitarbeitern in klarer Form bekannt gemacht werden sollten, sollten auf die speziellen Bedingungen hinweisen, unter denen die Genehmigungen zu erteilen sind. Die Bedingungen einer Bevollmächtigung einzuhalten bedeutet, dass die Mitarbeiter im Einklang mit den vom Management oder dem Gesetz vorgegebenen Richtlinien und Einschränkungen handeln.

## **2. Aufgabentrennung (Genehmigung, Auswertung, Erfassung und Überprüfung)**

Um das Risiko von Fehlern, Verschwendung oder unrechtmäßigem Handeln und das Risiko, dass derartige Probleme nicht aufgedeckt werden, zu reduzieren, sollte nie eine Person oder ein Team allein für alle Schlüsselfunktionen eines Geschäftsfalls oder Vorgangs zuständig sein. Vielmehr sollten die Aufgaben und Zuständigkeiten systematisch unter einer Anzahl von Einzelpersonen aufgeteilt werden, um wirksame gegenseitige Kontrollen sicherzustellen. Zu den Schlüsselfunktionen zählen die Genehmigung und Erfassung von Geschäftsfällen und deren Abwicklung, Überprüfung oder Revision. Geheime Absprachen können jedoch die Wirksamkeit dieser internen Kontrollen reduzieren oder zunichte machen. Eine kleine Körperschaft hat unter Umständen nicht genügend Mitarbeiter, um diese Kontrollen in vollem Umfang umzusetzen. In solchen Fällen ist das Management gefordert, sich die Risiken bewusst zu machen und andere ausgleichende Kontrollen einzusetzen. Eine möglicherweise hilfreiche Maßnahme besteht in einer Mitarbeiterrotation. Dadurch kann verhindert werden, dass eine Person allein über ungebührlich lange Zeiträume mit allen Schlüsselfunktionen in Bezug auf Geschäftsfälle und Vorgänge betraut ist. Darüber hinaus kann es zum Zweck der Risikobeschränkung auch nützlich sein, die Mitarbeiter zur Inanspruchnahme von Jahresurlauben anzuregen bzw. diese vorzuschreiben, und so eine vorübergehende Aufgabenrotation zu bewirken.

## **3. Kontrolle über den Zugriff auf Ressourcen und Unterlagen**

Der Zugriff auf Ressourcen und Unterlagen ist auf einen befugten Personenkreis zu beschränken, der für deren Verwahrung und/oder Verwendung verantwortlich ist. Die Verantwortung für die Verwahrung wird durch Belege, Inventarlisten oder sonstige Aufzeichnungen, welche die Übernahme oder die Übertragung zur Verwahrung belegen, dokumentiert. Durch die Einschränkung des Zugriffs auf die Mittel wird das Risiko einer unbefugten Verwendung bzw. von Verlusten für den Staat verringert und gleichzeitig dazu beigetragen, dass den Richtlinien des Managements Folge geleistet wird. Der Grad der Einschränkung hängt vom Gefährdungsgrad der Mittel und dem erkennbaren Verlustrisiko ab; beide Risiken sollten in regelmäßigen Abständen neu beurteilt werden. Bei der Feststellung des Gefährdungsgrades eines Vermögenswertes sollten Aspekte wie Wert, Transportfähigkeit und Austauschbarkeit mit in Betracht gezogen werden.

## **4. Verifizierung**

Geschäftsfälle und Vorgänge werden vor und nach ihrer Abwicklung auf ihre Richtigkeit überprüft. Bei Lieferungen, zum Beispiel, wird die gelieferte Stückzahl mit der bestellten Stückzahl und die verrechnete Stückzahl mit der erhaltenen Stückzahl verglichen. Bestände werden durch Bestandsaufnahmen erhoben und überprüft.

## 5. Übereinstimmungsvergleich

Aufzeichnungen werden in regelmäßigen Abständen mit der entsprechenden Dokumentation verglichen. So werden zum Beispiel Rechnungslegungsunterlagen, die sich auf Bankkonten beziehen, mit den entsprechenden Kontoauszügen verglichen.

## 6. Überprüfung der Betriebsleistung

Die Betriebsleistung wird anhand einer Reihe von Maßstäben in regelmäßigen Abständen auf ihre Wirksamkeit und Wirtschaftlichkeit überprüft. Sollte die Leistungsüberprüfung ergeben, dass die tatsächliche Leistung den bestehenden Zielen und Maßstäben nicht entspricht, sollten die Verfahren und Maßnahmen zur Erreichung der Ziele überprüft werden, um festzustellen, ob Verbesserungen erforderlich sind.

## 7. Überprüfung der Arbeits- und Betriebsabläufe, Verfahren und Tätigkeiten

Arbeits- und Betriebsabläufe, Verfahren und Tätigkeiten sollten in regelmäßigen Abständen überprüft werden, um zu gewährleisten, dass sie den geltenden Vorschriften, strategischen und operativen Vorgaben und sonstigen Erfordernissen entsprechen. Diese Art von Überprüfung der Tätigkeit einer Organisation sollte klar von der Überwachung der internen Kontrollen, die in Abschnitt 2.5 behandelt wird, unterschieden werden.

## 8. Beaufsichtigung (Zuweisung, Überprüfung, Genehmigung, Anleitung und Training)

Kompetente Beaufsichtigung trägt dazu bei, dass die Ziele der internen Kontrollen erreicht werden. Bei der Zuweisung, Überprüfung und Genehmigung der Tätigkeiten eines Mitarbeiters bedarf es:

- klarer Mitteilungen über die Aufgaben, Zuständigkeiten und Verantwortlichkeiten eines jeden Mitarbeiters;
- einer systematischen Überprüfungen der Arbeit eines jeden Mitarbeiters in dem jeweils erforderlichen Ausmaß;
- der Genehmigung zur Fortsetzung der Arbeiten an kritischen Punkten, damit gewährleistet ist, dass der Arbeitsablauf den vorgesehenen Verlauf nimmt.

Wenn ein Vorgesetzter Tätigkeiten delegiert, sollte dies die Rechenschaftspflicht des Vorgesetzten für die übertragenen Zuständigkeiten und Aufgaben nicht verringern. Die Vorgesetzten müssen ihren Mitarbeitern auch die notwendige Anleitung und Schulung bieten, um so dazu beizutragen, dass Fehler, Verschwendung und Unrechtmäßigkeiten auf ein Minimum reduziert werden und die Anweisungen der Führungskräfte in ihrer Bedeutung verstanden und in die Praxis umgesetzt werden.

Die obige Liste ist nicht vollständig, sie umfasst jedoch die üblichsten vorbeugenden und aufdeckenden Kontrolltätigkeiten. Die Kontrollmaßnahmen 1-3 sind vorbeugender, 4-6 vorwiegend

aufdeckender und 7-8 sowohl vorbeugender wie auch aufdeckender Natur. Eine Körperschaft sollte ein angemessenes Gleichgewicht zwischen aufdeckenden und vorbeugenden Kontrollmaßnahmen anstreben, wobei häufig eine Kombination verschiedener Kontrollen gewählt wird, um bestimmte Nachteile einzelner Kontrollmaßnahmen auszugleichen.

Bereits eingeführte Kontrollmaßnahmen müssen auf ihre Wirksamkeit überprüft werden. Daher müssen sie durch Korrekturen und Verbesserungsmaßnahmen ergänzt werden. Die Kontrolltätigkeiten sind außerdem nur eine Komponente des internen Kontrollsystems. Sie sollten daher mit den übrigen vier Komponenten des Systems in ein Ganzes integriert werden.

### **Beispiele**

Der Leser wird auf die im Anhang enthaltenen Beispiele zu jedem der Ziele und den Komponenten eines internen Kontrollsystems verwiesen.

### 2.3.1 Kontrolltätigkeiten im Bereich Informationstechnologie

Informationssysteme erfordern spezielle Kontrollmaßnahmen. Bei IT-Kontrollen werden zwei Hauptgruppen unterschieden:

#### (1) Allgemeine Kontrollen

Die allgemeinen Kontrollen umfassen die für einen weitgesteckten Bereich gültigen Strukturen, Strategien und Verfahren, die dazu beitragen, ordnungsgemäße Arbeits- und Betriebsabläufe sicherzustellen. Sie schaffen das Umfeld, in dem die Anwendungen betrieben und die Kontrollen durchgeführt werden.

Zu den Hauptkategorien der allgemeinen Kontrollen zählen (1) die organisationsweite Sicherheitsprogramm- und Sicherheitsmanagementplanung, (2) Zugriffskontrollen, (3) Kontrollen betreffend die Entwicklung, die laufende Pflege und den Austausch von Anwendungssoftware, (4) Systemsoftware-Kontrollen, (5) Aufgabentrennung, und (6) Servicekontinuität.

#### (2) Anwendungsspezifische Kontrollen

Die anwendungsspezifischen Kontrollen umfassen die für separate, individuelle Anwendungssysteme gültigen und unmittelbar auf einzelne elektronische Anwendungen bezogenen Strukturen, Strategien und Verfahren. Diese Kontrollen zielen im Allgemeinen darauf ab, Fehler und Unregelmäßigkeiten im Fluss der Informationen durch die IT-Systeme zu verhindern, aufzudecken und zu beheben.

Allgemeine und anwendungsspezifische Kontrollen stehen in Wechselwirkung und sind beide erforderlich, um eine vollständige und fehlerfreie Informationsverarbeitung zu gewährleisten. Da sich die Informationstechnologie in einem rapiden Wandel befindet, müssen IT-Kontrollen generell laufend weiterentwickelt werden, um ihre Wirksamkeit garantieren zu können.

Mit dem Fortschritt der Informationstechnologie wurden die öffentlichen Verwaltungseinrichtungen in ihren Arbeits- und Betriebsabläufen und der Verarbeitung, Sicherung und Weiterleitung wesentlicher Informationen zunehmend von elektronischen Informationssystemen abhängig. Die Zuverlässigkeit und Sicherheit elektronischer Daten und der Systeme zur Verarbeitung, Sicherung und Weiterleitung dieser Daten entwickelte

sich damit zu einem bedeutenden Anliegen des Managements ebenso wie der Revisoren und Prüfer der Organisationen. Die Informationssysteme erfordern zwar ganz bestimmte Arten von Kontrollen, aber die Informationstechnologie bildet dennoch keinen für sich allein stehenden Kontrollbereich, sondern einen in weite Teile des Gesamtsystems eingebetteten Bestandteil der internen Kontrollen.

Der Einsatz automatisierter Systeme in der Informationsverarbeitung bringt eine Reihe von Risiken mit sich, mit denen sich eine Organisation auseinandersetzen muss. Diese Risiken ergeben sich unter anderem aus der standardisierten Abwicklung von Geschäftsfällen; der automatischen IT-gestützten Abwicklung der Geschäftsfälle; einer erhöhten Gefahr, dass Fehler nicht entdeckt werden; der Existenz, Vollständigkeit und dem Umfang von Revisions- und Prüfungsdokumentation; der Art der verwendeten Hardware und Software sowie der Erfassung von außerordentlichen und nicht routinemäßigen Geschäftsfällen. Ein der standardisierten Abwicklung von Geschäftsfällen inhärentes Risiko besteht zum Beispiel darin, dass sich Programmierungsfehler durchgehend auf alle vergleichbaren Vorgänge auswirken. Durch wirkungsvolle IT-Kontrollen kann das Management mit hinlänglicher Sicherheit gewährleisten, dass die mit den IT-Systemen der Organisation verarbeiteten Informationen und Daten den Kontrollzielen wie der Sicherstellung der Vollständigkeit, Aktualität, Gültigkeit und Integrität entsprechen.

Die IT-Kontrollen lassen sich in zwei Hauptgruppen unterteilen, allgemeine Kontrollen und anwendungsspezifische Kontrollen.

### **Allgemeine Kontrollen**

Die allgemeinen Kontrollen beziehen sich auf die für das gesamte IT-System einer Organisation oder einen großen Teilbereich – wie Rechenzentrum, Kleincomputer, Netzwerk und Endbenutzerumfeld – gültigen Strukturen, Strategien und Verfahren, die dazu beitragen, den ordnungsgemäßen Betrieb sicherzustellen. Sie bestimmen das Umfeld, in dem die Anwendungen betrieben und die Kontrollen durchgeführt werden.

Die Hauptkategorien der allgemeinen Kontrollen:

1. *Die organisationsweite Sicherheitsprogramm- und Sicherheitsmanagementplanung* schaffen einen Rahmen für die Tätigkeiten im Bereich Risikomanagement, die Entwicklung von Sicherheitsstrategien, die Übertragung von Zuständigkeiten und die Überwachung der Angemessenheit der IT-Kontrollen in der Organisation und stellen die regelmäßige Durchführung der Kontrollen sicher.
2. *Zugriffskontrollen* beschränken bzw. legen den Zugriff zu Computer-Ressourcen (Daten, Programmen, Ausrüstung und Anlagen) offen und schützen diese Betriebsmittel dadurch vor unbefugter Veränderung und Offenlegung oder Verlust. Die Zugriffskontrollen umfassen sowohl physikalische als auch logische Kontrollen.
3. *Kontrollen betreffend die Entwicklung, die laufende Pflege und den Austausch von Anwendungssoftware* verhindern den Einsatz von

- nicht genehmigten Programmen oder Änderungen an bestehenden Programmen.
4. *Systemsoftware-Kontrollen* beschränken und überwachen den Zugriff auf leistungsstarke Programme und sensible Dateien, die zur Hardware-Steuerung und zur Sicherung von im System unterstützten Anwendungen dienen.
  5. *Aufgabentrennung* bezieht sich auf die Entwicklung und Einrichtung von Strategien, Verfahren und einer Organisationsstruktur, die verhindern, dass eine Person allein alle Schlüsselaspekte von IT-bezogenen Arbeits- und Betriebsabläufen kontrolliert und dadurch unbefugten Maßnahmen oder unbefugtem Zugriff zu Vermögenswerten oder Aufzeichnungen Vorschub geleistet wird.
  6. *Servicekontinuität* gewährleistet Unterstützung um sicherzustellen, dass kritische Operationen im Fall unerwarteter Ereignisse ohne Unterbrechung weitergeführt oder umgehend wieder aufgenommen werden können und kritische und sensible Daten geschützt bleiben.

### **Anwendungsspezifische Kontrollen**

Anwendungsspezifische Kontrollen umfassen die Strukturen, Strategien und Verfahren, die sich direkt auf einzelne elektronische Anwendungen beziehen – zum Beispiel Systeme zur Verwaltung von Forderungen, Vorräten, Lohnverrechnung, Beihilfen oder Krediten – und die für die Kontrolle der Datenverarbeitung mit bestimmter Anwendungssoftware konzipiert sind.

Diese Kontrollen dienen in der Regel dazu, Fehler und Unregelmäßigkeiten im Fluss der Informationen durch die IT-Systeme zu verhindern, aufzudecken und zu beheben.

In Bezug auf anwendungsspezifische Kontrollen und die Art und Weise, wie die Information durch die IT-Systeme fließt, lassen sich im Verarbeitungszyklus drei unterschiedliche Phasen unterscheiden:

- Eingabe: die Daten werden genehmigt, aufbereitet und korrekt, vollständig und zeitgerecht in das Anwendungsprogramm eingegeben;
- Verarbeitung: die Daten werden vom Rechner ordnungsgemäß verarbeitet und die Dateien werden korrekt aktualisiert; und
- Ausgabe: die im Anwendungsprogramm erstellten Dateien und Berichte enthalten die tatsächlichen Geschäftsfälle und Vorgänge und stellen die Verarbeitungsergebnisse korrekt dar; die Berichte werden kontrolliert und an die berechtigten User weitergeleitet.

Die anwendungsspezifischen Kontrollen können auch nach ihren Kontrollzielen unterschieden werden, unter anderem in Bezug auf Genehmigung, Vollständigkeit, Richtigkeit und Rechtmäßigkeit der Geschäftsfälle und Informationen. Genehmigungskontrollen dienen zur Überprüfung der Rechtmäßigkeit von Geschäftsfällen und sind eine Maßnahme, mit der sichergestellt werden kann, dass es sich bei den erfassten Geschäftsfällen um Vorgänge handelt, die im betreffenden Zeitraum tatsächlich stattgefunden haben. Vollständigkeitskontrollen dienen zur Überprüfung, ob alle rechtmäßigen Geschäftsfälle erfasst und ordnungsgemäß zugeordnet sind. Mit Richtigkeitskontrollen wird

überprüft, ob die Geschäftsfälle korrekt erfasst und alle Daten und Datenelemente fehlerfrei eingegeben wurden. Ist jedoch die Kontrolle der Integrität der Datenverarbeitung und der Dateien unzulänglich, ist der Nutzen jeder der obgenannten anwendungsspezifischen Kontrollen in Frage gestellt und die Gefahr des Auftretens von nicht genehmigten Geschäftsfällen und unvollständigen oder fehlerhaften Datensätzen entsprechend erhöht.

Anwendungsspezifische Kontrollen umfassen programmierte Kontrollmaßnahmen, wie automatisierte Datenaufbereitungsfunktionen, ebenso wie die manuelle Weiterbearbeitung von elektronisch generierten Unterlagen wie die Revision von Berichten, in denen zurückgewiesene oder ungewöhnliche Positionen identifiziert werden.

### **Wechselwirkung zwischen allgemeinen und anwendungsspezifischen Kontrollen bei IT-Systemen**

Die Wirksamkeit von anwendungsspezifischen Kontrollen hängt wesentlich von der Wirksamkeit der allgemeinen Kontrollen ab. Wenn die allgemeinen Kontrollen schwach sind, sinkt die Zuverlässigkeit der einzelnen anwendungsspezifischen Kontrollen erheblich. Ohne wirksame allgemeine Kontrollen werden die anwendungsspezifischen Kontrollen unter Umständen auf Grund von Nichtbeachtung, Umgehung oder Abänderungen wirkungslos. Eine logische Kontrolle etwa, die den Nutzer daran hindern soll, eine unlogische Anzahl von Arbeitsstunden in das Lohnverrechnungssystem einzugeben (z.B. mehr als 24 Stunden pro Tag), kann eine wirkungsvolle, anwendungsspezifische Kontrolle sein. Diese Kontrolle verliert jedoch ihre Zuverlässigkeit, wenn die allgemeinen Kontrollen unbefugte Programmänderungen zulassen, die es möglich machen, einzelne Zahlungen von der logischen Kontrolle auszuschließen.

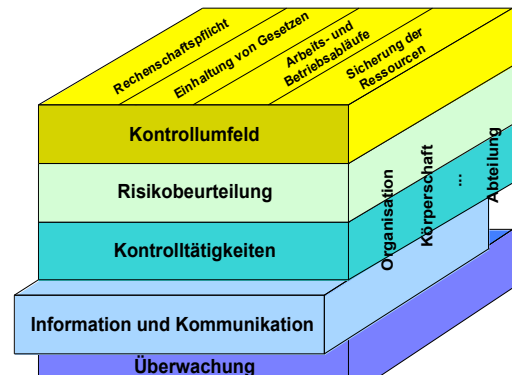
Während die grundlegenden Kontrollziele unverändert bleiben, müssen die Kontrollen selbst ständig weiterentwickelt werden, um dem rapiden Wandel im Bereich der Informationstechnologie Rechnung zu tragen und die Wirksamkeit der Kontrollen zu gewährleisten. Veränderungen wie die zunehmende Abhängigkeit von Netzwerken, leistungsfähigere Computer, durch welche die Verantwortung für die Datenverarbeitung beim Endanwender liegt, elektronische Handelssysteme und das Internet beeinflussen die Art und Umsetzung spezifischer Kontrollmaßnahmen.

Für weitere Informationen zum Thema IT-Kontrollen wird auf die Information Systems Audit and Control Association (ISACA), insbesondere die ISACA Control Objectives for Information and related Technology – ISACA Kontrollziele für Informations- und verwandte Technologien (COBIT), und den Leitfaden des INTOSAI Komitees für die IT-Prüfung verwiesen.

### **Beispiele**

Der Leser wird auf die im Anhang enthaltenen Beispiele zu jedem der Ziele und den Komponenten eines internen Kontrollsystems verwiesen.

## 2.4 Information und Kommunikation



Information und Kommunikation sind für die Umsetzung aller internen Kontrollziele von wesentlicher Bedeutung.

### Information

Eine Voraussetzung für die Bereitstellung zuverlässiger und zweckdienlicher Informationen ist die sofortige Aufzeichnung und ordnungsgemäße Zuordnung von Geschäftsfällen und anderen Vorgängen. Einschlägige Information sollte identifiziert, erfasst und den Mitarbeitern rechtzeitig in einer Form weitergeleitet werden, dass diese ihrer internen Kontrollfunktion und anderen Aufgaben nachkommen können (rechtzeitige Information der richtigen Stellen). Daher sollte das interne Kontrollsystem als solches ebenso wie alle Geschäftsfälle und Vorgänge vollständig dokumentiert werden.

Mit Hilfe der Informationssysteme werden Berichte erstellt, die Betriebs-, Finanz- und Geschäftsdaten und relevante Informationen in Bezug auf die Einhaltung von Gesetzen und Vorschriften enthalten, und den Führungskräften als Basis für das Management der Körperschaft und der Kontrolle der internen Arbeits- und Betriebsabläufe dienen. Die Reichweite der Systeme beschränkt sich nicht auf intern generierte Daten, sondern umfasst auch signifikante externe Ereignisse, Tätigkeiten und Bedingungen, die für den Entscheidungsfindungsprozess und das Berichtswesen von Bedeutung sind.

Die Qualität der Information beeinflusst den Entscheidungsprozess im Management. Daher muss angemessene, zeitgerechte, aktuelle und korrekte Information in zugänglicher Form bereitgestellt werden.

Information und Kommunikation sind für die Umsetzung aller internen Kontrollziele von wesentlicher Bedeutung. Eines der internen Kontrollziele, zum Beispiel, besteht in der Erfüllung der öffentlichen Rechenschaftspflicht. Dieses Ziel wird erreicht, indem zuverlässige und zweckdienliche Finanz- und Managementinformationen erstellt und bereitgehalten werden und diese in angemessener Weise zeitgerecht veröffentlicht werden. Information und Berichterstattung über die operativen Ergebnisse einer Organisation schaffen die Möglichkeit, Arbeits- und Betriebsabläufe am Maßstab ihrer Planmäßigkeit, Ethik, Wirtschaftlichkeit, Effizienz und Wirksamkeit zu beurteilen. Häufig erfordern Gesetze und Vorschriften die Offenlegung bestimmter Informationen.

Um eine wirksame interne Kontrolle und das Erreichen der Kontrollziele sicherzustellen werden auf allen Ebenen einer Organisation Informationen benötigt. Daher muss ein Katalog zweckdienlicher, zuverlässiger und einschlägiger Informationen festgelegt werden, die erfasst und den Mitarbeitern rechtzeitig und in einer Form weiterzuleiten sind, dass diese ihre interne Kontrollfunktion und andere Aufgaben erfüllen können. Eine Voraussetzung für die Bereitstellung zuverlässiger und zweckdienlicher Informationen ist die sofortige Aufzeichnung und ordnungsgemäße Zuordnung von Geschäftsfällen und Vorgängen.

Um dem Management zweckdienliche und einschlägige Information als Grundlage für Entscheidungsprozesse und zur Steuerung der Arbeits- und Betriebsabläufe bereitstellen zu können, müssen Geschäftsfälle und andere signifikante Vorgänge sofort aufgezeichnet werden. Dies gilt für den gesamten Vorgang bzw. die gesamte Abwicklungsphase eines Geschäftsfalles einschließlich der Anbahnung und Genehmigung, aller Verfahrensabschnitte, sowie die abschließende Zuordnung in zusammenfassenden Aufzeichnungen. Ebenso gilt dies in Bezug auf die umgehende Aktualisierung aller Dokumentationsunterlagen, um sie auf dem letztgültigen Stand zu halten.

Eine ordnungsgemäße Zuordnung von Geschäftsfällen und Vorgängen ist erforderlich, um sicherzustellen, dass dem Management zuverlässige Informationen zur Verfügung stehen. Dieser Prozess umfasst die systematische Aufbereitung, Kategorisierung und Formatierung von Informationen, die für die Erarbeitung von Berichten, Zeitplänen und Jahresabschlüssen herangezogen werden.

Mit Hilfe der Informationssysteme werden Berichte erstellt, die Betriebs-, Finanz- und Geschäftsdaten sowie Information in Bezug auf die Einhaltung von Gesetzen und Vorschriften enthalten und die dem Management als Basis für die Kontrolle der Arbeits- und Betriebsabläufe dienen. In den IT-Systemen werden nicht nur intern generierte Daten quantitativ und qualitativ verarbeitet, sondern auch externe Ereignisse, Tätigkeiten und Bedingungen, die für die Entscheidungsprozesse und das Berichtswesen von Bedeutung sind.

Angemessene Management-Entscheidungen hängen von der Qualität der verfügbaren Information ab. Daher muss die bereitgestellte Information:

- angemessen (ist die erforderliche Information verfügbar?);
  - zeitgerecht (ist sie verfügbar, wenn sie gebraucht wird?);
  - aktuell (ist sie am letzten verfügbaren Stand?);
  - korrekt (ist sie fehlerfrei?);
  - zugänglich (ist sie für die betreffenden Personen leicht zugänglich?);
- sein.

Um eine hohe Qualität des Informations- und Berichtswesens zu gewährleisten, die Durchführung der internen Kontrollen und Aufgaben zu erleichtern und die Überwachung effizienter und wirkungsvoller zu gestalten, sollte das interne Kontrollsystem als solches ebenso wie alle Geschäftsfälle und Vorgänge vollständig und transparent dokumentiert werden (z.B. Ablaufdiagramme und Berichte). Diese Dokumentation sollte jederzeit einsehbar sein.

Die Dokumentation des internen Kontrollsystems sollte eine Beschreibung der Organisationsstruktur und Strategien sowie der Aufgabenbereiche und der jeweils geltenden Zielsetzungen und Kontrollverfahren enthalten. Eine Organisation muss über schriftliche Unterlagen verfügen, welche die Komponenten des internen Kontrollverfahrens einschließlich der Organisations- und Kontrollziele beschreiben.

Der Umfang der Dokumentation des internen Kontrollsystems hängt von Faktoren wie der Größe und der Komplexität der betreffenden Körperschaft ab.

## Kommunikation

Wirksame Kommunikation sollte in jeder Richtung stattfinden, von oben nach unten, quer durch alle Ebenen und von unten nach oben sowie alle Teilbereiche und die gesamte Struktur durchdringen.

Das oberste Management sollte allen Mitarbeitern eindeutig und klar vermitteln, dass die Kontrollaufgaben ernst zu nehmen sind. Die Mitarbeiter sollten ihre Rolle im internen Kontrollsystem verstehen und sich der Zusammenhänge der einzelnen Aufgaben mit den Tätigkeiten anderer Mitarbeiter bewusst sein.

Ebenso muss für eine wirksame Kommunikation nach außen gesorgt sein.

Information bildet die Grundlage von Kommunikation. Diese muss die Erwartungen der betroffenen Gruppen und Einzelpersonen erfüllen und sie in die Lage versetzen, die ihnen obliegenden Aufgaben wirksam zu erfüllen. Wirksame Kommunikation sollte in jeder Richtung stattfinden, von oben nach unten, quer durch alle Ebenen der Organisation und von unten nach oben sowie alle Teilbereiche und die gesamte Struktur durchdringen.

Einer der wichtigsten Kommunikationskanäle ist der zwischen dem Management und dessen Mitarbeitern. Das Management muss in Bezug auf die operativen Ergebnisse, Entwicklungen, Risiken und das Funktionieren der internen Kontrolle sowie andere wichtige Ereignisse und Themen am jeweils aktuellen Stand gehalten werden. Umgekehrt obliegt es dem Management, die Mitarbeiter klar darüber zu informieren, welche Informationen benötigt werden sowie Feedback und die entsprechenden Anleitungen zu geben. Auch die Verhaltensgrundsätze sollten vom Management im Detail und zielgerichtet kommuniziert werden. Dies beinhaltet auch eine klare Darstellung der dem internen Kontrollansatz zu Grunde liegenden Philosophie und Strategie und eine Beschreibung der Kompetenzverteilung.

Die Kommunikationsmaßnahmen sollten so ausgelegt sein, dass sie das Bewusstsein für die Bedeutung und Sachdienlichkeit wirksamer interner Kontrollen erhöhen, das Maß der Risikobereitschaft und der Risikotoleranz der Körperschaft verständlich machen, und den Mitarbeitern ihre Aufgaben und Zuständigkeiten in der Durchführung und Unterstützung der einzelnen Aspekte der internen Kontrolle bewusst machen.

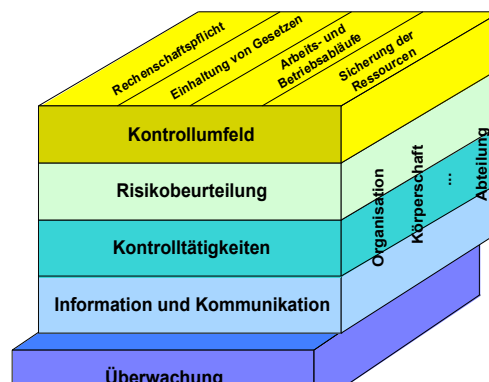
Neben internen Kommunikationsmaßnahmen sollte vom Management auch sichergestellt werden, dass geeignete Kommunikationsmittel zum Austausch von Information mit externen Stellen zur Verfügung stehen, da externe Kommunikationskanäle unter Umständen sehr bedeutsame Informationen für die Erreichung der Organisationsziele liefern.

Es obliegt dem Management, auf Basis der aus internen und externen Kanälen gewonnenen Informationen die erforderlichen Maßnahmen zu treffen und rechtzeitig weitere Schritte zu setzen.

### **Beispiele**

Der Leser wird auf die im Anhang enthaltenen Beispiele zu jedem der Ziele und den Komponenten eines internen Kontrollsystems verwiesen.

## 2.5 Überwachung



Interne Kontrollsysteme sollten überwacht werden, um die Qualität der Systemperformance im Zeitablauf zu beurteilen. Die Überwachung erfolgt durch Routinetätigkeiten, zusätzliche Evaluierungen oder eine Kombination der beiden.

### (1) Laufende Überwachung

Die laufende Überwachung der internen Kontrollen ist in die regulären Arbeits- und Betriebsabläufe einer Körperschaft eingebunden. Sie umfasst regelmäßige, vom Management und den mit der Überwachung betrauten Instanzen durchgeführte Maßnahmen und Tätigkeiten, die von den Mitarbeitern im Rahmen der Erfüllung ihrer Aufgaben ausgeübt werden.

Die laufende Überwachung erstreckt sich auf jede der im internen Kontrollsystem enthaltenen Teilkomponenten und beinhaltet Maßnahmen zur Verhinderung ordnungswidriger, unethischer, verschwenderischer, unzweckmäßiger und unwirksamer interner Kontrollen.

### (2) Zusätzliche Evaluierungen

Umfang und die Häufigkeit zusätzlicher Evaluierungen hängen in erster Linie von einer Beurteilung der Risiken und der Wirksamkeit der laufenden Überwachungsverfahren ab.

Spezielle, zusätzliche Evaluierungsprozesse dienen zur Beurteilung der Wirksamkeit des internen Kontrollsystems und zur Sicherstellung, dass mit den vorgegebenen Methoden und Verfahren die erwünschten Ergebnisse der internen Kontrollen erzielt werden. Über Mängel in den internen Kontrollsystemen sollte

der zuständigen Managementebene Meldung erstattet werden.

Die Überwachung sollte sicherstellen, dass die Prüfergebnisse und Empfehlungen in geeigneter Weise und umgehend umgesetzt werden.

Durch die Überprüfung der internen Kontrollen soll sichergestellt werden, dass die Kontrollen ihre beabsichtigte Funktion erfüllen und geänderten Bedingungen in angemessener Form Rechnung tragen. Des Weiteren dient die Überwachung der Beurteilung, ob die von der Aufgabenstellung der Körperschaft bestimmten und der Konzeption der internen Kontrolle zu Grunde liegenden allgemeinen Zielsetzungen erreicht werden. Diese Beurteilung erfolgt durch laufende Überwachung, zusätzliche Evaluierungen, oder eine Kombination dieser beiden Verfahren und dient zur Sicherstellung, dass die internen Kontrollen auf allen Ebenen und in allen Bereichen der Körperschaft laufend durchgeführt werden und ihre Ziele erreichen. Die Überwachung der internen Kontrollen sollte klar getrennt sein von der Überprüfung der Arbeits- und Betriebsabläufe einer Organisation, die, wie in Abschnitt 2.3 beschrieben, Teil der internen Kontrollen bildet.

Die laufende Überwachung der internen Kontrollen erfolgt im Rahmen der regulären Arbeits- und Betriebsabläufe einer Organisation. Die laufende Überwachung ist ein ständiger, zeitnaher Prozess; sie reagiert dynamisch auf geänderte Bedingungen und ist eng in die Arbeits- und Betriebsabläufe der Organisation eingebettet. Daher ist sie wirksamer als zusätzliche Evaluierungen; dadurch sind die entsprechenden Korrekturen potenziell weniger kostspielig. Im Vergleich zu zusätzlichen Evaluierungen, die eine rein nachträgliche Maßnahme darstellen, können Probleme durch die laufende Überwachung häufig schneller geortet werden.

Umfang und Häufigkeit der zusätzlichen Evaluierungen sollte in erster Linie von der Einschätzung der Risiken und der Wirksamkeit der laufenden Überwachungsverfahren abhängen. Bei dieser Einschätzung sollte die Organisation die folgenden Faktoren mit in Betracht ziehen: Art und Umfang der durch interne und externe Umstände verursachten Veränderungen und die damit zusammenhängenden Risiken; die Kompetenz und Erfahrung der mit der Umsetzung der Risikostrategien und der entsprechenden Kontrollen betrauten Mitarbeiter; sowie die Ergebnisse der laufenden Überwachung. Bei zusätzlichen Evaluierungen können sich auch auf einen bestimmten Zeitpunkt fokussierte Überprüfungen der Wirksamkeit der Kontrollen als nützlich erweisen. Zusätzliche Evaluierungen können in Form von Selbstbewertungen, einer Überprüfung der Kontrollkonzeption oder durch Feststellung der Wirksamkeit der Kontrollen durch Erprobung durchgeführt werden. Zusätzliche Evaluierungen können auch von den ORKB oder durch externe Prüfer oder interne Revisoren durchgeführt werden.

In der Regel wird eine Kombination von laufenden Überwachungen und zusätzlichen Evaluierungen dazu beitragen, dass die Wirksamkeit der internen Kontrollen langfristig gesichert ist.

Alle Mängel, die im Rahmen der laufenden Überwachung oder zusätzlicher Evaluierungen festgestellt werden, sollten an die für die erforderlichen Maßnahmen zuständigen Stellen gemeldet werden. Der Begriff „Mängel“ bezieht sich hier auf Umstände, welche die Körperschaft in Bezug auf das Erreichen ihrer allgemeinen Ziele behindern können. Ein Mangel kann daher eine vermutete, potenzielle oder reale Unzulänglichkeit sein. Er kann aber auch in einer noch nicht wahrgenommenen Möglichkeit zur Verbesserung der internen Kontrollen bestehen, welche die Wahrscheinlichkeit erhöhen würde, dass die Körperschaft ihre allgemeinen Ziele erreicht.

Ein entscheidender Faktor in diesem Zusammenhang ist, dass die über Mängel in internen Kontrollen erforderliche Information an die richtigen Stellen weitergeleitet wird. Dazu sollten Protokolle erstellt werden, in denen festgelegt ist, welche Informationen auf welchen Ebenen für wirksame Entscheidungsprozesse gebraucht werden. Die Protokolle tragen dem allgemeinen Grundsatz Rechnung, dass Führungskräfte über die Tätigkeit und das Verhalten der Mitarbeiter in ihrem jeweiligen Verantwortungsbereich informiert werden sollten. Ebenso sollte den Führungskräften die für die Erreichung spezifischer Ziele maßgebliche Information zur Kenntnis gebracht werden.

Im Rahmen der Arbeits- und Betriebsabläufe erstellte Informationen werden in der Regel durch die üblichen Kanäle weitergeleitet, das heißt an die für die jeweilige Aufgabe verantwortliche Stelle bzw. eine mindestens eine Stufe über der betreffenden Ebene liegende Führungsebene. Allerdings sollten auch zusätzliche Kommunikationskanäle für die Weiterleitung sensibler Informationen, wie etwa in Bezug auf unrechtmäßige oder unzulässige Handlungen, zur Verfügung stehen.

Die Überwachung der internen Kontrollen sollte Strategien und Verfahren beinhalten, die sicherstellen, dass die Ergebnisse von Prüfungen, Revisionen und sonstigen Überprüfungen in angemessener Form und umgehend umgesetzt werden. Die Führungskräfte müssen (1) die Ergebnisse von Prüfungen, Revisionen und sonstigen Überprüfungen, einschließlich der von Revisoren und Prüfern vorgelegten Mängelberichte und Empfehlungen, umgehend bewerten, (2) in Reaktion auf die Revisions- und Prüfungsergebnisse und Empfehlungen zu ergreifende, angemessene Maßnahmen festlegen, und (3) innerhalb eines festgelegten Zeitraums alle Korrekturen und Maßnahmen zur Bereinigung der ihnen zur Kenntnis gebrachten Probleme ergreifen und durchführen.

Der Problemlösungsprozess beginnt mit der Unterbreitung der Prüfungs- oder Revisionsergebnisse beim Management, und er ist erst abgeschlossen, wenn Maßnahmen getroffen wurden, durch welche (1) die festgestellten Mängel behoben, (2) Verbesserungen erzielt, oder (3) erwiesen wird, dass die Ergebnisse und Empfehlungen keine vom Management zu setzenden Maßnahmen erfordern.

## **Beispiele**

Der Leser wird auf die im Anhang enthaltenen Beispiele zu jedem der Ziele und den Komponenten eines internen Kontrollsystems verwiesen.

### 3 Aufgaben und Zuständigkeiten

Jede in einer Organisation tätige Person trägt im Rahmen der internen Kontrollen ein bestimmtes Maß an Verantwortung:

|                   |   |
|-------------------|---|
| Führungskräfte    | sind direkt verantwortlich für alle Tätigkeiten einer Organisation, unter anderem für die Konzeption, die Einrichtung, die Aufsicht über das ordnungsgemäße Funktionieren, die Führung und die Dokumentation des internen Kontrollsystems. Ihre Zuständigkeiten variieren je nach ihrer Funktion und den Merkmalen der Organisation.  |
| Interne Revisoren | prüfen die Wirksamkeit des internen Kontrollsystems mittels Evaluierungen, unterbreiten Empfehlungen und tragen dadurch zu dessen nachhaltiger Wirksamkeit bei. In dieser Funktion spielen sie eine wesentliche Rolle zur Sicherung wirksamer interner Kontrollen. Im Unterschied zu den Führungskräften tragen sie jedoch nicht die primäre Verantwortung für die Konzeption, die Einrichtung, das ordnungsgemäße Funktionieren, die Führung und die Dokumentation des internen Kontrollsystems. |
| Mitarbeiter       | sind an der Durchführung der internen Kontrollen beteiligt. Interne Kontrollen sind explizit und implizit Teil der Aufgaben jedes Mitarbeiters. Jeder Mitarbeiter hat bestimmte Aufgaben bei der Durchführung der Kontrollen und sollte dafür verantwortlich sein, dass Probleme in den Arbeits- und  |

Betriebsabläufen, die Nichteinhaltung von Verhaltensnormen, oder Verletzungen strategischer Vorgaben gemeldet werden.

Externe Stellen spielen im internen Kontrollprozess ebenfalls eine wichtige Rolle. Sie können zum Erreichen der Organisationsziele beitragen oder wichtige Informationen zur Umsetzung der internen Kontrollen liefern. Sie tragen jedoch keine Verantwortung für die Konzeption, die Einrichtung, das ordnungsgemäße Funktionieren, die Führung und die Dokumentation des internen Kontrollsystems der Organisation.

Oberste  
Rechnungskontrollbehörden  
(ORKB)

fördern und unterstützen die Einrichtung wirksamer interner Kontrollen in öffentlichen Verwaltungseinrichtungen. Die Beurteilung des internen Kontrollsystems ist ein wesentlicher Faktor für die Durchführung von Rechtskonformitäts-, Rechnungs- und Geschäftsprüfungen durch die ORKB. Ihre Ergebnisse und Empfehlungen werden den jeweiligen involvierten und interessierten Stellen und Personenkreisen zur Kenntnisnahme weitergeleitet.

Externe Prüfer

werden in manchen Ländern mit der Prüfung bestimmter öffentlicher Verwaltungseinrichtungen betraut. Diese und ihre Fachorgane sollten für Beratungen und Empfehlungen im Bereich interne Kontrolle zur Verfügung stehen.

Gesetzgeber und  
Aufsichtsbehörden

legen die im Hinblick auf interne Kontrollen geltenden Vorschriften und Richtlinien fest. Sie sollten zum allgemeinen Verständnis interner Kontrollen beitragen.

|                     |  |
|---------------------|--|
| Sonstige Beteiligte | arbeiten mit den Organisationen zusammen (Begünstigte, Lieferanten, etc.) und liefern Information hinsichtlich der Erreichung der Ziele. |
|---------------------|--|

Die interne Kontrolle wird in erster Linie durch die innerhalb der jeweiligen Körperschaft verantwortlichen Personengruppen wie Führungskräfte, interne Revisoren und andere Mitarbeiter umgesetzt. Maßnahmen und Tätigkeiten externer involvierter und interessierter Stellen und Personenkreise haben jedoch ebenfalls Auswirkungen auf das Funktionieren des internen Kontrollsystems.

### **Führungskräfte**

Alle Mitarbeiter einer Organisation erfüllen bei der Durchführung interner Kontrollen wichtige Aufgaben. Die Gesamtverantwortlichkeit für die Konzeption, die Einrichtung, die Durchführung und die Aufsicht über das ordnungsgemäße Funktionieren sowie die laufende Pflege und die Dokumentation des internen Kontrollsystems liegt jedoch bei den Führungskräften. Die Managementstrukturen können Ausschüsse und Revisionskomitees umfassen, die jeweils unterschiedliche Aufgaben und Zusammensetzungen aufweisen und in den verschiedenen Ländern unterschiedlichen gesetzlichen Bestimmungen unterliegen.

### **Interne Revisoren**

Das Management richtet häufig eine interne Revisionsstelle als Teil des internen Kontrollsystems ein, die zur Überwachung der Wirksamkeit der internen Kontrollen beiträgt. Die internen Revisoren berichten regelmäßig über das Funktionieren der internen Kontrollen, wobei der Evaluierung der Konzeption und der operativen Abläufe der internen Kontrollen hohe Bedeutung zukommt. Sie berichten über die Stärken und Schwächen und geben Empfehlungen in Bezug auf mögliche Verbesserungen der internen Kontrollen. Ihre Unabhängigkeit und Objektivität sollte jedoch garantiert sein.

Daher sollte die interne Revision eine unabhängige, objektive Funktion der Qualitätssicherung und Beratung sein, die zur Verbesserung der Arbeits- und Betriebsabläufe der jeweiligen Organisation beiträgt und damit die Wertschöpfung erhöht. Durch einen systematischen und gründlichen Bewertungsansatz trägt die interne Revision zur Erreichung der Organisationsziele bei und verbessert die Effizienz des Risikomanagements sowie der Verfahren der Kontrolle und der Corporate Governance.

Interne Revisoren können im Bereich interne Kontrolle zwar eine wertvolle Qualitätssicherungs- und Beratungsfunktion ausüben, doch sollte der interne Revisor nicht als Ersatz für ein starkes internes Kontrollsystem betrachtet werden.

Um die Wirksamkeit der internen Revisionsfunktion zu gewährleisten, ist es von wesentlicher Bedeutung, dass die internen Revisoren

unabhängig vom Management sind, ihre Arbeit unparteiisch, korrekt und ehrlich verrichten, und dass sie ihre Ergebnisse direkt an die höchste Verantwortungsebene in der Organisation berichten. Dies erlaubt den Revisoren, in der Beurteilung der internen Kontrollen eine unparteiische Stellung einzunehmen und die auf die Korrektur von Mängeln abzielenden Vorschläge objektiv darzustellen. Zur fachlichen Orientierung sollten interne Revisoren das Professional Practices Framework (PPF) des Institute of Internal Auditors (IIA) einschließlich der Definition, der berufsethischen Grundsätze, der Standards und der Praktischen Ratschläge zu Rate ziehen. Darüber hinaus sollten interne Revisoren dem Pflichten- und Verhaltenskodex der INTOSAI folgen.

Über ihre Aufgabe zur Überwachung der internen Kontrollen einer Körperschaft hinaus können kompetente interne Revisoren durch gezielte Unterstützung der externen Prüfer zum effizienten Ablauf externer Prüfungen beitragen. Art, Umfang und Zeitaufwand der externen Prüfverfahren ist von der aus Sicht des externen Prüfers verlässlichen Arbeit des internen Revisors abhängig.

### **Mitarbeiter**

Angestellte und andere Mitarbeiter sind ebenfalls an der Durchführung der internen Kontrollen beteiligt. Es ist in der Regel dieser an vorderster Front stehende Personenkreis, der die Kontrollen im Rahmen der laufenden Tätigkeit durchführt und überprüft, Anwendungsfehler korrigiert und Probleme erkennt, denen am besten durch Kontrollen begegnet werden kann.

### **Externe Stellen**

Externe Stellen wie externe Prüfer (einschließlich der ORKB), Gesetzgeber und Aufsichtsbehörden und andere Stellen bilden die zweite große Hauptgruppe der maßgeblich an den internen Kontrollen beteiligten Personen. Sie können zum Erreichen der Organisationsziele beitragen oder wichtige Informationen zur Umsetzung der internen Kontrollen liefern, tragen jedoch keine Verantwortung für die Konzeption, die Einrichtung, die Durchführung und das ordnungsgemäße Funktionieren oder die Dokumentation des internen Kontrollsystems der Organisation.

### **ORKB und externe Prüfer**

Zu den Aufgaben externer Stellen, insbesondere der externen Prüfer und der ORKB, zählen die Beurteilung des Funktionierens des internen Kontrollsystems und die Berichterstattung über die Ergebnisse der Prüfungen an das Management. Es ist jedoch das von den jeweiligen Stellen ausgeübte Mandat, das den dabei jeweils eingenommenen Blickwinkel bestimmt.

Die folgenden Aspekte sollten vom Prüfer bei der Bewertung der internen Kontrollen in Betracht gezogen werden:

- Festlegung des Stellenwertes des Risikos und der Risikosensitivität der zu bewertenden Kontrollen;

- Beurteilung der Gefahr für einen Missbrauch von Ressourcen und für ein Verfehlen der Ziele in Bezug auf ethische, wirtschaftliche, effiziente und wirksame Abläufe, oder von Versäumnissen in der Erfüllung der Rechenschaftspflicht sowie der Gefahr der Nichteinhaltung von Gesetzen und Vorschriften;
- Identifizierung und Verstehen der jeweils relevanten Kontrollen;
- Feststellung von bereits vorhandenem Wissen über die Wirksamkeit von Kontrollen;
- Bewertung der Angemessenheit der Kontrollkonzeption;
- Feststellung der Wirksamkeit der Kontrollen durch Erprobung;
- Berichterstattung über die Beurteilung der internen Kontrollen und Erörterung der erforderlichen Verbesserungsmaßnahmen.

Die ORKB hat außerdem ein rechtmäßiges Interesse sicherzustellen, dass, soweit erforderlich, leistungsstarke interne Revisionsstellen bestehen. Diese Stellen sind ein wichtiges Element der internen Kontrolle, da sie zur laufenden Qualitätssicherung und Verbesserung der Arbeits- und Betriebsabläufe beitragen. In manchen Ländern sind die internen Revisionsstellen möglicherweise nicht unabhängig genug, zu schwach oder nicht vorhanden. In diesen Fällen sollte die ORKB, wenn möglich, mit Unterstützung und Rat zur Entwicklung und zum Aufbau derartiger Einrichtungen beitragen und die Unabhängigkeit interner Revisionsstellen sicherstellen. Diese Unterstützung kann unter anderem die folgenden Maßnahmen umfassen: Abordnung oder Ausleihung von Personal, Vortragstätigkeit, Bereitstellung von Trainingsmaterial, und Entwicklung von methodischem Grundsatzmaterial und Arbeitsprogrammen. Durch diese Maßnahmen darf die Unabhängigkeit der ORKB oder der externen Prüfer nicht in Frage gestellt werden.

Die Oberste Rechnungskontrollbehörde muss darüber hinaus ein gutes Klima der Zusammenarbeit mit den internen Revisionsstellen schaffen, sodass Erfahrungen und Wissen ausgetauscht und die Arbeit jedes Einzelnen ergänzt und vervollständigt werden kann. Eine Möglichkeit, dieses Arbeitsverhältnis zu fördern, besteht darin, zweckdienliche Feststellungen der internen Revision in den Prüfbericht einzubeziehen und entsprechend zu würdigen. Die ORKB sollte Verfahren für die Bewertung der Arbeit der internen Revisionsstellen entwickeln, um feststellen zu können, inwieweit die Revisionsergebnisse zuverlässig sind. Eine leistungsstarke interne Revisionsstelle kann die Prüftätigkeit der ORKB erleichtern und zur Vermeidung unnötigen Doppelaufwands beitragen. Die ORKB sollte sicherstellen, dass ihr die internen Revisionsberichte und die diesen zu Grunde liegenden Arbeitsunterlagen sowie die für eine Umsetzung der Prüfungsfeststellungen erforderlichen Daten zur Verfügung gestellt werden.

Darüber hinaus sollte die ORKB im öffentlichen Sektor eine beispielhafte Rolle vorgeben, indem sie in der eigenen Organisationsstruktur ein internes Kontrollsystem verankert, das den in diesen Richtlinien enthaltenen Grundsätzen entspricht.

Nicht nur die ORKB, sondern auch die externen Prüfer tragen wesentlich dazu bei, dass die internen Kontrollziele einer Organisation, insbesondere in Bezug auf die „Erfüllung der Rechenschaftspflicht“ und die „Sicherung der Ressourcen“ erreicht werden. Von externen Prüfern erstellte Prüfberichte zu Finanz- und Geschäftsberichten sind ein integraler Bestandteil der Rechenschaftslegung und der Good Governance. Sie bilden für externe involvierte oder interessierte Stellen und Personengruppen neben Information über die Geschäftstätigkeit jedenfalls einen wichtigen Maßstab zur Ergebnisbewertung.

### **Gesetzgeber und Aufsichtsbehörden**

Gesetze tragen dazu bei, eine Basis für das allgemeine Verständnis und einen einheitlichen Ansatz in Bezug auf die Definition und die Ziele interner Kontrollen zu schaffen. Im Wege der Gesetzgebung ist es möglich, strategische Grundsätze vorzugeben, die intern und extern involvierten Stellen und Personengruppen als Vorgabe für die Wahrnehmung von Aufgaben und Zuständigkeiten im Rahmen des internen Kontrollsystems dienen.

## **Anlage 1 Beispiele**

**Erfüllung der Rechenschaftspflicht Beispiel (1)** : Ein für die sichere Beförderung mit dem Schiff verantwortliches Ministerium ist in mehrere Abteilungen aufgegliedert. Die Abteilungen sind zuständig für den Lotsendienst, das Ausbaken, die Prüfung der Qualität des Wassers, die Förderung der Schifffahrt, Investitionen in die und Instandhaltung der Infrastruktur (Brücken, Deiche, Kanäle und Schleusen).

| Kontrollumfeld  | Risikobeurteilung  | Kontrolltätigkeiten  | Information & Kommunikation   | Überwachung   |
|---|--|--|---|---|
| Der für jede Abteilung bestimmte Leiter muss den allgemeinen Manager des Ministeriums informieren. Die Abteilungsleiter verfügen über die richtige Fachkompetenz und die erforderlichen Machtbefugnisse um gewisse Entscheidungen treffen zu können. Sie unterschreiben alle eine berufsständische Ordnung. | Etwaige Risiken sind der Zusammenstoß von Schiffen, toxische oder Ölverschmutzung und Deichbrüche. Falls das Ministerium durch Nachlässigkeit einen Unfall herbeiführt, kann es dafür völlig haftbar gemacht werden. | Etwaige Kontrolltätigkeiten sind die Führung von Schiffen durch zuverlässige Lotsen, das Ausbaken und das Ausbojen, die visuelle Luftüberwachung und die Überprüfung der Wasserqualität. | Die Information und Kommunikation für diese Situation umfasst etwa die Berichterstattung über Zusammenstöße um andere Schiffe zu warnen, das Informieren über die Wetterlage und die Veröffentlichung der Namen der Verschmutzer und die damit verbundenen Sanktionen, und die Maßnahmen zur Beseitigung der Verschmutzung. | Die Zahl von Zusammenstößen und Umweltverstößen muss verfolgt werden, ebenso wie die Ergebnisse der Probeentnahmen und ein Vergleich mit anderen Ländern und mit historischen Daten. Diese Kontrollprüfungen können zur Verbesserung der Wirksamkeit und der Zweckmäßigkeit der Lotsendienste für die Schifffahrt, des Ausbakens, der Überwachungen sowie der Probeentnahmen beitragen. |

**Erfüllung der Rechenschaftspflicht Beispiel (2)** : Der Abteilungsleiter für Sport setzte im Vorjahr das Ziel dass die sportliche Betätigung in den kommenden Jahren um 15 % steigen würde.

| Kontrollumfeld   | Risikobeurteilung  | Kontrolltätigkeiten  | Information & Kommunikation  | Überwachung  |
|--|--|--|--|--|
| Die Verwaltung verließ sich auf den guten Ruf des Abteilungsleiters und berief nicht die üblichen Versammlungen ein um seine Fortschritte zu überprüfen. | Weil die Zielsetzungen nicht genau definiert sind, besteht das Risiko dass die Ziele nicht erreicht werden. Die Gefahr besteht dass die Berichterstattung nicht zeitnah stattfinden wird, weil der Abteilungsleiter die Berichterstattung verzögern möchte, solange er die 15 % Zielsetzung nicht erreicht hat. Überdies wurde nicht erklärt auf welche Weise die Zunahme um 15 % gemessen werden sollte. Er kann also behaupten, dass die Zahl von Sportlern zugenommen hat, oder die Stundenzahl der sportlichen Betätigung, oder dass sogar die Zahl von Sportzentren oder Sportklubs um 15 % gestiegen ist. Dadurch wird die Qualität der mitgeteilten Informationen erheblich beeinträchtigt. | Dieses Risiko kann verringert werden indem geeignete Linien für die Berichterstattung sowie ein Berichterstattungsmodell das die zu erteilenden Informationen festlegt, eingesetzt werden. | Der Bericht muss rechtzeitig eingereicht werden und mit dem vorgefassten Modell im Einklang sein. Er sollte die Zielsetzungen in Sachen Wachstum angeben, die Art auf die sie gemessen werden und warum sie auf diese Weise gemessen werden. Alle Hintergrundinformationen sollten vorhanden sein. | Die Feststellung, ob die Berichterstattung den Anforderungen ja oder nein entspricht, welche Informationen erteilt werden und welche Informationen noch fehlen, ist eine Form von Überwachung. |

**Einhaltung von Gesetzen und Richtlinien – Beispiel :** Das Verteidigungsministerium hat die Absicht mittels eines öffentlichen Auftrags neue Jagdflugzeuge zu kaufen und veröffentlicht alle diesbezüglichen Bedingungen und Verfahrensweisen. Alle eingereichten Angebote werden ungeöffnet aufbewahrt bis die Angebotsfrist abläuft. In dem Moment werden in Anwesenheit des verantwortlichen Managers und einiger Beamter alle Angebote geöffnet. Lediglich diese Angebote werden überprüft und verglichen um das beste Angebot auszuwählen.

| Kontrollumfeld   | Risikobeurteilung  | Kontrolltätigkeiten   | Information & Kommunikation  | Überwachung  |
|--|--|---|--|--|
| Das Team das den Ankauf tätigt, setzt sich aus Fachleuten zusammen die ein Dokument unterschreiben woraus hervor geht dass sie mit den Submittenten keine finanzielle oder familiäre Bindung haben. Die verantwortlichen Manager und Beamten unterschreiben dieses Dokument ebenfalls. | Eines der Risiken bei öffentlichen Aufträgen und öffentlichen Verträgen ist <i>insider dealing</i> . Einer der Submittenten könnte ein Vorwissen über die Preise der anderen Angebote haben und aufgrund dieses Vorwissens ein gewinnendes Angebot einreichen, was nicht von selbst die beste Auswahl aus den Angeboten zur Folge hat. Ein anderes Risiko ist die Auswahl des falschen Angebots, was möglicherweise ein neuer öffentlicher Auftrag zur Folge hat weil das andere Angebot den Erwartungen nicht entsprach. Andere Submittenten die sich benachteiligt fühlen, können eine Klage einreichen. | Um die Risiken einzuschränken, sollten Verfahrensweisen entwickelt und angewandt werden die allen Gesetzen und Richtlinien bezüglich der öffentlichen Aufträge entsprechen. | Die Verfahrensweisen bezüglich der Veröffentlichung der Bedingungen des öffentlichen Auftrags, die Bewertung der eingereichten Angebote und die Veröffentlichung des auserwählten Angebots müssen schriftlich festgelegt werden und alle zu treffenden Maßnahmen im Einzelnen darlegen. Bei der Bewertung sollten alle Gründe für die (Nicht) Berücksichtigung eines Angebots belegt werden. | Die interne Kontrolle kann die Dossiers überprüfen und die Beschwerden weiter verfolgen. |

**Methodische, ethische, sparsame, wirtschaftliche und wirksame Verrichtungen – Beispiel (1):** Das Ministerium für Kultur hat die Absicht die Zahl von Museumbesuchern zu steigern. Zu diesem Zweck schlägt es vor neue Museen zu bauen, an jeden Bürger einen Kulturscheck zu verteilen und das Eintrittsgeld zu verbilligen. Um sparsam, wirtschaftlich und wirksam vorzugehen, soll das Management überprüfen ob die Ziele, wie diese formuliert wurden, aufgrund seiner Vorschläge erreicht werden können und wie viel jeder einzelne Vorschlag kosten wird.

| Kontrollumfeld   | Risikobeurteilung   | Kontrolltätigkeiten  | Information & Kommunikation   | Überwachung   |
|--|---|--|---|---|
| Das Ministerium für Kultur hat für eine angepasste Organisationsstruktur zu sorgen, so dass es den Entwurf und den Bau der vorgeschlagenen Museen und deren Planung und Verrichtungen überwachen kann. | Eines der Risiken ist die Tatsache, dass der Museumbesuch nicht zunimmt. Auch wohl möglich ist die Tatsache, dass einige Initiativen fehlschlagen und die Grenze des Budgets überschreiten. Wenn zum Beispiel die Senkung der Ticketpreise nicht eine Zunahme des Museumbesuchs auslöst, bedeutet dies eine Minderung der öffentlichen Einnahmen. Wenn für den Bau von Museen eine geeignete Planung nicht vorliegt und die Erfordernisse für Beleuchtung, Temperatur und Sicherheit nicht in Betracht gezogen werden, kann dies kostspielige Anpassungsarbeiten während der oder nach den Bauarbeiten zur Folge haben. | Mögliche Kontrolltätigkeiten die sich auf die erwähnten Risiken beziehen, sind : eine Budgetprüfung die die gegenwärtige Lage mit den Veranschlagungen vergleicht, Überwachung des Fortgangs der Arbeiten und die Untersuchung der Verantwortlichkeit falls das Budget überschritten wird. | Die Information und Kommunikation für dieses Beispiel setzt sich möglicherweise zusammen aus der Dokumentation der Versammlungen mit den Architekten, der Feuerwehr (Sicherheitsmaßnahmen), den Künstlern und anderen. Die Information und Kommunikation kann auch Berichte enthalten in Bezug auf die Weiterverfolgung des Budgets und den Fortgang der Bauarbeiten. | Überwachung heißt: die Analyse der Verantwortlichkeit im Falle einer Budgetüberschreitung, die sich darauf beziehenden Zinskosten infolge Rückstand in den Arbeiten oder Zahlungen. |

**Methodische, ethische, sparsame, wirtschaftliche und wirksame Verrichtungen – Beispiel (2):** Die Regierung hat die Absicht die Landwirtschaft zu entwickeln und die Lebensqualität auf dem Lande zu verbessern. Sie gewährt Zuschüsse für Bewässerungsanlagen und Schöpfbrunnen.

| Kontrollumfeld  | Risikobeurteilung  | Kontrolltätigkeiten   | Information & Kommunikation  | Überwachung  |
|---|--|---|--|--|
| Die Regierung hat dafür zu sorgen, dass sie über eine geeignete Abteilung verfügt um die Zuschussverrichtungen in die Praxis umzusetzen und zu führen. Auch soll sie das geeignete Umfeld schaffen für eine rechtzeitige und wirksame Erledigung dieses Projekts. | Das Risiko besteht, dass es Vereinigungen skrupellos gelingt Zuschüsse zu bekommen, aber die Mittel nicht für das bewusste Ziel einsetzen. | Mögliche Kontrolltätigkeiten sind: <ul style="list-style-type: none"> <li>- Überprüfung der Qualifizierung der Vereinigungen die Zuschüsse beantragen</li> <li>- Prüfung vor Ort des Fortgangs der Arbeiten und Prüfung der Fortschrittsberichte</li> <li>- Überwachung der Ausgaben der Vereinigungen durch Prüfung deren Rechnungen und durch Verschiebung der Auszahlung (eines Teils) deren Zuschüsse auf den Abschluss der Prüfung.</li> </ul> | Fortschrittsberichte berichten im Detail von den Kosten, der Zahl von gebohrten Schöpfbrunnen und den bewässerten Flächen. | Überwachung kann sein die Weiterverfolgung der Bohrungen der Schöpfbrunnen und der Bewässerungsanlagen und der Vergleich mit anderen ähnlichen Projekten.<br><br>Auch eine Weiterverfolgung des Ertrags der bewässerten Flächen kann in Erwägung gezogen werden. |

**Sicherstellung der Ressourcen – Beispiel (1)** : Das Verteidigungsministerium hat einige Lager, Vorräte und Kraftstoffdepots. Es ist die Politik der Armeeführung diese Vorräte ausschließlich für militärische und nicht für persönliche Zielsetzungen zu verwenden.

| Kontrollumfeld   | Risikobeurteilung   | Kontrolltätigkeiten  | Information & Kommunikation   | Überwachung  |
|--|---|--|---|--|
| Eine wirksame Personalpolitik würde darin bestehen, dass für die Besetzung dieser Lager die richtigen Mitarbeiter angestellt und beibehalten werden. | Das Risiko besteht, dass Leute Waffen stehlen um diese unerlaubt anzuwenden oder zu verkaufen. Auch andere Vorräte wie Kraftstoff könnten gestohlen werden. | Vorbeugende Kontrolltätigkeiten sind das Ummauern oder das Einzäunen der Lager und Depots, oder die Zugänge unter Bewachung mit Hunden stellen. Eine ständige Bestandskontrolle und Verfahrensweisen die besagen, dass Güter nur mit Zustimmung eines hohen Offiziers ausgehändigt werden können, würden auch zur Sicherstellung der Mittel beitragen. | Berichterstattung über beschädigte Zäune und Differenzen bei den Bestandskontrollen. Genehmigung zur Ergänzung der Vorräte und Verfahrensweisen sind ebenfalls zweckdienlich. | Überwachung kann sein eine Inspektion der Zäune, nicht angekündigte Bestandskontrollen, Weiterverfolgung der Vorratsbewegungen oder sogar eine geheime Sicherheitsprüfung. |

**Sicherstellung der Ressourcen – Beispiel (2)** : Große Mengen vertraulicher Informationen sind im Computer in einer Abteilung des Justizministeriums gespeichert. Trotzdem wird der IT-Aufsicht wenig Bedeutung beigemessen und weist die IT-Aufsicht dadurch wichtige Mängel auf.

| Kontrollumfeld   | Risikobeurteilung   | Kontrolltätigkeiten   | Information & Kommunikation   | Überwachung   |
|--|---|---|---|---|
| Das Management soll sich für Sachkenntnis und richtiges Benehmen in Sachen IT engagieren und für die erforderliche fachliche Ausbildung sorgen. Die Personalpolitik spielt auch eine Schlüsselrolle bei einem positiven IT-Kontrollumfeld. | <p>Hinsichtlich der allgemeinen Kontrolle hat die Abteilung :</p> <ul style="list-style-type: none"> <li>- den Zugriff der Benutzer nicht auf die für die Aufgabenstellung erforderlichen Mittel beschränkt;</li> <li>- keine geeigneten Kontrollstrukturen für die Systemsoftware entwickelt um Programme und sensible Informationen sicherzustellen;</li> <li>- die Softwareänderungen nicht erfasst;</li> <li>- unkompatible Aufgaben nicht getrennt;</li> <li>- die Kontinuität der Abteilung nicht sichergestellt;</li> <li>- das Netz nicht gegen unerwünschten Verkehr geschützt.</li> </ul> <p>In Sachen Prüfung der Computeranwendungen hat die Abteilung keine Zugriffsgenehmigungen erteilt.</p> | <p>Die Abteilung kann:</p> <ul style="list-style-type: none"> <li>logische (Passwort) und physische Zugriffskontrollen (Schloss, Identifizierungsnachweis, Alarm) anwenden;</li> <li>- den Benutzern von Anwendungsgebieten die Möglichkeit in das Lenkungssystem einzuloggen, verweigern;</li> <li>- den Zugang zum Produktionsgebiet auf das Personal das sich mit Entwicklungen befasst, beschränken;</li> <li>- Kontrolltagebücher anwenden, so dass Zugriffe (Versuche) und Aufträge registriert und Verstöße gegen die Sicherheit entdeckt werden;</li> <li>- einen Plan für Notfälle und Katastrophen erarbeiten, so dass die wesentlichen Ressourcen weiterhin zur Verfügung stehen und die Kontinuität des Betriebs gefördert werden kann;</li> <li>- Firewalls installieren und den Webserver überprüfen um den Netzverkehr sicherzustellen.</li> </ul> | <p>IT-Kontrollverfahrensweisen sollten vorhanden sein und Softwareänderungen sollten erfasst werden bevor die Software installiert wird.</p> <p>Es sollten eine Strategie und Tätigkeitsbeschreibungen entwickelt werden die die Prinzipien der Aufgabentrennung fördern.</p> <p>Kontrolltagebücher für Logins (Versuche) und unerlaubte Aufträge sollten periodisch mitgeteilt und überprüft werden.</p> | <p>Mögliche Aktivitäten sind die Durchführung einer IT-Prüfung und einer Katastrophen-simulation, die Überprüfung der Tätigkeiten des Webservers.</p> |

## **Anlage 2 Glossar**

Dieses Glossar legt die wichtigsten Begriffe aus die im Zusammenhang mit der Definition und Praxis der internen Kontrolle verwendet werden. Einige Definitionen wurden in die Richtlinien eingeführt. Daneben haben wir nachstehend auch bestehende Definitionen aus verschiedenen Quellen aufgenommen :

- Code of ethics and auditing standards, INTOSAI, 2001. (INTOSAI auditing standards)
- Internal Control – Integrated Framework, COSO, 1992. (COSO 1992)
- Glossarium, Office for official publications of the European communities, P. Everard and D. Wolter, 1989. (glossarium)
- Auditing and assurance services, an integrated approach, A. A. Arens, R. J. Elder and M. S. Beasley, Prentice Hall international edition, ninth edition, 2003. (Arens, Elder & Beasley)
- the COSO exposure draft “Enterprise Risk Management Framework”, COSO, 2003. (COSO ERM)
- Handbook of international auditing, assurance, and ethics pronouncements, IFAC, 2003. (IFAC)
- Transparency International Source Book 2000, (Transparency International)
- XVI INCOSAI, Montevideo, Uruguay, 1998, Principal Paper Theme 1A (Preventing and Detecting Fraud and Corruption), February 1997, (XVI INCOSAI, Uruguay, 1998)

## A

### Abläufe

- Der Begriff „Abläufe“ verbunden mit „Zielsetzungen“ oder „Kontrollen“ deutet auf die Wirksamkeit und die Effizienz der Tätigkeiten einer Körperschaft hin. Abläufe umfassen Leistungserbringung, gewinnbringende Zielsetzungen und die Sicherstellung von Ressourcen. (COSO 1992)
- Die für die Zielerreichung der Körperschaft erforderlichen Funktionen, Prozesse und Tätigkeiten.

### Allgemeine Kontrollen

- Allgemeine Kontrollen beziehen sich auf die für das gesamte IT-System einer Organisation oder auf einen großen Teilbereich gültigen Strukturen, Strategien und Verfahren, die dazu beitragen, den ordnungsgemäßen Betrieb sicherzustellen. Sie schaffen das Umfeld, in dem die Anwendungen betrieben und die Kontrollen durchgeführt werden.
- Strategien und Verfahren die dazu beitragen, den kontinuierlichen und ordnungsgemäßen Betrieb des IT-Systems sicherzustellen. Sie umfassen Kontrollen des IT-Managements, der IT-Infrastruktur, des Sicherheitsmanagements und der Beschaffungs-, Entwicklungs- und Wartungsphase für Software. Allgemeine Kontrollen unterstützen das Funktionieren von programmierten anwendungsspezifischen Kontrollen. Andere Begriffe für allgemeine Kontrollen sind allgemeine Computerkontrollen und IT- Kontrollen. (COSO ERM)

### Anwendungsspezifische Kontrollen

- Die anwendungsspezifischen Kontrollen umfassen die für separate, individuelle Anwendungssysteme gültigen Strukturen, Strategien und

Verfahren. Sie sind entwickelt worden um die Datenverarbeitung innerhalb spezifischer Anwendungssoftware abzusichern.

- Programmierete Verfahren in Anwendungssoftware und dazugehörige manuelle Verfahren die entwickelt worden sind um die Vollständigkeit und die Genauigkeit der Informationsverarbeitung zu gewährleisten. Beispiele sind elektronische Kontrollen der eingetragenen Daten, Kontrollen der numerischen Reihen und manuelle Verfahren um in Ausnahmelisten aufgenommene Items weiterzuverfolgen. (COSO 1992)

### **Aufdeckende Kontrollmaßnahmen**

Eine Kontrolle zwecks Aufdeckung einer unbeabsichtigten Veranstaltung oder eines unbeabsichtigten Ergebnisses (im Gegensatz zu vorbeugenden Kontrollmaßnahmen) (COSO 1992)

### **Aufgabentrennung**

- Um das Risiko von Fehlern, Verschwendung oder unrechtmäßigem Handeln und das Risiko, dass derartige Probleme nicht aufgedeckt werden, zu reduzieren, sollte nie eine Person oder ein Team allein für die Schlüsselfunktionen eines Geschäftsfalls (Genehmigung, Auswertung, Erfassung, Überprüfung) oder Vorgangs zuständig sein.
- Aufgabentrennung in einer Organisation bezieht sich auf :  
Verwahrung von Vermögenswerten, Genehmigung, Verantwortung für Betriebsabläufe. (Arens, Elder & Beasley)

### **Ausgabe (Output)**

In IT handelt es sich um vom Computer verarbeiteten Daten und Informationen, wie eine graphische Darstellung auf einem Terminal oder eine Kopie.

## **B**

### **Betrug**

- Eine illegale Wechselwirkung zwischen zwei Entitäten, bei der eine Partei sich vorsätzlicher Täuschung bedient mittels falscher Darstellung um sich unzulässige ungerechte Vorteile zuzueignen. Täuschung, Schwindel, Verheimlichung, Vertrauensbruch sind betrügerische Handlungen die angewendet werden um sich auf eine ungerechte und unehrliche Weise Vorteile zuzueignen. (XVI INCOSAI, Uruguay, 1998)
- Betrug wird definiert als eine von einer oder mehreren Personen (Führungskräften, Mitarbeitern, Drittpersonen) begangene vorsätzliche Handlung die zu einer falschen Darstellung der Jahresabschlüsse führt. (IFAC)
- Eine vorsätzliche falsche Darstellung der Jahresabschlüsse. (Arens, Elder & Beasley)

## **C**

### **Computeranwendung**

Computerprogramm entwickelt um Leute bei einer bestimmten Kategorie Arbeit zu begleiten, inklusive Sonderaufträge wie Lohnbuchhaltung, Inventarkontrolle, Buchhaltung und Auftragsunterstützung. Entsprechend der Arbeit wofür das Programm entwickelt wurde,

verarbeitet es deren Texte, Zahlenmaterial, Graphiken oder eine Kombination von diesen Elementen.

### **Computer Informationssystem**

Ein Computer Informationssystem ist vorhanden wenn ein Computer, ohne Rücksicht auf Typ oder Größe, an der Verarbeitung durch die Körperschaft für die Prüfung wichtiger finanzwirtschaftlicher Daten beteiligt ist, unabhängig davon, dass der Computer von der Körperschaft oder von Dritten bedient wird. (IFAC)

### **Computerkontrollen**

1. Kontrollen durch den Computer durchgeführt, d.h. in die Computersoftware hineinprogrammierte Kontrollen (im Gegensatz zu manuellen Kontrollen).
2. Kontrollen der Datenverarbeitung durch den Computer, d.h. allgemeine Kontrollen und anwendungsspezifische Kontrollen (sowohl programmierte als auch manuelle). (COSO 1992)

### **COSO**

Committee of Sponsoring Organisations of the Treadway Commission, eine Gruppe von verschiedenen Organisationen für Rechnungsführung. In 1992 hat COSO eine wertvolle Studie in Sachen interne Kontrolle unter dem Titel „Internal Control – Integrated Framework“ veröffentlicht. Die Studie wird oft als der „COSO Report“ bezeichnet.

## **D**

### **Daten**

Fakten und Informationen die mitgeteilt und manipuliert werden können.

### **Dokumentation**

- Dokumentation der Struktur der internen Kontrolle sollte folgendes umfassen : Identifizierung der Struktur und der Strategie einer Organisation sowie ihre Wirkungsbereiche und die dazugehörigen Zielsetzungen und Kontrollverfahrensweisen. Diese Informationen sollten in die Richtlinien des Managements, die Verwaltungsprinzipien, die Handbücher für Verfahrensweisen und für Rechnungsführung aufgenommen werden.
- Dokumentation ist das Material (Arbeitsunterlagen) das vorbereitet worden ist durch und für, oder erworben und aufbewahrt durch den Prüfer im Zusammenhang mit der Durchführung der Prüfung. (IFAC)
- Die Analyse durch den Prüfer der Unterlagen und Berichte des Kunden um die Informationen zu belegen die in die Jahresabschlüsse aufgenommen sind oder aufgenommen hätten sein müssen. (Arens, Elder & Beasley)

## **E**

### **Edit-Prüfung**

In das Frühstadium des Inputverfahrens hineinprogrammierte Kontrollen um fehlerhafte Datenfelder zu erkennen. Diese Kontrolle ist in der Lage die in numerische Felder eingetragenen alphanumerischen Zeichen zurückzuweisen. Programmierte Edit-Prüfungen können zur Anwendung

kommen wenn Daten bezüglich Transaktionen aus einer anderen Anwendung in den Verarbeitungszyklus hineinfließen.

### **Effizient**

Bezieht sich auf das Verhältnis der eingesetzten Ressourcen zu der zur Zielerreichung erbrachten Leistung. Dabei steht die Forderung im Vordergrund, dass eine bestimmte Menge oder Qualität einer Leistung mit dem geringstmöglichen Ressourceneinsatz produziert wird. Beziehungsweise mit einer bestimmten Menge oder Qualität an Ressourceneinsatz die maximale Leistung erzielt wird.

### **Effizienz**

- Das Verhältnis des Outputs im Sinn von produzierten Gütern, Dienstleistungen und anderen Ergebnissen und den dafür eingesetzten Mitteln. (INTOSAI auditing standards)
- Maximierung des Outputs durch Einsatz der vorhandenen Geld-, Personal- und Sachmittel oder Minimierung des Inputs durch eine quantitative und gegebene qualitative Bestimmung des Outputs. (Glossar)

### **Eingabe (Input)**

Die Daten werden in den Computer eingegeben.

### **Eingreifen des Managements**

Handeln des Managements indem es Strategien und Verfahren aus berechtigten Gründen zurückweist. Das Eingreifen ist erforderlich um sich einmaligen und nichtgängigen Geschäftsfällen und Vorgängen zu widersetzen, die vom System ohne Eingreifen nicht auf eine angemessene Weise abgewickelt werden (siehe Nichtbeachtung von seiten des Managements) (COSO 1992)

### **Einhaltung von Gesetzen**

Hier geht es um die Einhaltung geltender Gesetze und Vorschriften die für eine Körperschaft zutreffen. (COSO 1992)

### **Endbenutzersysteme**

Bezieht sich auf die Anwendung von nicht zentralisierten (d.h. nicht-IT-Abteilung) Datenverarbeitung wobei von Endbenutzern entwickelte automatisierte Verfahren angewendet werden, gewöhnlich anhand von Softwarepaketen (z.B. Spreadsheet und Datenbank). Endbenutzerprozesse können weiter entwickelt werden und eine besonders wichtige Informationsquelle für Management werden. Ob die ausreichend getestet und dokumentiert werden, ist die Frage.

### **Entwurf**

1. Absicht; wie in der Definition, interne Kontrolle wird durchgeführt in der Absicht die Zielerreichung auf eine berechnete Weise sicherzustellen; wenn die Absicht realisiert wird, kann das System als wirksam betrachtet werden.
2. Plan; ein bestimmtes Funktionieren des Systems als Voraussetzung haben, im Gegensatz zum tatsächlichen Funktionieren des Systems (COSO 1992)

### **Ethisch**

Bezieht sich auf moralische Prinzipien.

**Ethische Werte**

Moralische Werte versetzen die Führungskraft in die Lage eine geeignete Verhaltensweise festzustellen; diese Werte sollten auf dem „richtigen Verhalten“ basieren, das die gesetzlichen Anforderungen übersteigt. (COSO 1992)

**Externe Kontrolle**

Prüfung die durch eine externe von der geprüften Körperschaft unabhängige Einrichtung vorgenommen wird und die darauf abzielt, einerseits ein Urteil über die Rechnungsführung und Rechnungslegung, über die Ordnungsmäßigkeit und Rechtmäßigkeit der Geschäftsvorfälle und/oder über die Haushalts- und Wirtschaftsführung abzugeben sowie andererseits entsprechende Berichte zu erstellen.

**F****Flussdiagramm**

- Eine grafische Darstellung der Dokumente und Berichte (Arens, Elder & Beasley)
- Diagramm, in dem der Ablauf von Verfahren bzw. der Weg von Informationen und Dokumenten dargestellt ist. Mit Hilfe dieser Technik ist es möglich komplexe Kreisläufe oder Verfahren übersichtlich zu beschreiben. (Glossar)

**H****Haushaltsplan**

Quantitativer und finanzieller Ausdruck eines Maßnahmenprogramms, dessen Realisierung für einen gegebenen Zeitraum vorgesehen ist. Der Haushaltsplan dient zur Planung des zukünftigen Handelns und zur nachgängigen Prüfung der erzielten Ergebnisse. (Glossar)

**Haushaltskontrolle**

Prüfung, durch die eine Behörde, die den Haushaltsplan einer Körperschaft genehmigt hat, sich vergewissert, dass dieser Haushaltsplan gemäß den Voranschlägen, Mittelbewilligungen und den geltenden Vorschriften ausgeführt wurde. (Glossar)

**Hinlängliche Sicherheit**

- Ein hinlängliches Maß an Sicherheit setzt voraus, dass – unter Berücksichtigung der Kosten, des Nutzens und der Risiken – ein zufriedenstellendes Maß an Vertrauen geschaffen wird.
- Auch ein wohlgedachtes und gewissenhaft eingesetztes internes Kontrollsystem bietet keine absolute Gewähr dass die Zielsetzungen der Körperschaft erreicht werden. Diese Tatsache ist auf die den internen Kontrollsystemen inhärenten Einschränkungen zurückzuführen. (COSO 1992)

**I****Inhärente Einschränkungen**

Es handelt sich hier um jene Einschränkungen die für alle internen Kontrollsysteme gelten. Die Einschränkungen beziehen sich auf

menschliche Fehleinschätzungen; die begrenzten Ressourcen und die Notwendigkeit die Kosten der Kontrollen gegen die Nutzen abzuwägen; die Möglichkeit eines Systemzusammenbruchs; die Möglichkeit dass das Management sich über das interne Kontrollsystem hinwegsetzt und die Möglichkeit von geheimen Absprachen. (COSO 1992)

### **Inhärentes Risiko**

Das inhärente Risiko ist jenes Risiko, dem eine Organisation ohne Maßnahmen zur Reduktion der Auswirkungen oder der Eintrittswahrscheinlichkeit ausgesetzt ist. (COSO ERM)

Institute of Internal Auditors (IIA)

Das IIA ist eine Organisation die ethische Normen und Methoden entwickelt, die sorgt für Ausbildung und für die Förderung eines hohen professionellen Niveaus für ihre Mitarbeiter.

### **Integrität**

Integrität ist die ethische Wertehaltung; Redlichkeit, Aufrichtigkeit und Wahrhaftigkeit, der Wunsch gerecht zu handeln.(COSO 1992)

### **International Organisation of Supreme Audit Institutions (INTOSAI)**

INTOSAI ist die Internationale Organisation der Obersten Rechnungskontrollbehörden (ORKB) für Mitgliedstaaten der Vereinten Nationen oder einer ihrer Sonderorganisationen. Die ORKB spielen eine wichtige Rolle in ihren Staaten; sie prüfen die Haushalts- und Wirtschaftsführung der Regierungen und tragen zu ihrer Verbesserung bei. INTOSAI wurde im Jahre 1953 gegründet; ihre Mitgliederzahl ist mittlerweile von ursprünglich 34 auf mehr als 170 Staaten angestiegen.

### **Interne Kontrolle**

Die interne Kontrolle ist ein in die Arbeits- und Betriebsabläufe einer Organisation eingebetteter Prozess, der von den Führungskräften und den Mitarbeitern durchgeführt wird, um bestehende Risiken zu erfassen und zu steuern und mit ausreichender Gewähr sicherstellen zu können, dass die betreffende Körperschaft im Rahmen der Erfüllung ihrer Aufgabenstellung die folgenden allgemeinen Ziele erreicht :

Sicherstellung ordnungsgemäßer, ethischer, wirtschaftlicher, effizienter und wirksamer Abläufe; Erfüllung der Rechenschaftspflicht; Einhaltung der Gesetze und Vorschriften; Sicherung der Vermögenswerte vor Verlust.

### **Internes Kontrollsystem**

Ein Synonym für die in einer Organisation durchgeführte interne Kontrolle (COSO 1992)

### **Interne Revisionsstelle**

Dienststelle (oder Tätigkeit) innerhalb einer Organisation die sich im Auftrag der Leitung mit Kontrollen und der Bewertung der Systeme und Verfahren der Organisation befasst, damit etwaiges betrügerisches, fehlerhaftes oder unwirtschaftliches Handeln weitmöglichst verringert wird. Die interne Revision muss innerhalb der Organisation unabhängig sein und der Leitung unmittelbar Bericht erstatten. (Glossar)

**Interne Revisoren**

Prüfen die Wirksamkeit des internen Kontrollsystems mittels Evaluierungen, unterbreiten Empfehlungen und tragen dadurch zu dessen nachhaltige Wirksamkeit bei.

**K****Komponente**

Eines der fünf Elemente der internen Kontrolle. Die Komponenten der internen Kontrolle einer Körperschaft sind internes Kontrollumfeld, Risikobeurteilung, Kontrolltätigkeiten, Information und Kommunikation, und Überwachung. (COSO 1992)

**Kontrolle**

1. Das Vorhandensein einer Kontrolle – eine Strategie oder Verfahrensweise die Bestandteil ist einer internen Kontrolle. Eine Kontrolle kann innerhalb einer der fünf Komponenten vorhanden sein.
2. Eine Kontrolle durchführen – Ergebnisse der Strategie und Verfahrensweisen die für die Kontrolle entwickelt worden sind; diese Ergebnisse sind oder sind nicht eine wirksame interne Kontrolle.
3. Kontrollieren – regulieren; eine Strategie anwenden die sich auf die Kontrolle auswirkt. (COSO 1992)

**Kontrollinstanz**

Öffentliche Instanz, ungeachtet ihrer Bestimmung, Zusammensetzung oder Organisation, die gemäß dem Gesetz externe Kontrollen durchführt. (Glossar)

**Kontrolltätigkeit**

Kontrolltätigkeiten sind Verfahrensweisen die entwickelt worden sind um Risiken zu behandeln und die Zielsetzungen der Körperschaft zu erreichen. Die von einer Organisation eingesetzten Verfahrensweisen um Risiken zu behandeln werden Kontrolltätigkeiten genannt.

**Kontrollumfeld**

Das Kontrollumfeld bestimmt die Einstellung innerhalb einer Organisation und beeinflusst das Kontrollbewusstsein der Mitarbeiter. Es bildet die Basis aller übrigen Komponenten interner Kontrolle und gibt die Disziplin und Struktur vor.

**Körperschaft**

Eine Organisation die für ein bestimmtes Ziel gegründet ist. Eine Körperschaft ist zum Beispiel ein Geschäftsbetrieb, eine Non-Profit-Organisation, eine öffentliche Einrichtung oder eine akademische Behörde. Organisation und Abteilung werden als Synonym gebraucht. (COSO 1992)

**Korruption**

Jede Form der unmoralischen Anwendung öffentlicher Befugnis für persönliche oder private Zwecke (XVI INCOSAI, Uruguay, 1998). Missbrauch der Macht für private Zwecke (Transparency International).

**Kosten-/Nutzenrechnung**

Siehe Wirtschaftlich, Wirksamkeit und Effizienz.

**L****Legislative**

Die gesetzgebende Gewalt in einem Staat, z.B. das Parlament.  
(INTOSAI auditing standards)

**Logischer Zugriff**

Der Zugriff zu Computerressourcen wird begrenzt auf "Lesezugriff", ein erweiterter Zugriff umfasst die Möglichkeit Daten abzuändern, neue Dateien zu schaffen und bestehende Dateien zu löschen. (siehe auch physikalischer Zugriff)

**M****Management**

Vorgesetzte und andere Mitarbeiter die Managementaufgaben erfüllen. Management umfasst die Direktoren und den Prüfungsausschuss nur wenn sie solche Aufgaben erfüllen. (IFAC)

**Mangel**

Eine wahrgenommene, potentielle oder tatsächliche Prüfungsunzulänglichkeit, oder eine Gelegenheit um die interne Kontrolle zu verstärken so dass die Probabilität der Zielerreichung der Körperschaft erhöht wird. (COSO 1992)

**Manuelle Kontrollen**

Kontrollen die manuell, nicht vom Computer durchgeführt werden (siehe Computerkontrollen). (COSO 1992)

**N****Netzwerk**

In IT ein System von netzartig verbundenen Computern und dazugehörenden Einrichtungen. Ein Netzwerk umfasst permanente Verbindungen wie z.B. Kabel, oder zeitlich begrenzte Verbindungen über Telefon oder andere Kommunikationswege. Ein Netzwerk ist entweder ein kleines, lokales Netzwerk mit einigen Computern, Druckern und anderen Geräten, oder besteht aus vielen kleinen und großen Computern in einem geographisch ausgedehnten Gebiet.

**Nichtbeachtung von seiten des Managements**

Handeln des Managements indem es Strategien und Verfahren aus unberechtigten Gründen zurückweist um sich persönliche Vorteile zuzueignen oder um einen falschen Eindruck entstehen zu lassen bezüglich der Finanzlage der Körperschaft oder der Einhaltung von Vorschriften (siehe Eingreifen des Managements). (COSO 1992)

**O****Oberste Rechnungskontrollbehörden (ORKB)**

Die Behörde eines Staates, die, ohne Rücksicht auf ihre Zusammensetzung oder Organisation, kraft des Gesetzes die obersten öffentlichen Kontrollbefugnisse eines Staates hat. (INTOSAI auditing standards & IFAC)

**Öffentliche Rechenschaftspflicht**

Die Verpflichtung für Personen oder Körperschaften, einschließlich öffentlicher Unternehmen und Gesellschaften, denen öffentliche Mittel anvertraut werden, um für die steuerlichen, unternehmerischen und Programmaspekte Rechenschaft abzulegen. Die Rechenschaftslegung geschieht gegenüber denjenigen die den betreffenden Personen und Körperschaften die Verantwortung übertragen haben. (INTOSAI auditing standards)

**Öffentlicher Sektor**

Der Begriff „öffentlicher Sektor“ verweist auf nationale Regierungen, regionale Regierungen (z.B. Bundesstaat, Provinz, Bezirk), lokale Regierungen (z.B. Stadt, Gemeinde) und die dazugehörigen Körperschaften (z.B. Agenturen, Ausschüsse, Kommissionen und Unternehmen). (IFAC)

**Ordnungsgemäß**

Einer bestimmten Ordnung entsprechend, oder methodisch.

**P****Personengruppen (Stakeholders)**

Beteiligte Stellen und Personengruppen wie die Aktieninhaber, die Mitarbeiter, die Kundschaft und die Lieferanten. (COSO ERM)

**Physikalischer Zugriff**

Zugriff auf Bereiche und Körperschaften. (siehe logischer Zugriff)

**Prozessmanagement**

Eine Reihe von Arbeits- und Betriebsabläufen die vom Management durchgeführt werden. Interne Kontrolle ist in das Prozessmanagement eingebettet. (COSO 1992)

**Prüfung**

Prüfung der Tätigkeiten und Geschäftsvorfälle einer Körperschaft mit dem Ziel festzustellen, ob diese gemäß bestimmten Zielen, Haushaltsplänen und bestimmten Vorschriften und Normen durchgeführt werden bzw. ablaufen. Ziel dieser Prüfung ist es, in regelmäßigen Zeitabständen Abweichungen aufzudecken die möglicherweise Abhilfemaßnahmen notwendig machen. (Glossar)

**Prüfungsausschuss**

Ein Ausschuss innerhalb des Vorstands der sich insbesondere mit Finanzberichterstattung sowie mit Vorgängen beschäftigt um die geschäftlichen und finanziellen Risiken im Griff zu haben, und für die Einhaltung wichtiger geltender gesetzlicher, ethischer und ordnungsmäßiger Anforderungen. Kennzeichnend für den Prüfungsausschuss ist, dass er den Vorstand unterstützt bei der Aufsicht über (a) die Integrität der Jahresabschlüsse, (b) die Einhaltung gesetzlicher und ordnungsmäßiger Anforderungen, (c) die Qualifizierungen und Unabhängigkeit des Prüfers, (d) das Funktionieren der Innenrevision und des unabhängigen Prüfers sowie (e) die

Entschädigung der Führungskräfte des Betriebs (in Ermangelung eines Entschädigungsausschusses).

## R

### **Rechenschaftspflicht**

- Prozess, durch welchen öffentliche Verwaltungseinrichtungen und deren Mitarbeiter über ihre Entscheidungen und Tätigkeiten im Rahmen ihrer Verantwortung für die Verwendung öffentlicher Mittel und deren angemessenem Einsatz sowie alle übrigen Aspekte der Arbeits- und Betriebsabläufe Rechenschaft ablegen.
- Einer Person oder geprüften Körperschaft auferlegte Pflicht nachzuweisen, dass sie die ihr anvertrauten Mittel gemäß den Bedingungen, unter denen die Mittel ihr zur Verfügung gestellt wurden, verwaltet oder kontrolliert hat. (Glossar)

### **Rechenzentrum**

Ein Computer von hohem Niveau zur Leistung intensiver Computeraufgaben. Am Rechenzentrum nehmen verschiedene Benutzer mittels Terminals teil.

### **Risiko**

- Die Prüfer nehmen ein gewisses Maß an Unsicherheit bei der Durchführung von Kontrollen hin (Arens, Elder & Beasley)
- Die Möglichkeit eines plötzlich eintretenden Ereignisses das sich auf die Zielerreichung negativ auswirkt. (COSO ERM)

### **Risikobereitschaft**

- Die Risikobereitschaft definiert das Risiko, das die Körperschaft einzugehen bereit ist, ohne Gegenmaßnahmen zu treffen.
- Das Risiko das ein Unternehmen einzugehen bereit ist um seine allgemeinen Zielsetzungen zu erreichen. (COSO ERM)

### **Risikobeurteilung**

Risikobeurteilung ist ein Verfahren zur Identifizierung und Analyse von Risiken, welche die Erreichung der Ziele einer Körperschaft gefährden könnten, und dient zur Festlegung einer angemessenen Risikomanagementstrategie.

### **Risikoevaluierung**

Ist die Beurteilung der Bedeutung des Risikos und der Wahrscheinlichkeit des Eintretens.

### **Risikoprofil**

Die Übersicht oder Matrix der Hauptrisiken einer Verwaltungseinrichtung oder untergeordneten Körperschaft, die auch das Ausmaß der Auswirkungen (z.B. hoch, mittel, gering) und die Wahrscheinlichkeit des Eintretens beinhaltet.

### **Risikotoleranz**

Die annehmbare Abweichung von der Zielerreichung. (COSO ERM)

## S

### **Servicekontinuität**

Servicekontinuität gewährleistet Unterstützung um sicherzustellen, dass kritische Operationen im Fall unerwarteter Ereignisse ohne Unterbrechung weitergeführt oder umgehend wieder aufgenommen werden können und kritische und sensible Daten geschützt bleiben.

### **Sicherheitsprogramm**

Die organisationsweite Sicherheitsprogramm- und Sicherheitsmanagementplanung sind die Basis für die Sicherheitsstruktur der Organisation und stellen das Engagement der obersten Führungskräfte für Risikomanagement dar. Das Programm sollte einen Rahmen für die Tätigkeiten im Bereich Risikomanagement, die Entwicklung von Sicherheitsstrategien und die Überwachung der Angemessenheit dieser Verfahren schaffen.

### **Sparsamkeit**

- Minimierung der Kosten der für eine bestimmte Aktivität eingesetzten Mittel bei Wahrung der geeigneten Qualität. (INTOSAI auditing standards)
- Beschaffung qualitativ und quantitativ geeigneter Geld-, Personal- und Sachmittel zum richtigen Zeitpunkt und mit geringstmöglichem Kostenaufwand. (Glossar)

### **Strategie**

Dienstliche Anordnung des Managements bezüglich der Durchführung von Kontrollen. Die Strategie ist die Basis für die Einführung von Verfahren und deren Umsetzung. (COSO 1992)

### **Systemsoftware**

Diese Software gewährleistet hauptsächlich die Koordinierung und Steuerung der Ressourcen für Hardware und Kommunikation, den Zugriff auf Unterlagen und die Steuerung der Anwendungen.

### **Systemsoftware-Kontrollen**

Die Kontrolle der Programme und der betreffenden Routine dient dazu die Abwicklung der Computervorgänge zu überwachen.

## U

### **Überwachung**

Überwachung ist eine Komponente der internen Kontrolle und ein Evaluierungsprozess zur Beurteilung der Qualität der Systemperformance im Zeitablauf.

### **Unabhängigkeit**

- Handlungsfreiheit die einer Rechnungskontrollbehörde und deren Prüfern nach Maßgabe des Prüfungsauftrags ohne jegliche Einmischung von außen eingeräumt wird. (Glossar)
- Die Handlungsfreiheit der ORKB um die Kontrollen nach Maßgabe des Kontrollmandats und ohne jegliche externe Einmischung und Anweisung durchzuführen. (INTOSAI auditing standards)

- Der Prüfer kann in der Ausübung seines Dienstes eine unparteiische Stellung einnehmen (Unabhängigkeit im eigentlichen Sinne) (Arens, Elder & Beasley)
- Der Prüfer kann gegenüber anderen Personen eine unparteiische Stellung einnehmen (äußerliche Unabhängigkeit). (Arens, Elder & Beasley)

### **Unsicherheit**

Unvermögen um im voraus die Wahrscheinlichkeit des Eintretens eines künftigen Ereignisses oder dessen Auswirkung zu kennen. (COSO ERM)

## **V**

### **Verarbeitung**

In IT handelt es sich um die durch das Verarbeitungszentrum eines Computers zur Ausführung gebrachten Anweisungen eines Programms.

### **Verfahren**

Eine Maßnahme zur Umsetzung einer Strategie. (COSO 1992)

### **Verschwörung**

Eine gemeinsame Planung von Arbeitnehmern mit dem Ziel einem Geschäft Bargeld, Inventar oder andere Aktivvermögen zu entwenden. (Arens, Elder & Beasley)

### **Vorbeugende Kontrollmaßnahmen**

Eine Kontrolle zwecks Vorbeugung einer unbeabsichtigten Veranstaltung oder eines unbeabsichtigten Ergebnisses (im Gegensatz zu aufdeckenden Kontrollmaßnahmen) (COSO 1992)

## **W**

### **Wirksam**

Wirksam bezieht sich auf die Erreichung von Zielen beziehungsweise das Ausmaß, in dem das Ergebnis einer Tätigkeit der Zielsetzung oder dem beabsichtigten Effekt dieser Zielsetzung entspricht.

### **Wirksamkeit**

- Der Zielerfüllungsgrad und das Verhältnis zwischen der beabsichtigten Wirkung und der tatsächlichen Wirkung einer Tätigkeit. (INTOSAI auditing standards)
- Grad der Zielverwirklichung entsprechend einem günstigen Kosten-Nutzen-Verhältnis. (Glossar)

### **Wirtschaftlich**

Wirtschaftlich bedeutet einen weder verschwenderischen noch übermäßigen Einsatz von Ressourcen. Hier geht es darum, die angemessene Menge an Ressourcen in der richtigen Qualität, zur rechten Zeit und an der richtigen Stelle zum niedrigsten Kostpreis bereitzustellen.

## Z

### **Zugriffskontrolle**

Es handelt sich um Kontrollen die in der Informationstechnologie entwickelt worden sind um Ressourcen gegen unerlaubte Änderungen, Verlust oder Veröffentlichung zu schützen.