

Teil 6 Interne Kontrolle

**Dieter WIDMER, dipl. Wirtschaftsprüfer, Partner, Mitglied der
Geschäftsleitung, KPMG**

**Hans-Ulrich PFYFFER, dipl. Wirtschaftsprüfer, Certified Internal
Auditor (CIA), Partner, Leiter Internal Audit Services (IAS), KPMG**

Inhaltsverzeichnis Teil 6

I.	Einleitende Bemerkungen	3
	1. Ausgangslage	3
	2. Verwaltungsrat und Geschäftsleitung in der Pflicht	3
	3. Interne Kontrolle zur Erreichung von geschäftspolitischen Zielen	4
	4. Interne Kontrolle im Interesse der Eigentümer	4
	5. Empfehlungen des Swiss Code of Best Practice	4
	6. Interne Revision zur Überwachung der Internen Kontrolle	5
	7. Zielsetzung und Aufbau dieses Beitrages	5
II.	Neue Anforderungen aus den USA mit Auswirkungen auf die Schweiz	7
III.	Was ist Interne Kontrolle?	11
	1. Definition Interne Kontrolle	11
	2. Abgrenzung Interne Revision	13
	3. Abgrenzung externe Revision	14
	4. Abgrenzung übrige Überwachungsfunktionen	14
IV.	Kontroll-Modelle	16
	1. COSO-Framework	16
	1.1 Steuerungs- und Kontrollumfeld	18
	1.2 Risikobeurteilung	20
	1.3 Steuerungs- und Kontrollaktivitäten	24
	1.4 Information und Kommunikation	25
	1.5 Überwachung	26
	2. COSO-ERM-Framework	28
	3. CoCo-Framework	30
	4. Qualitätsmanagementsysteme	31
	5. Implementierung eines Kontrollmodells	33
V.	Aufgaben und Verantwortlichkeiten	34
	1. Verwaltungsrat	34
	2. Geschäftsleitung	36
	3. Mitarbeiter und Vorgesetzte	37
	4. Interne Revision	37
	5. Externe Revision	38

Inhaltsverzeichnis Teil 6

6. Zusammenarbeit der verschiedenen Überwachungsfunktionen	39
VI. Kontrollmassnahmen	41
1. Kontrollmassnahmen	41
1.1 Präventive und detektive Kontrollen	41
1.2 Selbsttätige, programmierte und manuelle Kontrollen	42
1.3 Kontrollen durch die Geschäftsleitung	43
2. Kontrollrisiken	44
VII. Überprüfung der Internen Kontrollen	46
1. Verwaltungsrat und Audit Committee	46
2. Geschäftsleitung	47
3. Control (Risk) Self Assessment	47
4. Interne Revision	48
5. Externe Revision	49
6. Gesetzgeber und Aufsichtsbehörden	50
VIII. Zusammenfassung und Ausblick	51
Anhang A: Beurteilungsmatrix Internes Kontrollsystem	53
Anhang B: Kontrollkomponenten Glossar	57

Literatur sowie weiterführende Literatur

BERTSCHINGER Peter/SCHAAD Martin, Prüfung amerikanischer und internationaler Konzerngesellschaften in der Schweiz, Der Schweizer Treuhänder 5/2004 (zit.: BERTSCHINGER/SCHAAD, Konzerngesellschaften); BERTSCHINGER Peter/SCHAAD Martin, Der amerikanische Sarbanes-Oxley Act of 2002 – Mögliche Auswirkungen auf die amerikanische und internationale Wirtschaftsprüfung und Corporate Governance, Der Schweizer Treuhänder 10/2002, S. 883 ff. (zit.: BERTSCHINGER/SCHAAD, Auswirkungen); BÖCKLI Peter, Schweizer Aktienrecht, 3. A., Zürich 2004 (zit.: BÖCKLI, Aktienrecht); BÖCKLI Peter, Corporate Governance auf Schnellstrassen und Holzwegen, Der Schweizer Treuhänder 3/2000, S. 133 ff. (zit.: BÖCKLI, Schnellstrassen); BUMBACHER Robert-Jan/SCHWEIZER Markus, Gegenseitige Anforderungen an die Interne Revision, Der Schweizer Treuhänder 11/2002, S. 1039 ff.; CHORAFAS Dimitris, Implementing and Auditing the Internal Control System, New York 2001; COSO, Committee of Sponsoring Organizations of the Treadway Commission, Internal Control – Integrated Framework, Jersey City, New Jersey 1992; COSO, Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management-Framework (Entwurf), www.erm.coso.org, 2004 (zit.: COSO, Enterprise Risk Management-Framework); ENGAMMARE Valérie, Système de contrôle interne et information des actionnaires, Der Schweizer Treuhänder 6/2003, S. 491 ff.; FORSTMOSER Peter, Aufgaben, Organisation und Verantwortlichkeit des Verwaltungsrates, Der Schweizer Treuhänder 5/2002, S. 485 ff.; Grundsätze zur Abschlussprüfung (GzA), Treuhand-Kammer, Zürich 2003; KLINGER Michael/KLINGER Oskar, ABC der Gestaltung und Prüfung des Internen Kontrollsystems (IKS) im Unternehmen, Wien 1998; KLINGER Michael/KLINGER Oskar, Das Interne Kontrollsystem im Unternehmen, München 2000; KPMG UK, Internal Control: A Practice Guide, 2. A., London 2000; JANS Victor, Erfahrungen mit Control & Risk Self Assessment, Der Schweizer Treuhänder 1/2003, S. 27 ff.; MARBACHER Lukas, Risikoorientierte Prüfung – ein Muss, Der Schweizer Treuhänder 11/2000, S. 1179 ff.; PALAZZESI Mauro/PFYFFER Hans-Ulrich, Ein neues Verständnis von Interner Revision, Der Schweizer Treuhänder 3/2002 (zit.: PALAZZESI/PFYFFER, Neues Verständnis); PALAZZESI Mauro/PFYFFER Hans-Ulrich, Interne Revision und Unternehmensüberwachung – von der Konkurrenz zur Kooperation, Der Schweizer Treuhänder 1-2/2004 (zit.:

PALAZZESI/PFYFFER, Kooperation); PICKETT Spencer, Internal Control: A Manager's Journey, New Jersey 2001; ROOT Steven, Beyond COSO: Internal Control to Enhance Corporate Governance, New Jersey 1998; ROTH James, COSO Implementation Guide for The Internal Auditing Department, Altamonte Springs 1995; SCHNEIDER Thomas, Controlling und Interne Revision im Internen Kontrollsystem, Der Schweizer Treuhänder 1/2003, S. 33 ff.; Schweizer Handbuch der Wirtschaftsprüfung 1998, Treuhand-Kammer Zürich 1998; STRAUB Ralf Michael, Verantwortlichkeit des Verwaltungsrats und Kodex, Der Schweizer Treuhänder 5/2002, S. 494 ff.; WIDMER Dieter/WEY Hans, Neuregelung der Revision – Erwartungen und Chancen, Der Schweizer Treuhänder 5/2004, S. 361 ff.

Materialien

Botschaft zur Änderung des Obligationenrechts (Revisionspflicht im Gesellschaftsrecht) sowie zum Bundesgesetz über die Zulassung und Beaufsichtigung der Revisorinnen und Revisoren vom 23. Juni 2004, BBI 2004, S. 3969 ff.; Guidance on Control, The Canadian Institute of Chartered Accountants, Toronto 1995; Richtlinie der SWX Swiss Exchange betreffend Informationen zur Corporate Governance vom 1. Juli 2002; Swiss Code of Best Practice for Corporate Governance, economiesuisse, Zürich 2002; The Professional Practices Framework, The Institute of Internal Auditors, Altamonte Springs 2003 (Deutsche Übersetzung: Grundlagen der Internen Revision, Deutsches Institut für Interne Revision e.V., Frankfurt am Main 2002); «Turnbull Report», The Turnbull Proposal on Internal Control, London 1999.

I. Einleitende Bemerkungen

1. Ausgangslage

In der jüngeren Vergangenheit haben handfeste Finanzskandale einige wichtige Schweizer Unternehmen erschüttert, wodurch unter den Investoren und in der Öffentlichkeit ein gewisses Misstrauen gegenüber den Verwaltungsräten sowie den Geschäftsleitungen grosser Unternehmen geweckt wurde. Der gemeinsame Aspekt der erhobenen Vorwürfe bestand darin, dass aufgrund mangelnder «Checks und Balances» mutmasslich ein Machtmissbrauch vorlag, welcher unangemessene oder rechtswidrig qualifizierte Praktiken erst ermöglichte. So wurden Kontrollmechanismen bewusst nicht eingerichtet oder infolge einer mangelhaften organisatorischen Ausgestaltung nicht sachgerecht umgesetzt oder aber bestehende Kontrollen vorsätzlich umgangen.

2. Verwaltungsrat und Geschäftsleitung in der Pflicht

Unternehmerische Verantwortung hat heute einen Stellenwert wie nie zuvor. Verwaltungsrat und Geschäftsleitung stehen in der Pflicht, ihre jeweiligen Aufgaben im Sinne der Gewaltentrennung wahrzunehmen und über das Geschehen im Unternehmen umfassend informiert zu sein, sodass die Unternehmensentwicklung umsichtig und vorausschauend gesteuert werden kann. Um diesen Anspruch zu erfüllen, braucht es funktionsfähige Kontrollmechanismen, profunde Kenntnisse der Prozesse sowie klare Konzepte im Umgang mit Risiken.

Corporate Governance soll eine langfristige Existenzsicherung des Unternehmens ermöglichen, was ebenfalls die unternehmerische Verpflichtung gegenüber den Stakeholdern beinhaltet. Voraussetzung für eine wirkungsvolle, nachhaltige Unternehmensführung ist ein effektives Überwachungs- und Kontrollsystem, welches alle Unternehmensbereiche einbezieht. Nachhaltigkeit bei der Unternehmensführung und damit bei den Kontrollen beginnt an der Spitze, d.h. beim Verwaltungsrat und der Geschäftsleitung. Information und Kommunikation spielen dabei eine Schlüsselrolle. Zudem müssen Unternehmens- und Kontrollkultur nicht nur definiert, sondern auch tagtäglich vorgelebt werden.

3. Interne Kontrolle zur Erreichung von geschäftspolitischen Zielen

Wer ein Unternehmen verantwortungsbewusst führen will, muss sich darauf verlassen können, dass die Prozesse effizient und sicher innerhalb der implementierten Überwachungsmechanismen ablaufen. Die Interne Kontrolle ist dabei ein Mittel zur Erreichung geschäftspolitischer Ziele, wobei ihre Grenzen in menschlichen Schwächen wie Unterlassungen, Missverständnissen oder falschen Entscheidungen liegen. Auch können Kontrollen durch Absprache von zwei oder mehreren Beteiligten absichtlich umgangen werden.

4. Interne Kontrolle im Interesse der Eigentümer

Diese Ausführungen zeigen, dass das Interne Kontrollsystem (IKS) einen höheren Stellenwert erhalten muss. Um den vorgängig erwähnten Mängeln entgegenzutreten und dem Aktionärsschutz die erforderliche Bedeutung beizumessen, sind die Unternehmen gefordert, die Implementierung und Pflege eines lückenlosen und effizienten IKS sicherzustellen. Ein wirksames System der Internen Kontrolle stellt ein zentrales Element der modernen Unternehmensführung und eine wichtige Voraussetzung für ein angemessenes Risikomanagement dar. Insbesondere wird auch die Qualität der finanziellen Berichterstattung wesentlich durch ein wirkungsvolles Kontrollsystem beeinflusst. Die Aktionäre haben ein starkes Interesse an Informationen über das Kontrollsystem, welche einen Anhaltspunkt für die Überlebensfähigkeit des Unternehmens und die Qualität ihrer Geldanlage geben. Zudem wird vermehrt die Offenlegung relevanter Informationen verlangt – an dieser Stelle seien Stichworte wie Sarbanes-Oxley Act (SOX), Turnbull Report oder die Richtlinie betreffend Informationen zur Corporate Governance der SWX Swiss Exchange erwähnt.

5. Empfehlungen des Swiss Code of Best Practice

Gemäss Ziff. 19 des Swiss Code of Best Practice (Swiss Code) muss ein Unternehmen über ein seiner Grösse, seiner Komplexität und seinem Risikopotenzial angemessenes IKS verfügen. Rein inhaltlich gesehen zielt das durch den Swiss Code begründete System auf drei Bereiche ab: Das Risikomanagement, die Normenkonformität und damit die Interne Kontrolle sowie die Interne Revision.

Der Swiss Code schlägt zudem die Schaffung eines Prüfungsausschusses vor, der aus nicht-exekutiven Verwaltungsratsmitgliedern zusammengesetzt sein sollte (Ziff. 23 Swiss Code). Dieser Prüfungsausschuss nimmt für den Informationsfluss zum Verwaltungsrat sowie zur Vorbesprechung und Beurteilung der Überwachungsfunktionen eine Schlüsselfunktion ein. Es gehört jedoch zu den unentziehbaren und unübertragbaren Hauptaufgaben des Verwaltungsrats, für die Einrichtung des erforderlichen effizienten IKS besorgt zu sein und die aufgrund der Regelwerke, z. B. SOX, teilweise verlangten Bestätigungen zur Wirksamkeit der Internen Kontrollen abzugeben.

6. Interne Revision zur Überwachung der Internen Kontrolle

Der Internen Revision kommt dabei eine neue, erweiterte Rolle zu. Die Funktion als Führungsinstrument und wertvolle Unterstützung von Verwaltungsrat und Geschäftsleitung ist unlängst vermehrt in den Mittelpunkt gerückt. Auch in öffentlichrechtlichen und Non-Profit-Organisationen sowie in der öffentlichen Verwaltung kann die Interne Revision einen wichtigen Beitrag zur Corporate Governance, der Wirksamkeit der Internen Kontrollen und damit zur Wertschöpfung leisten, beurteilt die Interne Revision doch die verschiedenen Geschäftsprozesse – insbesondere die Risikomanagement-, die internen Steuerungs- und Kontroll- sowie die Corporate Governance-Prozesse – und weist gegebenenfalls auf Verbesserungspotenziale hin. Dadurch wird die Interne Revision zu einem unabhängigen, objektiven und zuverlässigen Lieferanten entscheidungsrelevanter Informationen für die Verantwortlichen eines Unternehmens. Nicht umsonst empfiehlt Ziff. 19 Swiss Code die Einrichtung einer Internen Revision.

7. Zielsetzung und Aufbau dieses Beitrages

Der vorliegende Teil 6 soll einen Überblick über die Grundsätze der Internen Kontrolle, die verschiedenen Kontrollmodelle, die Verantwortlichkeiten und Kontrollmassnahmen sowie die Überprüfung der Internen Kontrollen geben. Dadurch soll illustriert werden, wie wichtig ein effizientes und wirkungsvolles Kontrollsystem für das Unternehmen ist.

Dieser Teil 6 ist wie folgt aufgebaut:

In II. «Neue Anforderungen aus den USA mit Auswirkungen auf die Schweiz» wird dargestellt, dass als Folge diverser Unternehmensskandale (als Beispiele seien Enron, Worldcom oder Parmalat erwähnt) die Anforderungen an eine funktionierende Interne Kontrolle regulatorisch verstärkt werden. Dabei werden zukünftig verstärkt Standards wie dasjenige des US-amerikanischen Committee of Sponsoring Organizations of the Treadway Commission (COSO) als Grundlage für die Interne Kontrolle verlangt.

In III. wird der Begriff Interne Kontrolle definiert und die Ziele der Internen Kontrolle aufgezeigt. Die Abgrenzung zur Internen Revision sowie zur externen Revision wird beschrieben.

Interne Kontrolle ist ein weiter Begriff und nicht einfach fassbar. Kontrollmodelle helfen, die konkreten Anforderungen an ein Kontrollsystem aufzuzeigen. In IV. wird das COSO-Modell – das sich weltweit als wichtigster Standard durchsetzt – beschrieben. Daneben gibt es weitere Kontrollmodelle, die kurz erwähnt werden.

V. setzt sich mit den Aufgaben und Verantwortlichkeiten der einzelnen Organe und den Funktionen bezüglich der Internen Kontrolle auseinander. In der Schweiz liegt die Gesamtverantwortung für die Interne Kontrolle beim Verwaltungsrat. Er kann sich dabei jedoch auf unterstützende Instrumente wie die Interne Revision abstützen.

In VI. wird dargestellt, dass als Bestandteil eines umfassenden Systems der Internen Kontrolle die konkreten Kontrollmassnahmen wichtige Elemente darstellen. Dabei werden einzelne Vorgänge, Methoden oder Massnahmen (wie zum Beispiel die Funktionentrennung) beschrieben. Dieses Kapitel gibt auf operationeller Ebene Hinweise, wie Kontrollen effizient und wirkungsvoll in die betrieblichen Prozesse eingebaut werden können.

Abschliessend werden in VII. die wesentlichen Merkmale der Internen Kontrolle nochmals zusammengefasst.

II. Neue Anforderungen aus den USA mit Auswirkungen auf die Schweiz

Als Folge diverser Unternehmensskandale hat der amerikanische Gesetzgeber den SOX verabschiedet¹. Durch das neue Regelwerk soll das Vertrauen von Aktionären und anderen Interessengruppen in die Finanzberichterstattung zurückgewonnen werden. Der SOX nimmt die Unternehmensleitung betreffend Vollständigkeit und Richtigkeit der Angaben bei der quartalsweisen und jährlichen Berichterstattung verstärkt in die Pflicht. Zusätzlich ergeben sich neue Anforderungen an die Unternehmensleitung, indem fortlaufend über die Funktionsfähigkeit des IKS im Rahmen des periodischen Unternehmensreportings zu berichten ist. Der SOX ist von schweizerischen Unternehmen mit kotierten Beteiligungspapieren an einer US-amerikanischen Börse sowie von schweizerischen Tochtergesellschaften von Muttergesellschaften mit kotierten Beteiligungspapieren an einer US-amerikanischen Börse umzusetzen.

SOX Section 404 (SOX 404) verlangt die Einrichtung eines funktionsfähigen IKS und dessen Dokumentation². Dabei sind sämtliche Internen Kontrollen, die im Zusammenhang mit der Rechnungslegung stehen, Gegenstand dieser Regelung. Zusammen mit der jährlichen Berichterstattung ist die Einschätzung und Bewertung der Zweckmässigkeit dieses Kontrollsystems durch die Unternehmensleitung – konkret dem Vorsitzenden der Geschäftsleitung und dem Finanzchef – zu bestätigen sowie zu veröffentlichen. Die externe Revision kontrolliert und berichtet über die regelmässige Einschätzung der Unternehmensleitung. Es handelt sich somit um ein zweistufiges Vorgehen: Zuerst bestätigt das Unternehmen die Qualität des IKS, anschliessend wird diese Bestätigung durch die externe Revision überprüft und gegebenenfalls testiert.

Diese neuen gesetzlichen Vorschriften der USA erfordern die Implementierung eines Regelwerkes für das IKS. Die Unternehmen

¹ BERTSCHINGER/SCHAAD, Auswirkungen, S. 883 ff.; BERTSCHINGER/SCHAAD, Konzerngesellschaften, S. 421 ff.

² BERTSCHINGER/SCHAAD, Konzerngesellschaften, S. 423.

entscheiden sich in der Regel für das COSO-Framework³, das sich als Standard durchgesetzt hat.

Es ist davon auszugehen, dass durch die Entwicklung in den USA und den damit verbundenen Auswirkungen auf andere Regionen und Länder – insbesondere Europa – auch nicht in den USA kotierte Unternehmen mit steigenden Anforderungen an die Ausgestaltung ihrer IKS rechnen müssen. Die Europäische Kommission hat beispielsweise am 16. März 2004 mitgeteilt, dass sie sich stark an den SOX ausrichten werde.

Konkret hat die EU-Kommission eine Neuregulierung der Wirtschaftsprüfung in der Europäischen Union vorgeschlagen, die bis 2006 von den EU-Mitgliedsstaaten einzuführen ist. Es handelt sich um die Neufassung der 8. EU-Richtlinie von 1984 zur Abschlussprüfung, auch «Lex Parmalat» genannt. Gemäss dieser Richtlinie muss der externe Revisor wesentliche Schwächen des IKS (Material weaknesses of internal control) dem Audit Committee mitteilen.

Vor diesem Hintergrund haben zahlreiche Mitgliedsstaaten bereits rechtliche Massnahmen im Sinne der unterbreiteten Vorschläge getroffen. Schon im Juli 2003 hat Frankreich das Gesetz über Finanzsicherheit (Loi sur la Sécurité Financière) verabschiedet, das französische Pendant der Vorschriften des SOX.

Auch in der Schweiz gibt es Anzeichen, dass das IKS noch weiter an Bedeutung gewinnen wird. Im Entwurf zur Neuregelung der Revision⁴ ist gemäss Art. 728a OR vorgesehen, dass die externe Revision zukünftig prüft und darüber Bericht erstattet, ob ein funktionierendes IKS existiert und eine Risikobeurteilung vorgenommen wurde. Dies bedeutet, dass inskünftig der Verwaltungsrat im Anhang der Jahresrechnung das IKS und das Risikomanagement seiner Gesellschaft angemessen zu beschreiben hat⁵ (Art. 728a Abs. 1 Ziff. 4 und 5, Art. 663b Ziff. 12 E OR).

³ Siehe weitere Ausführungen zu Kontroll-Modelle in IV.

⁴ Vgl. dazu Botschaft zur Änderung des Obligationenrechts, S. 3985.

⁵ WIDMER/WEY, S. 361 ff.

Einige schweizerische Gesellschaften haben bereits freiwillig das Gedankengut des SOX 404 aufgenommen, indem sie bereits jetzt das IKS verstärkt überwachen und die internen Prozesse und Kontrollen dokumentieren sowie regelmässig testen.

III. Was ist Interne Kontrolle?

1. Definition Interne Kontrolle

Unter Interner Kontrolle werden alle durch den Verwaltungsrat oder die Unternehmensleitung angeordneten Vorgänge, Methoden und Massnahmen verstanden, die dazu dienen, einen ordnungsgemässen Ablauf der betrieblichen Aktivitäten zu gewährleisten. Die organisatorischen Massnahmen der Internen Kontrolle sind in die betrieblichen Arbeitsabläufe integriert, d. h. sie erfolgen arbeitsbegleitend oder sind dem Arbeitsvollzug unmittelbar vor- oder nachgelagert. Dabei sind unter Interner Kontrolle nicht nur eigentliche Kontrolltätigkeiten, sondern auch Aktivitäten zur Steuerung und Planung zu verstehen, weshalb oft auch von Steuerungs- und Kontrollprozessen gesprochen wird.

Insbesondere wirkt die Interne Kontrolle unterstützend bei

- der Erreichung der geschäftspolitischen Ziele durch eine wirksame und effiziente Geschäftsführung,
- der Einhaltung der anwendbaren Normen wie z. B. Gesetze, Verordnungen, Reglemente und Weisungen (Compliance),
- dem Schutz des Geschäftsvermögens,
- der Verhinderung, Verminderung und Aufdeckung von Fehlern und Unregelmässigkeiten,
- der Sicherstellung der Zuverlässigkeit und Vollständigkeit der Buchführung sowie
- der zeitgerechten und verlässlichen finanziellen Berichterstattung.

Die Interne Kontrolle hat – im Rahmen eines kontinuierlichen Prozesses – sicherzustellen, dass sich die Risiken innerhalb der durch das Risikomanagement definierten Toleranzwerte bewegen, Zielabweichungen erkannt werden sowie entsprechender Handlungsbedarf identifiziert und umgesetzt wird. Dies bedingt, wie schon erwähnt,

den Einbezug von Verwaltungsrat, Geschäftsleitung sowie allen Mitarbeitern. Das Vier-Augen-Prinzip, die Funktionentrennung wie auch die Zutrittskontrolle sind Elemente der Internen Kontrolle.



Abb. 1: Interne Kontrolle als System von Vorgängen, Methoden und Massnahmen

Die Notwendigkeit einer Internen Kontrolle ergibt sich unter anderem auch aus den Grundsätzen der ordnungsmässigen Buchführung und Rechnungslegung (Ziel: Sicherstellen einer verlässlichen finanziellen Berichterstattung). Für die organisatorischen Vorkehrungen und die Sicherstellung der dauernden Wirksamkeit der Internen Kontrolle sind der Verwaltungsrat und die Geschäftsleitung verantwortlich.

Um eine verlässliche finanzielle Berichterstattung und damit die ordnungsgemässe Rechnungslegung zu gewährleisten, sind demzufolge geeignete Kontrollmassnahmen⁶ zu implementieren, welche

⁶ Siehe weitere Ausführungen zu den Kontrollmassnahmen in VI.

- die Vollständigkeit, Richtigkeit und Gültigkeit des verwendeten Datenmaterials,
- das Vorhandensein und die Echtheit von relevanten Beständen,
- eine korrekte ergebnisbezogene Periodenabgrenzung sowie
- eine den gewählten Rechnungslegungsstandards entsprechende korrekte Bewertung, Gliederung und Präsentation sicherstellen.

Ein wesentlicher Mangel der Internen Kontrolle liegt dann vor, wenn in wichtigen Bereichen der Buchführung und Rechnungslegung die Ordnungsmässigkeit nicht gegeben ist.

2. Abgrenzung Interne Revision

Im Gegensatz zur Internen Kontrolle ist die Interne Revision⁷ eine nicht in die betrieblichen Arbeitsabläufe integrierte, prozessunabhängige Stelle, welche u. a. mit der Überprüfung der Internen Kontrolle beauftragt ist.

Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen⁸, welche darauf ausgerichtet sind, die Geschäftsprozesse zu verbessern und Mehrwerte zu schaffen. Sie unterstützt die Unternehmen bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen sowie der Führungs- und Überwachungsprozesse bewertet und diese zu verbessern hilft⁹.

⁷ PALAZZESI/PFYFFER, Neues Verständnis, S. 137 ff.; PALAZZESI/PFYFFER, Kooperation, S. 7 ff.

⁸ Neben den eigentlichen Prüfungsaufgaben kann die Interne Revision auch für Beratungsdienstleistungen eingesetzt werden. Gemäss den Berufsstandards der Internen Revision (Standards des Institute of Internal Auditors (IIA) müssen diese Aktivitäten allerdings klar von den Assurance-Tätigkeiten abgegrenzt und als solche gekennzeichnet werden.

⁹ Es handelt sich dabei um die offizielle deutsche Übersetzung der Definition gemäss den Standards des Institute of Internal Auditors (IIA). Das IIA ist der internationale Berufsverband der Internen Revisionen.

3. Abgrenzung externe Revision

Die externe Revision ist vom IKS unabhängig und berücksichtigt im Rahmen des risikoorientierten Prüfungsansatzes die Qualität der Internen Kontrolle. Die Interne Kontrolle wird damit zum Prüfungsgegenstand der externen Revision und beeinflusst je nach Ausgestaltung die weiteren Revisions Schritte. Im Gegensatz zur Internen Revision prüft die externe Revision allerdings nur diejenigen Komponenten der Internen Kontrolle, welche sich auf das Finanz- und Rechnungswesen auswirken. Es sind jene Kontrollen, welche sicherstellen sollen, dass die Geschäfte vollständig und richtig im Jahresabschluss bzw. in den Zwischenabschlüssen abgebildet werden.

4. Abgrenzung übrige Überwachungsfunktionen

Neben der Internen Revision und der externen Revision bestehen im Bereich Überwachung je nach Unternehmen noch weitere Funktionen wie Strategisches Controlling, Risikomanagement oder Compliance. Sofern diese Funktionen an den Verwaltungsrat resp. das Audit Committee rapportieren, können sie als «Assurance-Funktionen» bezeichnet werden. Da alle diese Funktionen einzelne Aspekte des IKS überprüfen, kann es Überlappungen oder Lücken in der Überwachung geben. Es ist deshalb notwendig, dass bereits in der Planungsphase und auch vor den Prüfungen die Koordination sichergestellt wird.

Illustratives Beispiel 1 – Assurance Map

In einem Unternehmen haben die verschiedenen internen und externen Funktionen ihre Prüfungen isoliert durchgeführt. Die Berichterstattung an das Audit Committee erfolgte individuell. Im Auftrag des Audit Committees wurde zur Optimierung der Überwachung die folgende Abbildung 2 erstellt. Sie zeigt auf, welche Ziele und Aufgaben die einzelnen Funktionen erbringen und wo Überschneidungen respektive Lücken bestehen.

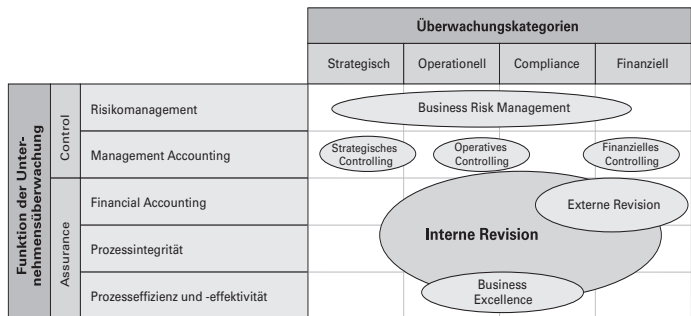


Abb. 2: Assurance Map¹⁰

Für weitere Erläuterungen zur Wechselbeziehung der verschiedenen Funktionen, die das IKS überprüfen, wird auf den Artikel «Interne Revision und Unternehmensüberwachung – von der Konkurrenz zur Kooperation» verwiesen¹¹.

¹⁰ Unter Business Excellence können unternehmensinterne Funktionen zur Steigerung der Performance verstanden werden – z. B. Prozessüberwachung und -optimierung oder Qualitätsmanagement.

¹¹ PALAZZESI/PFYFFER, Kooperation, S. 7 ff.

IV. Kontroll-Modelle

Welches sind nun die konkreten Anforderungen an ein Kontrollsystem? Ziff. 19 Swiss Code impliziert, dass ein IKS von unternehmensspezifischen Faktoren abhängig ist. Als solche Faktoren werden die Grösse und die Komplexität des Unternehmens sowie dessen Risikoprofil angeführt. Unter Beachtung dieser Faktoren muss jedes Unternehmen das optimale Kontrollsystem einrichten und betreiben.

Konkrete Anforderungen an ein wirksames Kontrollsystem finden sich in den internationalen Standards des US-amerikanischen COSO-Frameworks oder im kanadischen Standard Guidance on Criteria of Control (CoCo). Nachfolgend werden diese beiden Regelwerke erläutert. Die US-amerikanische Wertpapier- und Börsenaufsichtsbehörde (Securities and Exchange Commission; SEC) nennt, abgesehen vom COSO-Konzept, auch ausdrücklich das CoCo-Konzept sowie den Turnbull Report der Chartered Accountants in England und Wales als Beispiele für geeignete allgemein anerkannte Kontrollmodelle.

Zwecks Abgrenzung wird in diesem Kapitel auch kurz auf Qualitätsmanagementsysteme¹² eingegangen.

1. COSO-Framework

COSO, welches in den USA eine breite Unterstützung verschiedener Berufsorganisationen genießt, hat die verschiedenen Konzepte und Definitionen von Interner Kontrolle in ein Grundlagenkonzept integriert, in das sogenannte COSO-Framework. COSO definiert Interne Kontrolle als ein Prozess, der beeinflusst wird durch den Verwaltungsrat, die Geschäftsleitung und die Mitarbeiter und der konzipiert ist, eine zweckmässige Sicherheit in Bezug auf die Erreichung der drei folgenden Kernziele zu bieten, nämlich:

¹² Als bekanntestes Beispiel für Qualitätsmanagementsysteme gelten die am Standard ISO 9000 der International Organization for Standardization (ISO) ausgerichteten Qualitätsmanagementsysteme.

- Effizienz und Effektivität der Tätigkeiten;
- Zuverlässigkeit und Integrität der finanziellen Berichterstattung;
- Einhaltung der anwendbaren Normen (Compliance).

Diese drei Kernziele stellen eine der drei Dimensionen des COSO-Würfels dar, wie der Abbildung 3 entnommen werden kann. Diese Kernziele können durch die beiden weiteren Dimensionen – die Komponenten einerseits und die Unternehmen und seine einzelnen Divisionen andererseits – erreicht werden. Die fünf Komponenten

- Steuerungs- und Kontrollumfeld,
- Risikobeurteilung,
- Steuerungs- und Kontrollaktivitäten,
- Information und Kommunikation sowie
- Überwachung

sind für die Kernziele sowie das Unternehmen resp. die einzelnen Divisionen zu definieren, zu implementieren, entsprechend aufeinander abzustimmen und untereinander zu koordinieren.

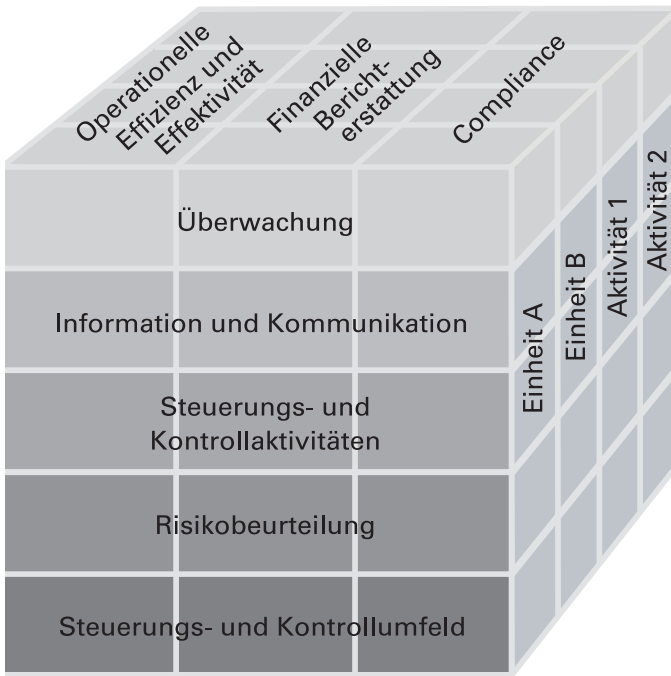


Abb. 3: COSO-Framework

Nachfolgend werden die fünf Komponenten erläutert, wobei die jeweils zu prüfenden Hauptmerkmale angeführt werden¹³.

1.1 Steuerungs- und Kontrollumfeld

Das Steuerungs- und Kontrollumfeld bildet die Grundlage der internen Steuerung und Kontrolle und beeinflusst dadurch die Struktur der Geschäftsaktivitäten und den Umgang mit Risiken. Der Verwaltungsrat und die Geschäftsleitung sind dafür verantwortlich, dass alle erforderlichen Massnahmen getroffen werden, um ein optimales Kontrollumfeld zu gewährleisten¹⁴. Mit ihrem Verhalten prägen

¹³ Siehe dazu die Ausführungen in IV. 1.1–1.5.

¹⁴ Siehe dazu weitere Bemerkungen zu den Mitarbeitern und Vorgesetzten in V. 3.

Verwaltungsrat und Geschäftsleitung die Unternehmenskultur, insbesondere die Risiko- und Kontrollkultur, die durch hohe Integritätsstandards gekennzeichnet sein soll. Die Risikophilosophie und Kontrollkultur sind zu dokumentieren und in schriftlicher Form zu kommunizieren. Mitarbeiter aller Hierarchiestufen müssen ihre Verantwortung, Aufgaben und Zuständigkeiten im Prozess der Internen Kontrolle kennen und verstehen. Dabei tragen Verwaltungsrat und Geschäftsleitung die Verantwortung zur Definition und Implementierung des Steuerungs- und Kontrollumfeldes.

Die Hauptmerkmale des Kontrollumfeldes sind:

- Integrität und gepflegte ethische Werte;
- Verpflichtung zu Kompetenz und Sorgfalt;
- Professionalität des Verwaltungsrats und der Geschäftsleitung sowie die Fachkompetenz und Unabhängigkeit des Audit Committees;
- integre Managementphilosophie und Arbeitsweise;
- angemessene Organisationsstruktur;
- klare Zuweisung von Aufgaben, Kompetenzen und Verantwortung;
- Personalpolitik und deren Umsetzung in Personalrekrutierung, -beurteilung, -honorierung und -entwicklung.

Illustratives Beispiel 2 – Autorität und Verantwortlichkeit

Das Unternehmen hat die Verantwortlichkeiten und die betragslichen Limiten für die Gewährung von Debitorenforderungsverzichten nicht klar geregelt. Der für die Debitoren verantwortliche Buchhalter gewährt einen Forderungsverzicht von CHF 1 Mio., obschon dies nicht zu seinem Verantwortlichkeitsbereich gehört.

Illustratives Beispiel 3 – Verwaltungsrat und Audit Committee

Der Verwaltungsrat eines börsenkotierten Unternehmens wird politisch zusammengestellt. Es wird nicht darauf geachtet, ob die Mitglieder des Verwaltungsrats über die notwendige Branchen- oder Fachkompetenz verfügen. Da kein Mitglied über vertiefte Kenntnisse im Finanz- und Rechnungswesen verfügt, wird auch auf die Bildung eines Audit Committees verzichtet. Das Unternehmen setzt sich dem Risiko aus, dass der Verwaltungsrat nicht in der Lage ist, das Unternehmen angemessen zu kontrollieren.

Illustratives Beispiel 4 – Ethische Werte

Der Vorsitzende der Geschäftsleitung einer grösseren Gesellschaft hält sich nicht an die internen Richtlinien, indem er sich und seine Familie von einem grossen Lieferanten zu Luxusferien einladen lässt. Damit wird er seiner Vorbildfunktion nicht gerecht. Er riskiert, dass sich auch andere Mitarbeiter nicht an interne Vorschriften halten.

1.2 Risikobeurteilung

Risiko wird definiert als die Ungewissheit darüber, ob ein Ereignis eintritt, welches sich auf die Zielerreichung auswirken könnte. Das Risiko wird im Hinblick auf seine quantitativen Auswirkungen und seine Eintrittswahrscheinlichkeit gemessen. Die verschiedenen Risiken, welchen sich ein Unternehmen heute gegenübergestellt sieht, sind komplex und verlangen nach klar strukturierten Risikomanagementprozessen. Unternehmertum ist zwangsläufig verbunden mit dem Eingehen von Risiken; das alte Sprichwort «ohne Risiko kein Gewinn» kommt nicht von ungefähr.

Eine der zentralen Herausforderungen der modernen Unternehmensführung besteht deshalb darin, ein zukunftsorientiertes Risikomanagementkonzept zu definieren, welches mit den bestehenden Planungs- und Führungsprozessen vollständig integriert ist und sowohl auf die

- Verhinderung und Verminderung von Verlustrisiken als auch auf

- die Identifizierung, Analyse und Beurteilung von Chancen ausgerichtet ist¹⁵.

In diesem Rahmen soll das IKS sicherstellen, dass alle Risiken, welche die Erreichung der Geschäftsziele substantiell beeinflussen könnten, zeitgerecht und kontinuierlich erkannt sowie evaluiert werden. In diese Beurteilung sind die Geschäftsrisiken, welche u. a. in folgenden Bereichen des Unternehmens zu finden sind, einzubeziehen:

- Strategie, Planung und Controlling;
- Führung, Organisation;
- Absatz- und Beschaffungsmarkt;
- Leistungserbringung und Produktion;
- Finanzierung und Investition;
- Personal;
- Standort;
- Umwelt.

Das IKS soll zudem die nötige Flexibilität aufweisen, um auf neue oder bisher unkontrollierte Risikotypen rasch und angemessen reagieren zu können.

COSO definiert bezüglich der Risikobeurteilung die folgenden vier zu berücksichtigenden Hauptmerkmale:

- unternehmensweite Zielsetzungen;

¹⁵ Siehe dazu Teil 1, Anhang B, in dem das Enterprise Risk Management (ERM) als ein wichtiger Führungsprozess im Unternehmen beschrieben wird.

- prozessbezogene Zielsetzungen
(z. B. Verkauf, Einkauf, Personal);
- Risikoidentifikation und -beurteilung;
- Umgang mit Änderungen.

Illustratives Beispiel 5 – Risikoidentifikation und -beurteilung

Das Unternehmen tätigt Maschineninvestitionen, ohne die erforderlichen Investitionsüberlegungen vorzunehmen und ohne die Finanzierungsfrage abschliessend geklärt zu haben. Die gekauften Maschinen erweisen sich als überdimensioniert und die Investitionskosten gefährden die Überlebensfähigkeit des Unternehmens.

Ein effizientes und wirkungsvolles Risikomanagement kann durch die Geschäftsleitung nur aufgebaut werden, wenn umfassende Kenntnisse der Geschäftstätigkeiten, der zu erreichenden Ziele sowie der Faktoren, welche diese Zielerreichung gefährden können, vorhanden sind. Zentral ist auch eine prozessorientierte Risikobeurteilung unter Einbezug der verschiedenen Anspruchsgruppen. Diese stellt sicher, dass auch nicht-finanzielle (qualitative) Elemente, z. B. Reputation oder Umweltaspekte, in die Betrachtungsweise einfließen, was die Formulierung von Messgrössen begünstigt und eine zukunftsorientierte Ausgestaltung des Risikomanagements als Frühwarnsystem erlaubt. Risikomanagement hat jeweils auf geeigneten organisatorischen Ebenen stattzufinden. Es ist zudem sicherzustellen, dass sämtliche Informationen bezüglich Risikomanagement in stufengerechtem Aggregations- bzw. Detaillierungsgrad zur Verfügung stehen. Bedeutsam für ein gutes Risikomanagement ist ferner die Zusammenarbeit und offene Kommunikation auf Unternehmensebene sowie zwischen Verwaltungsrat, Geschäftsleitung, Interner Revision, externer Revision und der Funktion des Risikomanagements im Speziellen.

Das Risikomanagement soll auf die Besonderheiten des Unternehmens abgestimmt sein und den spezifischen Eigenheiten Rechnung tragen. Dabei sollen sowohl interne (z. B. Komplexität der Organisationsstruktur oder Geschäftstätigkeit) als auch externe Einfluss-

faktoren (z. B. ökonomische Rahmenbedingungen sowie technologische oder soziologische Entwicklung) berücksichtigt werden.

Jedes Unternehmen sollte eine Strategie zur Handhabung der geschäftsspezifischen Risiken entwerfen, wobei diese stark durch die Risikobereitschaft des Verwaltungsrats und der Geschäftsleitung sowie die Risikofähigkeit des Unternehmers geprägt wird. Wesentlich ist aber, die Summe der Risiken zu kennen, einerseits ausgedrückt in «Bruttorisiken» und andererseits unter Berücksichtigung von getroffenen Massnahmen als «Netto- oder Restrisiken».

Es können vier verschiedene Alternativen zur allgemeinen Handhabung der Geschäftsrisiken verfolgt werden:

- *Vermeiden von Risiken.* Indem auf risikoinhärente Tätigkeiten verzichtet wird, können Risiken gemieden werden, wodurch jedoch gleichzeitig auch Gewinnchancen reduziert werden.
- *Vermindern von Risiken.* Das Unternehmen ergreift Massnahmen, welche potenzielle Auswirkungen von Risiken abschwächen. Hierbei ist eine ausgewogene Balance zwischen der Risikobereitschaft und dem Aufwand zur Aufrechterhaltung von Steuerungs- und Kontrollsystemen zu finden.
- *Überwälzen von Risiken.* Indem sich das Unternehmen versichert, gegen Risiken absichert («hedging») oder unterschiedliche Finanzierungsinstrumente einsetzt, kann es einen Teil der finanziellen Auswirkungen der Risiken an Dritte überwälzen.
- *Selbst-Tragen der Auswirkungen von Risiken.* Entschliesst sich ein Unternehmen, abgesehen von der laufenden Beurteilung, keine spezifischen Massnahmen zur Handhabung von Risiken zu treffen, oder ist sich das Unternehmen der spezifischen Risiken nicht bewusst, so hat es die finanziellen und anderen Auswirkungen beim Eintreten eines negativen Ereignisses selbst zu tragen.

1.3 Steuerungs- und Kontrollaktivitäten

Unter Steuerungs- und Kontrollaktivitäten werden diejenigen Regelungen und Prozesse zusammengefasst, welche sicherstellen sollen, dass die von der Geschäftsleitung geforderten Massnahmen zur Risikoerkennung und -beherrschung ergriffen werden. Die Kontrollaktivitäten bilden einen integralen Bestandteil der Arbeitsprozesse – dabei ist zwischen verfahrensorientierten Ablauf-, resultatorientierten Ergebniskontrollen sowie direkten Verhaltensüberprüfungen zu unterscheiden:

- Ablaufkontrollen haben Zielabweichungen zu einem frühen Zeitpunkt festzustellen, sodass Korrekturen noch leicht möglich sind (ex ante).
- Ergebniskontrollen überprüfen die Zielerreichung mittels Vergleich zwischen Zielvorgaben und tatsächlich erreichten Resultaten. Sie werden eingesetzt, wenn eine unmittelbare Korrektur nicht nötig und/oder nicht möglich ist (ex post).
- Mit Verhaltensprüfungen wird direkt das Verhalten von individuellen und organisatorischen Einheiten überprüft. Sie werden insbesondere eingesetzt, wenn erwartete Resultate nicht beobachtbar sind.

Methodisch kann von verschiedenen Kontrolltypen Gebrauch gemacht werden¹⁶. Für eine wirkungsvolle interne Steuerung und Kontrolle sind, abgesehen von den formellen Kontrollmassnahmen (Gesetze, Weisungen, Ablaufbeschreibungen, Organisationsstrukturen, Funktionentrennung, finanzielle Kontrollen), vor allem auch informelle Kontrollmassnahmen (Wissen, Vertrauen, hohe ethische Standards, Offenheit und Transparenz) erforderlich.

COSO fasst die im Rahmen der Steuerungs- und Kontrollaktivitäten zu beurteilenden Hauptmerkmale wie folgt zusammen:

- Vorhandensein von zweckmässigen Weisungen und Prozessen;
- Wirksamkeit festgelegter Kontrollen.

¹⁶ Siehe dazu weitere Ausführungen zu Kontrollmassnahmen in VI.

Illustratives Beispiel 6 – Wirksamkeit festgelegter Kontrollen

Die interne Weisung eines Unternehmens schreibt vor, dass der für das Warenlager verantwortliche Mitarbeiter die Auslieferung der Waren nur an dazu ermächtigte und in der internen Weisung namentlich aufgeführte Personen vornehmen darf.

Nachdem der Mitarbeiter die erforderliche Auslieferungskontrolle nur ungenügend vornahm und auch der Vorgesetzte die periodische Einhalteprüfung vernachlässigte, wurden Waren an unberechtigte Personen ausgeliefert. Als Konsequenz erlitt das Unternehmen einen finanziellen Schaden.

1.4 Information und Kommunikation

Wie in sämtlichen anderen Managementprozessen, kommt auch im Bereich der Steuerung und Kontrolle der Information und Kommunikation ein besonderer Stellenwert zu. Relevante Informationen sind zu identifizieren, aufzuarbeiten und bezüglich Form und Zeithorizont so zu kommunizieren, dass die zuständigen Personen ihren Verantwortungen nachkommen können.

COSO verweist bezüglich Information und Kommunikation auf die folgenden zwei Hauptmerkmale:

- Qualität der Informationen (vollständig, wahr, klar, adäquat);
- Effektivität der Kommunikation (zeitgerecht und effektiv).

Illustratives Beispiel 7 - Qualität der Informationen

Die von einem Mitarbeiter der Finanzbuchhaltung erstellten Monatsberichte für die Geschäftsleitung wurden seit Monaten nicht durch eine Zweitperson kontrolliert. Erst im Folgejahr wird festgestellt, dass die im jeweiligen Monatsbericht angeführten Vergleichszahlen falsch waren und die Monatsberichte nicht alle wesentlichen Informationen enthielten. Die Analyse der Geschäftsleitung basierte auf unzureichenden Informationen und verliert an Aussagekraft.

Als Voraussetzung für die Wirksamkeit der Internen Kontrolle gilt, dass geeignete Informationssysteme bestehen, welche sicherstellen, dass alle relevanten Informationen über die betrieblichen Geschäfts-

felder zuverlässig und zeitgerecht erhoben, verteilt und bearbeitet werden (Management-Informationen-System). Als relevante Informationen sind einerseits operationelle, finanzielle und auf die Einhaltung von Compliance bezogene Informationen zu verstehen, welche die Steuerung und Kontrolle eines Unternehmens ermöglichen. Andererseits umfassen sie Informationen betreffend externe Ereignisse, Zustände und Aktivitäten, welche im Sinn eines Frühwarnsystems erfasst werden, der besseren Entscheidungsfindung dienen und die offene Kommunikation des Unternehmens beeinflussen.

Auch auf die stufengerechte Kommunikation von Zielen, Resultaten und Massnahmen der Internen Kontrolle ist besonders Wert zu legen. Sämtliche Mitarbeiter müssen Grundsätze, Zusammenhänge und Abläufe der Internen Kontrolle so weit kennen, als ihre eigene Verantwortung betroffen ist.

Durch die Schaffung geeigneter organisatorischer Strukturen soll der entsprechende, für Koordination und Reaktionsfähigkeit notwendige Informationsfluss sowohl «bottom up» als auch «top down» sowie horizontal und mit der Unternehmensumwelt sichergestellt werden. Von entscheidender Bedeutung ist die qualifizierte Aufbereitung der Informationen sowie die zeitgerechte Rapportierung.

1.5 Überwachung

Die diesbezüglichen COSO-Hauptmerkmale sind:

- Permanente Überwachung;
- Spezialprüfung;
- Berichterstattung bezüglich identifizierter Kontrollschwachstellen inkl. Eliminierung der Schwachstellen.

Illustratives Beispiel 8 – Permanente Überwachung

Das Unternehmen hat zwecks Minimierung von Debitorenverlusten für die Hauptdebitoren Kreditlimiten, basierend auf einer Risikobe-

urteilung, festgelegt. Die Höhe dieser Limiten sollte einmal jährlich anhand einer neuen Risikobeurteilung überprüft werden. Dem Verantwortlichen der Debitorenbuchhaltung war diese Vorschrift nicht bekannt, weshalb die Limiten nie angepasst wurden. Der Vorgesetzte stellte diese fehlende, periodische Überprüfung erst nach drei Jahren und aufgrund eines grösseren Debitorenverlustes fest.

Illustratives Beispiel 9 – Permanente Überwachung

Ein grösseres, börsenkotiertes Unternehmen verzichtet aus Kostengründen auf eine Interne Revision. Der Verwaltungsrat stützt sich ausschliesslich auf die Geschäftsleitung ab. Dadurch nimmt der Verwaltungsrat das Risiko in Kauf, dass das Risk Management und das IKS nicht regelmässig durch eine unabhängige und objektive Funktion überprüft und beurteilt werden.

Die Wirksamkeit der Internen Kontrolle sollte laufend überwacht werden. Mittels permanenter Überwachungsaktivitäten und/oder separater Evaluationen (Spezialprüfungen) sowie der Verbesserung identifizierter Schwachstellen wird sichergestellt, dass das IKS wirkungsvoll bleibt. Durchgeführte Kontrollen sowie Resultate sind in geeigneter Weise möglichst konkret zu dokumentieren.

Die Veränderung von internen und externen Unternehmensbedingungen ist gebührend zu berücksichtigen. Diverse Veränderungen können zu entsprechenden Kontrollmassnahmen Anlass geben: Einführung neuer Produkte, rasches Wachstum einzelner Geschäftsfelder/Aktivitäten, Personalfuktuation, neue Informationssysteme, organisatorische Umstrukturierungen, Fusionen, Veränderungen des gesetzlichen und regulatorischen Umfelds oder Veränderungen der internationalen Tätigkeit.

Im Falle der Feststellung von Abweichungen und Mängeln ist sicherzustellen, dass Korrekturmassnahmen eingeleitet werden. Die betroffenen Stellen und Hierarchiestufen sind zeitgerecht über entsprechende Probleme zu informieren, über schwerwiegende Fälle sind Verwaltungsrat und Geschäftsleitung zu orientieren.

2. COSO-ERM-Framework

Das Enterprise Risk Management-Framework (ERM-Framework) ist eine Weiterentwicklung des COSO-Framework und berücksichtigt zusätzlich die strategischen Kernziele¹⁷. Das ERM-Framework identifiziert und analysiert die Risiken aus einer ganzheitlichen Perspektive. Mit diesem erweiterten Framework steht ein umfassendes Risikomanagementmodell zur Verfügung.

Die fünf ursprünglichen COSO-Komponenten¹⁸ wurden um drei weitere ergänzt:

- Ziele setzen (Objective Setting): u. a. Strategiefestlegung, Risikobereitschaft, Risikotoleranz;
- Ereignisse identifizieren (Event Identification): u. a. Risiken und Chancen, Ereigniskategorien, Ereignisabhängigkeiten;
- Risikobehandlung (Risk Response): u. a. Identifikation und Evaluation möglicher Risikobehandlung.

Die grafische Darstellung zeigt die acht Kontrollkomponenten des COSO-ERM auf, welche sich im Unternehmen und seinen einzelnen Divisionen widerspiegeln.¹⁹

¹⁷ Diese Weiterentwicklung sollte noch im Jahr 2004 in Kraft gesetzt werden.

¹⁸ Siehe dazu weitere Bemerkungen in IV. 1.

¹⁹ Coso, Enterprise Risk Management-Framework, S. 14 ff. Vgl. dazu www.erm.coso.org.

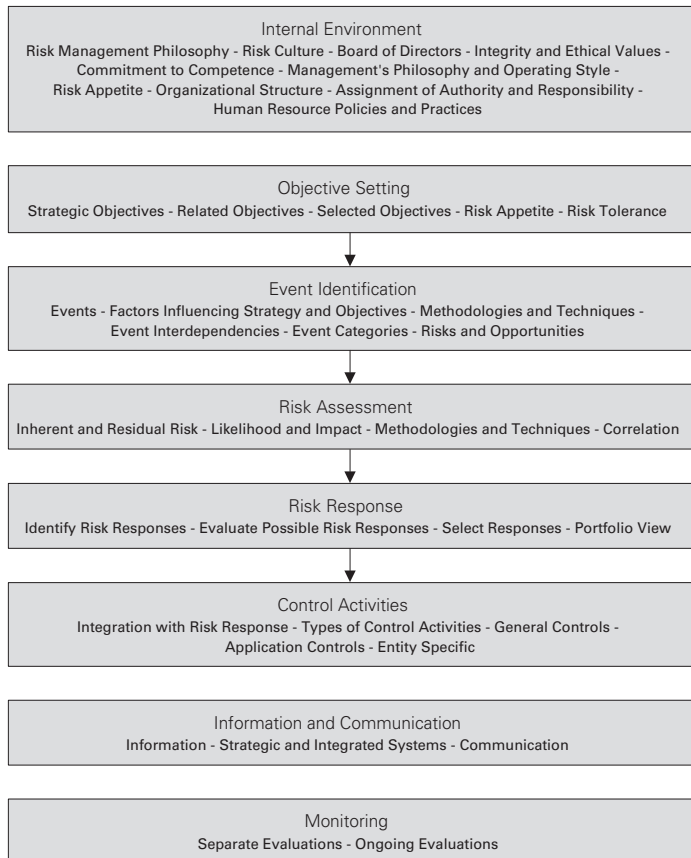


Abb. 4: COSO-ERM-Komponenten

Jede strategische und operative Massnahme ist mit dem Eingehen von Risiken verbunden. Entscheidend für den Unternehmenserfolg ist es, die Risiken in ihrer Gesamtheit zu erkennen, sie richtig einzuschätzen und die risikospezifischen Erkenntnisse in die strategische und operative Führung einzubeziehen. Ein wirkungsvolles ERM bildet im Sinn eines Frühwarnsystems die Voraussetzung für die

bewusste Wahrnehmung der Risiken und schafft die nötige Transparenz für zielgerichtete Führungsentscheide. Ein proaktives ERM-System besitzt die Fähigkeit, Risiken zu antizipieren sowie zu steuern. Dies führt primär zu einer grösseren Planungssicherheit, zu weniger Kontrollfehlern und zu einer höheren Wahrscheinlichkeit, dass Chancen ergriffen und die Unternehmensziele erreicht werden, was sich letztlich in einem höheren Unternehmenswert widerspiegelt.

3. CoCo-Framework

Praktisch gleichzeitig mit dem US-amerikanischen COSO wurde vom Canadian Institute of Chartered Accountants das CoCo-Framework entwickelt. Die CoCo-Zielsetzungen beinhalten:

- Effektivität und Effizienz der Tätigkeiten,
- Zuverlässigkeit der internen und externen Berichterstattung,
- Compliance mit Gesetzen, Verordnungen sowie internen Weisungen

und sind somit praktisch identisch mit den drei Kernzielen von COSO.

Das CoCo-Modell ist dynamischer und managementorientierter als das COSO-Modell. Trotzdem hat sich das kanadische Modell kaum durchgesetzt und wird nur wenig eingesetzt. Für weiterführende Informationen wird auf das kanadische Institut der Wirtschaftsprüfer verwiesen²⁰.

²⁰ Vgl. dazu die folgende Internetadresse: www.cica.ca sowie den Vermerk Guidance on Control.

4. Qualitätsmanagementsysteme

Qualität stellt nicht mehr länger eine isolierte, unabhängige Funktion im Unternehmen dar, sondern erhält eine strategische Bedeutung. Die Qualität ist entscheidend für den Unternehmenserfolg und ermöglicht, Mitbewerber durch überlegene relative Qualität zu übertreffen. Ein Total Quality Management (TQM) verfolgt einen ganzheitlichen Ansatz, wobei die verschiedensten, am Geschäftsprozess beteiligten Parteien und Stellen berücksichtigt werden. Eine permanente Qualitätsüberprüfung ermöglicht Verbesserungen und Weiterentwicklungen des Systems, sodass die Qualität gewährleistet bleibt. Als strategisches Prinzip kann deshalb festgehalten werden: Auf lange Sicht ist der wichtigste Einzelfaktor, der den Erfolg einer Geschäftseinheit bestimmt, die Qualität ihrer Mitarbeiter, Produkte und Dienstleistungen im Vergleich zu ihren Konkurrenten.

Qualitätsmanagementsysteme rücken daher in den Brennpunkt der Unternehmensführung. Dabei steht nicht das System im Vordergrund, mit dem das Unternehmen arbeiten will (z.B. ISO²¹, EFQM²², Six Sigma²³), sondern die Ziele und Anforderungen an ein solches System. Auf operativer Ebene lassen sich vier Aufgabenbereiche unterscheiden:

- Planung, Gestaltung und Entwicklung (Qualitätsplanung);
- Beschaffung, Produktion und Vertrieb (Qualitätslenkung);

²¹ International Organization for Standardization (ISO) verwaltet verschiedene Internationale Standards für Wirtschaft, staatliche Institutionen, Öffentlichkeit und Gesellschaft. Vgl. dazu www.iso.org.

²² European Foundation for Quality Management (EFQM), die das EFQM-Modell erarbeitet hat und bei deren Umsetzung unterstützt. Vgl. dazu www.efqm.com.

²³ Das Ziel von Six Sigma ist ein Umdenken innerhalb des gesamten Unternehmens. Der Kern des Six-Sigma-Ansatzes ist die ständige Verbesserung des Total Quality Managements und die substanzielle Verbesserung von Geschäftsergebnissen. Es ist eine Messgröße für ein Qualitätsmanagement, das Perfektion anstrebt. Das Six-Sigma-Prinzip strebt Strategien an, die auf quantitativem Messen basieren, und versucht, Prozesse zu optimieren, Abweichungen bzw. Streuungen einzuschränken und Fehler oder Qualitätsprobleme aller Art zu eliminieren. Dazu werden etablierte Techniken der Qualitätssicherung mit einfachen und höheren Methoden der Datenanalyse und systematischem Training der Mitarbeiter aller Ebenen einer Organisation kombiniert. Zur Umsetzung von Six Sigma wird im Unternehmen eine Struktur und ein Team mit definierten Rollen und Verantwortlichkeiten benötigt. Vgl. dazu www.quality.de.

- Sicherung (Qualitätssicherung);
- Verbesserung (kontinuierliche Verbesserung).

Im Rahmen von Qualitätszertifizierungen werden in den Unternehmen Qualitätsaudits (z. B. im Rahmen von ISO 2000 Zertifizierungen)²⁴ vorgenommen. Diese Überprüfungen ersetzen das IKS nicht und reichen auch nicht aus, um eine qualifizierte Aussage zu den Internen Kontrollen vornehmen zu können. Die Erkenntnisse aus solchen Audits oder Reviews können trotzdem nützliche Zusatzinformationen zu den Internen Kontrollen liefern und Ansatzpunkte für Verbesserungsmöglichkeiten aufzeigen.

Illustratives Beispiel 10 – Verbesserung

Schon Christoph Kolumbus war bei der erfolgreichen Fahrt seiner «Santa Maria» auf ein Qualitätsaudit angewiesen.

Wir schreiben das Jahr 1492. Christoph Kolumbus befindet sich auf der Suche nach einem kürzeren Seeweg nach Indien. Nach etlichen Tagen Fahrt und zahlreichen Stürmen läuft die Flotte auf die Kanarischen Inseln zu. Navigationsprobleme und Unklarheiten bei der Führung der Mannschaft haben Substanz gekostet.

Kolumbus beauftragt den ersten Offizier, den Problemen nachzugehen und Verbesserungsmaßnahmen vorzuschlagen. Der Offizier findet heraus, dass es zwischen Kapitän und Navigator Missverständnisse bei der Berechnung der neuen Route gegeben hat, was zu Umwegen führte. Zudem hatte die Mannschaft Befehle teilweise falsch interpretiert und durch die Lagerung war ein Teil der Vorräte bereits verdorben.

Die Missverständnisse wurden geklärt, bessere Regeln eingeführt und die Nahrungsmittel richtig gelagert.

²⁴ Manchmal auch als Qualitätsreviews bezeichnet.

5. Implementierung eines Kontrollmodells

In allen Unternehmen werden Interne Kontrollen auf verschiedenen Stufen wahrgenommen, möglicherweise erfolgen diese Kontrollen aber nicht standardisiert und nicht im Rahmen eines umfassenden und anerkannten Kontrollmodells. Soll oder muss (z. B. zwecks Erfüllung der SEC-Anforderungen) ein solches Modell eingeführt werden, sind die folgenden sechs Schritte für eine erfolgreiche Implementierung erforderlich:

- Zusammenstellen eines Projektteams zwecks Evaluation der Kontrollen und Festlegen des Zeitplans;
- Auswahl des Kontrollmodells;
- Beurteilen und Dokumentieren der Internen Kontrollen auf Unternehmensebene;
- Beurteilen und Dokumentieren der Internen Kontrollen auf Prozess-, Transaktions- oder Applikationsstufe (nach Wesentlichkeitsüberlegungen und unter Beachtung der Kernprozesse);
- Beurteilen der Effektivität der Kontrollen und Identifizieren von Schwachstellen, Überwachen der Bereinigungsmassnahmen, inkl. erforderliche Schulung von Mitarbeitern und Vorgesetzten, welche in die Kontrollprozesse involviert sind;
- Erstellen des Management-Kontrollberichts sowie Prüfung und Bestätigung durch die externe Revision.

Die Hauptaufgabe wird vor allem bei der Erstellung oder Ergänzung der Dokumentation liegen, kann doch davon ausgegangen werden, dass vielfach keine oder nur mangelhafte Dokumentationsunterlagen vorhanden sind.

Selbstverständlich muss das Projektteam über die notwendige Unterstützung des Verwaltungsrates und der Geschäftsleitung sowie über die erforderlichen Ressourcen verfügen, z. B. unter Einbezug von IT, der Internen und/oder externen Revision sowie der Ausbildung und Sensibilisierung der Mitarbeiter.

V. Aufgaben und Verantwortlichkeiten

Die Basis für ein funktionierendes Kontrollsystem wird durch eine klare Funktionentrennung zwischen Verwaltungsrat, Geschäftsleitung und Revisionsorganen (Interne und externe Revision) geschaffen. Zur Gewährleistung der notwendigen Unabhängigkeit der einzelnen Funktionen sind Personalunionen möglichst zu vermeiden.

1. Verwaltungsrat

Der Verwaltungsrat²⁵ hat im Rahmen der pflichtbewussten Wahrnehmung seiner unentziehbaren und unübertragbaren Aufgaben gemäss Art. 716a Abs. 1 OR für ein dem Unternehmen angepasstes Risikomanagement und IKS zu sorgen²⁶:

- Das IKS ist der Grösse, der Komplexität und dem Risikoprofil des Unternehmens anzupassen.
- Das IKS deckt, je nach den Besonderheiten des Unternehmens, auch das Risikomanagement ab; dieses bezieht sich sowohl auf finanzielle wie auf operationelle Risiken.
- Das Unternehmen richtet eine Interne Revision ein. Diese erstattet dem Prüfungsausschuss (Audit Committee) und gegebenenfalls dem Präsidenten des Verwaltungsrats Bericht.

Der Verwaltungsrat trifft zudem Massnahmen zur Einhaltung der anwendbaren Normen (Compliance)²⁷:

- Der Verwaltungsrat ordnet die Funktion der Compliance nach den Besonderheiten des Unternehmens; er kann die Compliance dem IKS zuweisen.
- Der Verwaltungsrat gibt sich mindestens einmal jährlich darüber Rechenschaft, ob die für ihn und das Unternehmen an-

²⁵ Siehe dazu die Ausführungen in Teil 1, II. 3 Verwaltungsrat und Geschäftsleitung.

²⁶ Vgl. dazu Ziff. 19 Swiss Code.

²⁷ Vgl. dazu Ziff. 20 Swiss Code.

wendbaren Compliance-Grundsätze hinreichend bekannt sind und ihnen dauernd nachgelebt wird.

Gemäss Art. 716a Abs. 1 Ziff. 1 OR übernimmt der Verwaltungsrat die Oberleitung des Unternehmens. Somit ist der Verwaltungsrat für sämtliche relevanten Entscheide verantwortlich, wobei eine Delegation der Aufgaben möglich und sinnvoll ist²⁸. Die Ausarbeitung der Varianten und Vorlagen kann der Geschäftsleitung übertragen werden, aber der Verwaltungsrat fällt schliesslich die Entscheidungen und trägt die Verantwortung²⁹.

Im Combined Code (Turnbull Report) der London Stock Exchange³⁰ wird die Relevanz für Interne Kontrollen ebenfalls hervorgehoben. Dabei wird die Interne Kontrolle nicht nur allgemein als Anforderung für das Unternehmen formuliert, sondern auch speziell auf den Verwaltungsrat bezogen: «The Board should maintain a sound system of internal control (Principle D.2)».

Der Verwaltungsrat trägt insbesondere die Verantwortung für:

- die Genehmigung und periodische Überprüfung von Entscheidungen mit strategischer Bedeutung;
- die Festlegung adäquater Obergrenzen für ausgewählte und definierte Risikotypen;
- die Sicherstellung der Implementierung der im Rahmen der Internen Kontrolle durch die Geschäftsleitung zu treffenden Massnahmen (Identifikation, Messung, Überwachung und Kontrolle der durch das Unternehmen eingegangenen Risiken);
- die Sicherstellung einer angemessenen Kontrolle der Wirksamkeit von IKS durch die Geschäftsleitung.

²⁸ BÖCKLI, Aktienrecht, §13 N 303.

²⁹ Siehe dazu die Bemerkungen in Teil 1, II. 3.1.3 Delegation der Geschäftsleitung.

³⁰ Entstanden aus den drei Berichten Cadbury, Greenbury und Hampel; die kotierten Unternehmen haben sich seit Ende 2000 umfassend an den vereinheitlichten Kodex zu halten.

Zur Wahrnehmung dieser Verantwortlichkeiten sollte der Verwaltungsrat regelmässig mit der Geschäftsleitung die Effektivität der Massnahmen der Internen Kontrolle erörtern, die Bewertungen von IKS durch die Geschäftsleitung vornehmen lassen, die Internen und externen Revisionen sowie allenfalls die Aufsichtsbehörden zeitgerecht beurteilen und entsprechende Konsequenzen ziehen. Zudem sollte der Verwaltungsrat die Anordnung und Befolgung von Korrekturmassnahmen überwachen und auch die Strategie und Risikolimiten regelmässig überprüfen. Insbesondere kommt dem Verwaltungsrat bei festgestellten Mängeln der Internen Kontrolle die Verantwortung für die Sicherstellung der Umsetzung geeigneter Korrekturmassnahmen zu.

Der Verwaltungsrat kann zur Unterstützung sowie zur eigenen Entlastung im Bereich der Internen Kontrolle ein Audit Committee (Prüfungsausschuss)³¹ einsetzen. Dadurch kann jedoch der Verwaltungsrat nicht von der Gesamtverantwortung für die Interne Kontrolle befreit werden³².

2. Geschäftsleitung

Die Geschäftsleitung trägt die Verantwortung für die Erarbeitung und Umsetzung der vom Verwaltungsrat festgelegten Strategien und Geschäftsgrundsätze³³. Insbesondere ist die Geschäftsleitung verantwortlich für:

- die Entwicklung geeigneter Prozesse für die Identifikation, Messung, Überwachung und Kontrolle der durch die Unternehmen eingegangenen Risiken;
- die Aufrechterhaltung und Dokumentation einer Organisationsstruktur, welche Verantwortlichkeiten, Kompetenzen und Informationsflüsse eindeutig festhält;

³¹ Vgl. dazu das Audit Committee Institute der KPMG Schweiz, das unter der folgenden Internetadresse zu finden ist: www.auditcommittee.ch

³² Siehe dazu die Ausführungen in Teil 1, II. 3.1.1 Oberleitung der Gesellschaft.

³³ Siehe dazu die Ausführungen in Teil 1, II. 3 Verwaltungsrat und Geschäftsleitung.

- die Sicherstellung der Erfüllung delegierter Aufgaben;
- die Überwachung des optimalen Ressourceneinsatzes im Bereich der Internen Kontrolle.

Durch die Verfeinerung der gesetzten Ziele und durch die weitere Delegation der jeweiligen Verantwortlichkeiten werden Mitarbeiter der verschiedenen Ebenen in die Umsetzung der Strategien und in die Wahrnehmung der Internen Kontrolle einbezogen. Die Geschäftsleitung stellt die Quantität und Qualität, insbesondere die Ausbildung und Erfahrung der eingesetzten Mitarbeiter sicher. Die Entlohnungs- und Beförderungsstrukturen dürfen dabei keine Anreize zur Missachtung interner Kontrollmechanismen beinhalten.

3. Mitarbeiter und Vorgesetzte

Die Kontrollverantwortung umfasst alle Mitarbeiter auf allen Stufen (Controls are Everybody's Business). Praktisch alle Mitarbeiter liefern Informationen, welche im IKS gebraucht werden oder aber führen Tätigkeiten aus, welche den Kontrollen unterliegen. Demzufolge sollten alle Mitarbeiter die Grundsätze der Internen Kontrolle kennen und über die betreffenden Kontrollen detailliert informiert sein. Die Mitarbeiter müssen sich ihrer Verantwortung im Kontrollprozess bewusst sein und sicherstellen, dass die ihnen übertragenen Kontrollaufgaben effizient und effektiv ausgeführt werden. Der Mitarbeiterausbildung ist somit die erforderliche Beachtung zu schenken.

4. Interne Revision

Der Swiss Code empfiehlt die Einrichtung einer Internen Revision (Ziff. 19 Swiss Code)³⁴. Das schweizerische Recht schreibt Unternehmen (Ausnahmen gelten für regulierte Finanzgesellschaften) keine Interne Revision vor. Die Tätigkeit der Internen Revision ist nicht an nationale Gesetze oder Verordnungen gebunden, sondern kann weltweit gemäss den gleichen Prinzipien und Konzepten ausgeübt werden. Diese Prinzipien sind im umfangreichen Regelwerk

³⁴ Siehe dazu die Bemerkungen in Teil 1, II. 3.6 Internes Kontrollsystem, Umgang mit Risiken und Compliance.

der Beruflichen Praxis des internationalen Berufsverbandes der Internen Revisoren (IIA)³⁵ zusammengefasst. Insbesondere in multinationalen Unternehmen kann die Interne Revision durch ihre weltweite Tätigkeit und ihre ganzheitliche Sichtweise wertvolle Dienste leisten.

In erster Linie unterstützt die Interne Revision den Verwaltungsrat als oberstes Organ im Unternehmen in der Wahrnehmung seiner Oberleitungsfunktion. In dieser Rolle beurteilt die Interne Revision die Risikomanagement-, Steuerungs- und Kontroll- sowie die Corporate-Governance-Prozesse des Unternehmens, kommuniziert ihre Beobachtungen dem Verwaltungsrat respektive dem Audit Committee und schlägt Prozessverbesserungen vor. Die Interne Revision steht auch der Geschäftsleitung beratend zur Seite, indem sie die verschiedenen Unternehmensführungsprozesse entlang der Wertschöpfungskette beurteilt. Durch die integrierte Sichtweise und die umfassenden Kenntnisse des Unternehmens kann die Interne Revision wirksame Möglichkeiten zur Verbesserung deren Effektivität, Effizienz und Wirtschaftlichkeit aufzeigen. In Ergänzung zu den erwähnten Kernbereichen kann die Interne Revision weitere Tätigkeiten für Funktionen ausüben, die der Internen Revision vorgesetzt sind, in der Regel der Verwaltungsrat.

5. Externe Revision

Die externe Revision ist nicht Bestandteil des IKS, doch wird im Rahmen des risiko-orientierten Prüfungsansatzes die Qualität der Internen Kontrolle berücksichtigt. In den Grundsätzen zur Abschlussprüfung Nr. 14 (GzA)³⁶ wird der Einbezug der Internen Kontrolle in die Planung und Durchführung der Abschlussprüfung behandelt. Demnach muss der Prüfer seine Prüfungshandlungen auf das Prüfungsrisiko ausrichten (Verweis auf GzA 11). Dies bedeutet, dass er die Ausgestaltung der Internen Kontrolle begutachtet und sie in seiner Risikobeurteilung berücksichtigt. In diesem Sinne ist die Prüfung und Beurteilung der Internen Kontrolle ein wichtiger Bestandteil für die Festlegung der Prüfungshandlungen der externen

³⁵ Als «Framework for the Professional Practices» bezeichnet.

³⁶ Die zurzeit gültigen GzA werden per 1. Januar 2005 durch die neuen Schweizer Prüfungsstandards (PS) ersetzt. Siehe dazu weitere Bemerkungen in VII. 5.

Revision, insbesondere bei Unternehmen mit umfangreichen Transaktionsvolumen oder sensitivem Wert- und Datenfluss. Die Prüfung der Internen Kontrollen gibt zudem Aufschluss über den Zustand der Ordnungsmässigkeit von Buchführung und Rechnungslegung. Der Management-Letter über die Befunde der Prüfung liefert damit einen wichtigen Beitrag zur Stärkung und Verbesserung der Unternehmensüberwachung und -kontrolle.

6. Zusammenarbeit der verschiedenen Überwachungsfunktionen

Dem Zusammenwirken der verschiedenen Überwachungsfunktionen wie Interne Revision, externe Revision, aber auch Risk Management kommt eine zunehmend grössere Bedeutung zu. Sie leisten einen wichtigen Beitrag zur Unternehmensentwicklung, indem bestimmte Aufgabenbereiche kontrolliert, die Einhaltung von Vorgaben, Gesetzen und Vorschriften überprüft oder Fehler und Unregelmässigkeiten aufgedeckt werden. Die Überwachungsfunktionen sind sowohl Bestandteil des IKS als auch dessen Prüfinstanzen³⁷.

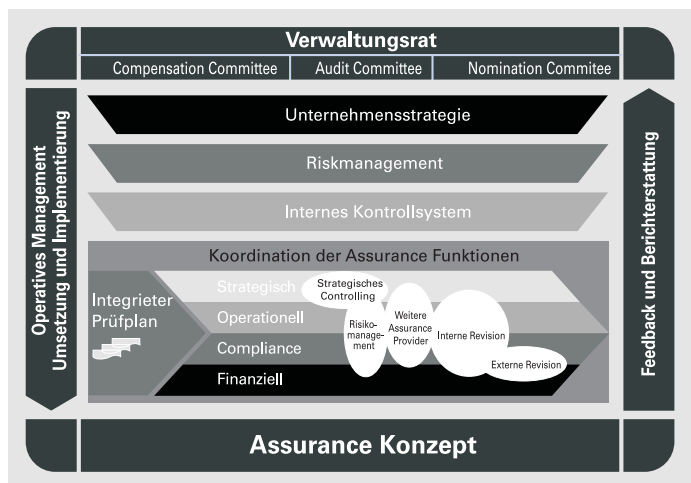


Abb. 5: Assurance-Konzept

³⁷ Siehe weitere Ausführungen in IV. 1.5.

Ein umfassendes Assurance-Konzept bildet die notwendige Voraussetzung, damit die verschiedenen Kontroll- und Überwachungsprozesse beurteilt und abgestimmt werden können. Zudem unterstützt es die Koordination der unterschiedlichen Tätigkeiten, sodass Sicherheit und die Effektivität bezüglich der Assurance-Aktivitäten gewährleistet werden können. Es geht darum, Lücken und Doppel-spurigkeiten in der Prüfungsabdeckung zu vermeiden. Der Verwaltungsrat, das Audit Committee und das Management zeichnen für die Implementierung respektive die Umsetzung verantwortlich.

VI. Kontrollmassnahmen

1. Kontrollmassnahmen

Kontrollen sind die einzelnen Vorgänge, Methoden und Massnahmen, welche im Rahmen eines IKS getroffen werden. Der Zeitdruck darf nicht zum Entscheidungsfaktor werden, ob und wie Kontrollen vorgenommen werden. Selbstverständlich sind dabei alle Einheiten eines Unternehmens im In- und Ausland (Abteilungen, Stellen, Tochtergesellschaften) in den Kontrollprozess einzubeziehen.

Die Kontrollmassnahmen lassen sich in drei unterschiedliche Kategorien einteilen:

- präventive und detektive Kontrollen;
- selbsttätige, programmierte und manuelle Kontrollen;
- Kontrollen durch die Geschäftsführung.

1.1 Präventive und detektive Kontrollen

Als *präventive Kontrollen* werden zwangsläufige Kontrollen, die auftauchende Fehler unmittelbar feststellen, bezeichnet. Mit präventiven Kontrollen soll verhindert werden, dass Fehler überhaupt gemacht werden. Präventivkontrollen können in Form von selbsttätigen Kontrollen, Management- oder unabhängigen Kontrollen, manuellen oder programmierten bzw. automatisierten Kontrollen bestehen. Von zentraler Bedeutung ist, dass diese vorsorglichen Kontrollen in der richtigen Form und an der sachlich geeigneten Stelle angesetzt werden, z.B. Funktionentrennung, Passwörter und Zugriffsvorschriften, physische Schutzvorkehrungen.

Unter *detektiven Kontrollen* werden sogenannte Aufdeckungskontrollen verstanden. Diese werden u. a. vorgenommen, wenn bei der Überprüfung von präventiven Kontrollen eine zu grosse Fehlerhäufigkeit aufgetreten ist, z. B. Durchsicht von Kontrollberichten, Abstimmungen, physische Inventur, Reviews.

Illustratives Beispiel 11 – Detektive Kontrollen – Präventive Kontrollen

Das Unternehmen hat die gesetzliche Pflicht, auf Ende des Geschäftsjahres ein Inventar aufzustellen (Art. 958 Abs. 1 OR). Dieses basiert entweder auf einer Stichtagsinventur oder auf der Übernahme der Bestände aus einer Lagerbuchhaltung.

Das Unternehmen nimmt die vorgeschriebene physische Inventur vor und stellt fest (detektiv), dass wesentliche Bestandesdifferenzen bestehen. Die weiteren Abklärungen zeigen, dass die Lagerräume nicht wie vorgesehen abgeschlossen werden (präventiv).

1.2 Selbsttätige, programmierte und manuelle Kontrollen

Die *selbsttätige Kontrolle* ist die wirksamste, effizienteste wie auch wirtschaftlichste Kontrolle, da sie durch organisatorische oder technische Massnahmen direkt in die betrieblichen Abläufe integriert ist. Organisatorische Massnahmen sind z.B. Funktionentrennung, Errichten von Kompetenzstufen und Regelung von Arbeitsabläufen.

Unter *programmierten Kontrollen* können z.B. Prüfziffern, Kontrollsummen oder Datenabgleich eingeordnet werden.

Die *manuellen Kontrollen* ergänzen die programmierten Kontrollen, z.B. Genehmigungen, kritische Durchsicht, Abstimmungen, physische Kontrollen, Durchsicht von Fehlerlisten.

Selbsttätige, programmierte und manuelle Kontrollen (Organisatorische Massnahmen)		Organisatorische Hilfsmittel
Steuerung und Kontrolle durch die vom Unternehmen gewählten Vorgehensweisen, z.B. durch: <ul style="list-style-type: none"> ■ Funktionentrennung ■ Kompetenzstufen, Genehmigungen ■ Regelung der Arbeitsabläufe 	Steuerung und Kontrolle durch die Anwendung technischer Hilfsmittel, z.B. durch: <ul style="list-style-type: none"> ■ Messeinrichtungen ■ Sicherungsvorrichtungen ■ IT-Kontrollen, z.B. Prüfziffern, Kontrollsummen 	Organisationsplan, Handbücher, Ablauf- und Funktionsdiagramm, Formular- und Belegwesen, Kontierungsvorgaben, Nummern- und Abstimmkreise, Zeiterfassung, Unterschriftenregelung, Visaordnung, Sperrcodes usw.

Tabelle 1: Organisatorische Massnahmen und Hilfsmittel zur Steuerung und Kontrolle

Illustratives Beispiel 12 – Funktionentrennung

Der für den Einkauf zuständige Mitarbeiter kann alle Bestellungen selbständig vornehmen und die Rechnungen zur Zahlung freigeben. Nachdem der Mitarbeiter zudem die materielle Eingangskontrolle der bestellten Waren vornimmt, wird erst bei einer längeren Abwesenheit des Mitarbeiters festgestellt, dass über Jahre Rechnungen für nicht tatsächlich an das Unternehmen gelieferte Waren bezahlt wurden und der Mitarbeiter mit dem Mitarbeiter des Zulieferers zum Schaden des Unternehmens gehandelt hat.

In Fällen, in denen eine Funktionentrennung aufgrund der Unternehmensgrösse nicht vollständig implementiert werden kann, ist besonders Wert auf eine entsprechend höhere Kontrollverantwortung der Vorgesetzten zu legen.

1.3 Kontrollen durch die Geschäftsleitung

Die unabhängige Kontrolle von Führungsverantwortlichen (u. a. Verwaltungsrat, Geschäftsleitung) beruht auf dessen Fachkenntnis und auf der Wahrnehmung der Führungs- und Überwachungsaufgaben. Beispiele sind: Output-Reviews u. a. bei fehlender Funktionentrennung bei kleinen Einheiten oder das Beurteilen von Budgetabweichungen bei fehlenden Transaktionskontrollen. So sollten alle

betroffenen Hierarchieebenen (inkl. Verwaltungsrat und Geschäftsleitung) regelmässig (täglich, wöchentlich, monatlich) stufengerechte Performance-Berichte erhalten und kritisch prüfen (z. B. Entwicklung der Finanzresultate im Verhältnis zu Budget und Zielsetzungen).

Unabhängige Kontrollen durch die Geschäftsleitung		Organisatorische Hilfsmittel
Steuerung und Kontrolle durch Geschäftsleitung und Kader: <ul style="list-style-type: none"> ■ Gestützt auf interne Weisungen ■ Nach freiem persönlichen Ermessen 	Steuerung und Kontrolle durch Beauftragte (Delegationsprinzip): <ul style="list-style-type: none"> ■ Assistenten, Stabsstellen, Ausschüsse, Sekretariate, Projektorganisationen ■ Externe Fachleute und Berater 	Geschäftsreglemente, Pflichtenhefte, Genehmigungsverfahren, Budgets, Vorschlags- und Antragswesen, Terminliste usw.

Tabelle 2: Unabhängige Kontrollen durch die Geschäftsleitung und Hilfsmittel zur Steuerung und Kontrolle

Illustratives Beispiel 13 – Kontrollen durch die Geschäftsleitung

Die Geschäftsleitung erhält monatlich von der Finanzbuchhaltung die Monatsresultate, versehen mit Vormonats- und Vorjahreszahlen. Die Geschäftsleitungsmitglieder sind angehalten, diese Monatsberichte kritisch zu sichten. Anlässlich der monatlichen Sitzung werden die Monatsberichte besprochen und allfällige Fragen vom Leiter der Finanzbuchhaltung beantwortet. Dies wird im Sitzungsprotokoll dokumentiert.

2. Kontrollrisiken

Unter Kontrollrisiko sind Risiken zu verstehen, welche sich aus Schwächen und/oder Ausfällen der Internen Kontrolle ergeben. Indem bestimmte Kontrollen zwar vorgesehen, aber nicht oder nur ungenügend wirksam sind, oder Mitarbeiter und Vorgesetzte ihre Überwachungsfunktion nicht wahrnehmen, entsteht das Risiko von Fehlern oder Unregelmässigkeiten. Dazu gehören zum Beispiel:

- Veruntreuung von Geldern oder Vermögensgegenständen;
- In-Rechnung-Stellen von Waren oder Dienstleistungen, die nicht tatsächlich an das Unternehmen geliefert wurden;
- rechtswidrige Geschäfte, die zum Beispiel gegen Gesetze, Vorschriften, Verordnungen oder Verträge verstossen;
- Annahme von Bestechungs- oder Schmiergeldern;
- Weitergabe eines gewinnversprechenden Geschäftes an einen Mitarbeiter privat oder einen Dritten, das normalerweise dem Unternehmen Gewinn einbringen würde;
- vorsätzliches Verschweigen oder Fehldarstellung von Ereignissen oder Daten.

VII. Überprüfung der Internen Kontrollen

Die Fragestellungen bezüglich Kontrollen haben sich mit der Zeit verändert. Klassischerweise standen etwa die folgenden Schlüsselfragen im Vordergrund:

- Werden die Geschäftsprozesse in Übereinstimmung mit den Vorgaben ausgeführt?
- Sind die Kontrollen innerhalb der Geschäftsprozesse adäquat definiert und wirkungsvoll umgesetzt?
- Sind die finanziellen Ergebnisse bzw. Messgrößen in Übereinstimmung mit dem Plan?

Oder anders ausgedrückt: Machen wir die Sachen richtig? Damit hatten die Kontrollen einen klar operativen und prozessorientierten Fokus. In neuerer Zeit sind zusätzliche Fragen dazugekommen, z. B.:

- Ist das Unternehmen darauf ausgerichtet, den Unternehmenswert für den Aktionär (sowie weitere Stakeholder des Unternehmens) zu erhöhen und nachhaltig zu sichern?
- Werden die Geschäftsrisiken (im Sinn von Chancen und Gefahren) kontinuierlich und umfassend adressiert?
- Sind die Geschäftsprozesse im Hinblick auf die Erreichung der strategischen Ziele richtig definiert?

Oder anders ausgedrückt: Machen wir die richtigen Sachen? Somit sind strategische Elemente dazugekommen und der Fokus hat sich in Richtung Risikomanagement und Risikokontrolle verlagert.

1. Verwaltungsrat und Audit Committee

Die vom Verwaltungsrat respektive vom Audit Committee vorgenommenen Prüfungen und Analysen müssen eine zuverlässige Beurteilung ermöglichen, damit genügend Klarheit über die Wirksamkeit der Internen Kontrollen besteht. Wie bereits eingangs erwähnt,

verlangen die US-amerikanischen Vorschriften die Überprüfung anhand eines anerkannten Kontrollmodells. Das COSO-Framework beinhaltet ein Prüfprogramm mit rund 300 Punkten, basierend auf den fünf COSO-Komponenten, und stellt damit ein nützliches Kontrollinstrument zur Verfügung. Anhang A zeigt ein Beispiel einer Beurteilungsmatrix, welche die wesentlichen Risiken identifiziert und auf die drei Kernziele ausgerichtet ist. Dies erlaubt es, pro Ziel ein Rating abzugeben, wie z. B. gut, zufriedenstellend, mit Vorbehalt, ungenügend. Abgesehen von den speziell auf die Wirksamkeit der Internen Kontrollen ausgerichteten Prüfungen sollte der Verwaltungsrat resp. das Audit Committee permanent die wesentlichen Berichte zur Internen Kontrolle erhalten und beurteilen. Dazu gehören ebenfalls die Berichte der Internen oder externen Revision.

Der Verwaltungsrat beurteilt jährlich seine Leistung und jene seiner Mitglieder (Ziff. 14 Punkt 4 Swiss Code). Mit dieser jährlich verlangten Standortbestimmung (Selbstevaluation) soll der Verwaltungsrat Rechenschaft darüber ablegen, in welchen Bereichen Schwächen aufgetreten sind oder in welchen Punkten die Corporate Governance verbessert werden muss³⁸.

2. Geschäftsleitung

Die Geschäftsleitung hat im Rahmen ihrer Führungsverantwortung ebenfalls dafür zu sorgen, dass das IKS effizient und wirkungsvoll ist. Analog dem Verwaltungsrat resp. dem Audit Committee können die Überprüfungen im Arbeitsprozess integriert sein (Arbeitsberichte) oder in Form von Direktprüfungen erfolgen. Die Geschäftsleitung hat zudem gegenüber dem Verwaltungsrat Rechenschaft über die Wirksamkeit der Internen Kontrollen abzulegen.

3. Control (Risk) Self Assessment

Nebst der herkömmlichen Prüfungen zur Beurteilung der Steuerungs- und Kontrollprozesse können auch Control Self Assessments durchgeführt werden, wodurch ebenfalls Kontrollschwachstellen

³⁸ Zu Fragen, die von Mitgliedern eines Audit Committees an die Unternehmensorgane und an Fachverantwortliche gestellt werden könnten, siehe Teil 1, Anhang D.

identifiziert und daraus abgeleitete Massnahmen zu deren Behebung eingeleitet werden können. Control Self Assessment ist ein formeller, dokumentierter Prozess, in dem die Geschäftsleitung und Mitarbeiter, welche direkt in die Geschäftsprozesse eingebunden sind, ihre Geschäftsprozesse auf folgende Punkte analysieren:

- Risiken und Gefahrenpotenziale identifizieren;
- Steuerungs- und Kontrollprozesse, welche diese Risiken mindern oder managen sollen, beurteilen;
- einen Massnahmenplan entwickeln, welcher die Risiken auf ein akzeptables Niveau reduziert;
- Möglichkeiten zur Verbesserung von Effektivität und Effizienz der Prozesse ermitteln;
- die Wahrscheinlichkeit der Erreichung der Unternehmensziele bestimmen.

Mit dem Einsatz von Control Self Assessments lässt sich ebenfalls das Verständnis für Risikomanagement auf allen Führungsstufen merklich steigern. Bei der Durchführung von Control Self Assessments übernimmt die Interne Revision oft die Rolle eines Moderators, wodurch einerseits eine partnerschaftliche Arbeitsweise gepflegt werden kann und andererseits die Risikoeinschätzungen und Hinweise aus den Workshops für zukünftige Revisionsplanungen verwendet werden können.

4. Interne Revision

Die Interne Revision hat die Angemessenheit und Effektivität des IKS zu beurteilen. Bei der Erfüllung dieser Aufgabe soll die Interne Revision u.a. feststellen, ob:

- das organisatorische Umfeld das Kontrollbewusstsein fördert;
- die organisatorischen Zielsetzungen realistisch sind;

- geeignete Genehmigungsverfahren für Transaktionen festgelegt und angewandt werden;
- Richtlinien, Verfahren, Berichte und andere Mechanismen zur Überwachung von Aktivitäten und Sicherung von Vermögenswerten – vor allem in Bereichen mit hohem Risiko – entwickelt sind;
- vorhandene Informationsmittel dem Verwaltungsrat und der Geschäftsleitung angemessene und zuverlässige Informationen zur Verfügung stellt;
- Verhaltensnormen bestehen, in denen verbotene Tätigkeiten sowie Sanktionen bei aufgedeckten Verstössen festgelegt sind.

Vorstellbar und wünschenswert ist es, dass die Aufgabenstellungen der Internen Revision spezifische Review-Arbeiten des IKS beinhalten und damit u.a. die Grundlage für den gemäss dem SOX und anderen Corporate-Governance-Standards vom Verwaltungsrat geforderten Bericht über die Interne Kontrolle bilden. Denkbar ist auch, dass die Interne Revision die Richtigkeit und Vollständigkeit der Corporate-Governance-Informationen des für Schweizer Publikumsgesellschaften verlangten zusätzlichen Kapitels im Geschäftsbericht beurteilt.³⁹

Weniger aus Kosten- als vielmehr aus Reputationsgründen ist eine konsequente Qualitätssicherung und Verbesserung der Aufgabenerfüllung der Internen Revision wichtig. Die Qualitätsbeurteilung der Arbeit der Internen Revision soll periodisch erfolgen – einerseits durch qualifizierte Stellen innerhalb des Unternehmens und andererseits durch externe Spezialisten (z. B. Revisionsgesellschaften, Berufskollegen von anderen Internen Revisionsabteilungen).

5. Externe Revision

Die externe Revision hat im Rahmen von Verfahrensprüfungen Prüfungshandlungen vorzunehmen, welche Rückschlüsse betref-

³⁹ Vgl. dazu Richtlinie betreffend Informationen zur Corporate Governance der SWX Swiss Exchange.

find die Wirksamkeit der Internen Kontrollen erlauben. Die stichprobenweise Prüfung der Kontrollen umfasst normalerweise die Einhalteprüfungen (formelle Prüfung) sowie allenfalls auch den Nachvollzug der Kontrollen (materielle Prüfung). Zur Dokumentation des Kontrollumfeldes und der Kontrollen stehen verschiedene Techniken zur Verfügung, z. B. Fragebogen, Checklisten oder Ablaufdiagramme. Die externe Revision kann sich teilweise auf Arbeiten und Ergebnisse Dritter (z. B. der Internen Revision) stützen, muss dann aber ein eigenständiges Urteil bilden, damit sie sich zur Festlegung ihrer Prüfungshandlungen auf die Interne Kontrolle abstützen kann.

Die für die externe Revision geltenden Standards sind u. a.:

- in der Schweiz: Schweizer Handbuch der Wirtschaftsprüfung HWP sowie Grundsätze für die Abschlussprüfung (GzA);
- in Grossbritannien: Turnbull Report;
- in den USA: Public Company Accounting Oversight Board (PCAOB) Standards sowie US Generally Accepted Auditing Standards (US GAAS);
- international: International Standards on Auditing (ISA).

6. Gesetzgeber und Aufsichtsbehörden

Im Rahmen der verschiedenen Aufsichtstätigkeiten (Kontrollstelle für Geldwäscherei, Bundesamt für Privatversicherungen, Eidgenössische Bankenkommission, Bundesamt für Zivilluftfahrt, Kantonschemiker, Lebensmittelinspektoren) werden Aspekte kontrolliert, die allgemein als schutzwürdig erachtet werden. Diese Aufsichtsbehörden stellen durch gezielte Kontrollen sicher, dass die Interessen beispielsweise der Konsumenten oder Investoren gewahrt und die zum Schutz dieser Gruppen erlassenen Gesetze und Verordnungen eingehalten werden. Die Aufsichtsstellen sind mit den notwendigen Kompetenzen versehen, Kontrollen durchzuführen und bei Mängeln die erforderlichen Massnahmen einzuleiten.

VIII. Zusammenfassung und Ausblick

Nachdem sehr oft bezüglich Internen Kontrollen falsche oder unklare Vorstellungen bestehen, halten wir hier einige wesentliche Merkmale fest:

- Die Interne Kontrolle basiert auf einer implementierten und von Verwaltungsrat sowie Geschäftsleitung vorgelebten Kontrollkultur.
- Die Kontrollverantwortung umfasst alle Mitarbeiter auf allen Ebenen, wobei die Hauptverantwortung beim Verwaltungsrat liegt.
- Die Internen Kontrollen decken alle Geschäftsbereiche ab und sind in die entsprechenden Geschäftsprozesse integriert.
- Die Internen Kontrollen geben eine erhöhte, aber nicht absolute Gewissheit, dass die geschäftspolitischen Ziele erreicht werden.
- Die Internen Kontrollen können – mit oder ohne Absicht – umgangen werden.
- Die Interne Revision überprüft die Internen Kontrollen.
- Die externe Revision begutachtet die Ausgestaltung der Internen Kontrollen und berücksichtigt diese in ihrer Risikobeurteilung und Festlegung ihrer Prüfungshandlungen.

Die in den vergangenen Jahren erarbeiteten nationalen und internationalen Regelwerke haben die Anforderungen an die Corporate Governance und damit auch an die Interne Kontrolle erheblich verstärkt. Es ist zu erwarten, dass diese Regelwerke weiteren Anpassungen unterworfen werden. So ist nicht auszuschliessen, dass sich Aufsichtsbehörden bei der Ausgestaltung ihrer eigenen Bestimmungen in Teilbereichen z. B. auf das sehr detaillierte, aber auch sehr formalistische SOX stützen werden.

Beurteilungsmatrix Internes Kontrollsystem

Beurteilungsmatrix Internes Kontrollsystem

Komponenten	Zu beurteilende Hauptmerkmale	Wesentliche Risiken	Beurteilung der Kernziele (Rating):		
			Effizienz und Effektivität der Tätigkeiten	Zuverlässigkeit und Integrität der finanziellen Berichterstattung	Compliance mit Gesetzen und Normen
Steuerungs- und Kontrollumfeld	<ul style="list-style-type: none"> - Integrität und im Unternehmen gepflegte ethische Werte - Verpflichtung zu Kompetenz und Sorgfalt - Verwaltungsrat und Audit Committee - Managementphilosophie und Arbeitsweise - Angemessenheit der Organisationsstruktur - Klare Zuweisung von Autorität und Verantwortlichkeit - Personalpolitik (Weisungen und Praxis) 	z. B. <ul style="list-style-type: none"> - Kein bzw. nicht kommunizierter oder nicht gelebter Verhaltenskodex - Verwaltungsrat und/oder Audit Committee nicht aktiv, nicht unabhängig oder schlecht informiert 	G	Z	G
Risikobeurteilung	<ul style="list-style-type: none"> - Unternehmensweite Zielsetzungen - Prozessbezogene Zielsetzungen - Risikoidentifikation und -beurteilung - Umgehen mit Änderungen 	z. B. <ul style="list-style-type: none"> - Zielsetzungen werden nicht hinsichtlich Risiken überprüft - keine Risikokultur implementiert - unterschiedliches Risikoverständnis innerhalb Management - Risikoappetit nicht definiert - Risikomanagement-Funktion nicht akzeptiert 	V	V	V
Steuerungs- und Kontrollaktivitäten	<ul style="list-style-type: none"> - Vorhandensein zweckmässiger Weisungen und Prozesse - Wirksamkeit festgelegter Kontrollen 	z. B. <ul style="list-style-type: none"> - IKS nur ansatzweise vorhanden - Weisungswesen nicht organisiert - Kontrollen funktionieren nicht - IKS wird nicht regelmässig überprüft 	Z	G	Z
Information und Kommunikation	<ul style="list-style-type: none"> - Qualität der Informationen (zeitgerecht und effektiv) - Effektivität der Kommunikation (Kommunikationswege und -mittel) 	z. B. <ul style="list-style-type: none"> - MIS liefert keine zeitgerechten Informationen - Auslandsgesellschaften haben keinen Zugriff aufs Intranet - Konzern- und Tochtergesellschaftsinformationen sind nicht konsistent - Konzernleitungsmitglieder widersprechen sich 	U	G	G
Überwachung	<ul style="list-style-type: none"> - Permanente Überwachung - Sonderprüfung - Berichterstattung identifizierter Kontroll-Schwachstellen, inkl. Eliminierung der Schwachstellen 	z. B. <ul style="list-style-type: none"> - es gibt keine interne Revisionsfunktion - Empfehlungen der externen und Internen Revision werden nicht umgesetzt - Audit Committee setzt sich aus Mitgliedern ohne Finanzkenntnisse zusammen 	U	G	U

Rating: G = Gut; Z = Zufriedenstellend; V = mit Vorbehalt; U = Ungenügend

Kontrollkomponenten Glossar

Kontrollkomponenten Glossar

Angemessene Steuerung und Kontrolle (Adequate Control) – Eine angemessene Steuerung und Kontrolle ist dann gegeben, wenn die Geschäftsleitung durch die Art seiner Planung und Organisation (Aufbau) hinreichend sicherstellt, dass die Risiken des Unternehmens wirksam zu «managen» sind und seine Ziele effizient und wirtschaftlich erreicht werden.

Assurance-Dienstleistungen (Assurance Services) – «Assurance Services» sind unabhängige Prüfungsdienstleistungen, welche die Qualität von entscheidungsrelevanten Informationen – d. h. insbesondere deren Zuverlässigkeit und Relevanz – erhöhen. Durch die Unabhängigkeit, Objektivität, Fachkompetenz und Sorgfalt sowie die umfassenden Unternehmenskenntnisse ist die Interne Revision geeigneter Anbieter von Assurance-Dienstleistungen. Beispielhaft seien hier Prüfungen (Audits) in den Bereichen Finanzen, Compliance oder Systemsicherheit genannt.

Beratungsleistungen (Consulting Services) – Beratungs- und ähnliche Kundendienstleistungen, deren Art und Umfang mit dem Kunden vereinbart sowie darauf ausgerichtet sind, die Aktivitäten des Unternehmens zu verbessern sowie die Zielerreichung zu unterstützen. Als Beispiele können beratende und verwandte Dienstleistungen («counsel», «advice», «facilitation») wie Moderation bei der Durchführung von Control Self Assessments, der Einbezug in die Prozessoptimierung oder die Weiterbildung der Mitarbeitenden genannt werden.

CoCo – Kontroll-Modell analog COSO, aber dynamischer mit den vier Elementen: Zielsetzung, Zusicherung, Möglichkeiten, Überwachung.

Corporate Governance-Prozesse – Die Regeln und Grundsätze sowie die Strukturen, Strategien und Verfahren, durch die ein Unternehmen geleitet und kontrolliert wird, um seinen Verantwortlichkeiten gegenüber den unterschiedlichen Anspruchsgruppen nachzukommen.

COSO – Das COSO-Framework ist ein Konzept der internen Steuerung und Kontrolle. Es umfasst die fünf Elemente (i) Steuerungs- und Kontrollumfeld, (ii) Risikobeurteilung, (iii) Kontrollaktivitäten, (iv) Information und Kommunikation sowie (v) Überwachung.

Einhaltung von Compliance – Die Fähigkeit, in hinreichendem Mass die Übereinstimmung und die Einhaltung von Unternehmensrichtlinien, Plänen, Verfahren, Gesetzen, Verordnungen und Verträgen sicherzustellen.

Enterprise Risk Management (ERM) – Der gezielte Umgang mit Risiken. Wichtig sind dabei eine sorgfältige Priorisierung bei der Beurteilung der verschiedenen Risikofaktoren und die bewusste Handhabung des Risikopotenzials.

Externer Dienstleistungsanbieter (External Service Provider) – Vom Unternehmen unabhängige Person oder Firma, die über Spezialwissen, Fähigkeiten und Erfahrungen in einem bestimmten Fachgebiet verfügt. Zu den externen Dienstleistungsanbieter gehören u. a. Aktuariere, Versicherungsmathematiker, Fachleute des Rechnungswesens, Schätzer, Umweltschutzexperten, Ermittler in Fällen doloser Handlungen, Rechtsanwälte, Ingenieure, Geologen, Sicherheitsexperten, Statistiker, Informationstechnologie-Fachpersonen, Wirtschaftsprüfer des Unternehmens und andere Audit-Organisationen.

Grundsätze zur Abschlussprüfung (GzA) – Normen der Treuhänder-Kammer, welche die Qualität der Abschlussprüfung gewährleisten und zu einer einheitlichen Prüfungspraxis führen sollen. Die derzeit gültigen GzA werden per 1. Januar 2005 durch die neuen Schweizer Prüfungsstandards (PS) ersetzt.

Interne Revision – Die Interne Revision ist eine Abteilung, ein Unternehmensbereich oder ein Team von Fachpersonen, die unabhängige, objektive Prüfungs- und Beratungsleistungen erbringen und darauf ausgerichtet sind, Mehrwerte zu schaffen sowie die Geschäftsprozesse zu verbessern. Die Interne Revision unterstützt ein Unternehmen bei der Erreichung seiner Ziele, indem es mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Steuerung und Kontrollen sowie der Corpora-

te-Governance-Prozesse bewertet und diese verbessern hilft. Die Interne Revision kann auch als Dienstleistung von externen Anbietern bezogen werden (z. B. von Wirtschaftsprüfungsgesellschaften). Im Rahmen des vorliegenden Teils umfasst der Begriff «Interne Revision» stets auch die externen Dienstleistungsanbieter.

Interne Kontrolle – siehe Steuerung und Kontrolle.

Qualität – Qualität bedeutet die Gesamtheit von Merkmalen und Merkmalswerten einer Einheit bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen.

Risiko (Risk) – Gefahr des Eintretens eines Schadensfalles bzw. Vermögensverlustes oder Entgehung einer Chance. Ein hohes Risiko entspricht einer hohen Eintretenswahrscheinlichkeit und/oder einem hohen Verlustpotenzial.

Risikokontrolle (Risk Control) – Unabhängige Überwachung des eingegangenen Risikoprofils des Unternehmens. Risikokontrolle legt die Grundlage der unternehmerischen Risikopolitik (Risk Policy), der Risikobereitschaft (Risk Appetite) sowie der Risikolimiten, die von den zuständigen Stellen zu erlassen sind, und überwacht die Einhaltung des dadurch festgelegten Rahmens.

Risikomanagement (Risk Management) – Umfassende und systematische Steuerung und Lenkung von Risiken auf der Grundlage wirtschaftlicher und statistischer Kenntnisse. Risikomanagement umfasst die Identifikation, Messung, Beurteilung, Steuerung und Berichterstattung über einzelne wie auch über aggregierte Risikopositionen.

Steuerung und Kontrolle (Control) – Jede von der Geschäftsleitung, vom Verwaltungsrat oder von anderen Stellen eingeleitete Massnahme, die das Risikomanagement verbessert und die Wahrscheinlichkeit erhöht, dass gesetzte Ziele erreicht werden. Das bekannteste Konzept zur internen Steuerung und Kontrolle ist das COSO-Framework.

Steuerungs- und Kontrollprozesse (Control Processes) – Richtlinien, Verfahren und Aktivitäten, die Teil der internen Steuerung und

Kontrolle sind. Sie dienen der Steuerung und Kontrolle von Risiken, sodass diese die vorgegebenen Risikotoleranzen nicht übersteigen.

Steuerungs- und Kontrollumfeld (Control Environment) – Die Einstellung und die Handlungen von Geschäftsleitung und Verwaltungsrat sowie anderer Verantwortungsträger im Hinblick auf die Bedeutung der Steuerung und Kontrolle im Unternehmen. Das Kontrollumfeld bestimmt den Rahmen und die Struktur für das Erreichen der Hauptziele der internen Steuerung und Kontrolle. Zum Kontrollumfeld gehören folgende Elemente:

- Integrität und ethische Werte;
- Philosophie und Arbeitsstil der Geschäftsleitung;
- Organisatorische Struktur;
- Zuordnung von Befugnissen und Verantwortung;
- Personalpolitik und deren Umsetzung;
- Fachkompetenz des Personals.

TQM –Total Quality Management siehe Qualität.

Unternehmen (Organization) – Der Begriff «Unternehmen» umfasst im vorliegenden Teil alle in der Rechtsform der Kapitalgesellschaften und Personengesellschaften geführten Firmen sowie Körperschaften, Verwaltungsbehörden, Non-Profit-Organisationen und sonstige Organisationen.