CIP-Kurztitelaufnahme der deutschen Bibliothek

Internes Kontrollsystem

Herausgeber: Thomas Rautenstrauch und Stefan Hunziker

Projektleitung: Mag. (FH) Christian Hartig

WEKA Business Media AG, Schweiz

WEKA Business Media AG
Hermetschloostrasse 77, CH-8010 Zürich
Telefon 044 434 88 88, Telefax 044 434 89 99
www.weka.ch

Zürich • Kissing • Paris • Amsterdam • Wien

ISBN 978-3-297-02029-6

1. Auflage 2011

Druck: Kösel GmbH & Co. KG, Layout: Dimitri Gabriel, Satz: Michael Bislin

Inhaltsverzeichnis

1. Einleitung ... 5

2. Grundlagen der Internen Kontrolle ... 9
2.1 Definition und Abgrenzung der Internen Kontrolle ... 10
2.1.1 Zuständigkeiten und Verantwortungsbereiche ... 14
2.1.2 Abgrenzung und Synergien zum Qualitätsmanagement, Risikomanagement und Compliance Management ... 14
2.1.2.1 Synergien zum Risikomanagement ... 15
2.1.2.2 Betrieb von IKS und Risikomanagement ... 17
2.1.2.3 Konzept und Kontrollumfeld ... 17
2.1.2.4 Identifikation, Bewertung und Bewältigung ... 18
2.1.2.5 Synergien zum QMS ... 20
2.1.2.6 Schlussfolgerungen ... 21
2.2 Corporate Governance als Rahmenbedingung interner Kontrolle ... 23
2.2.1 Entwicklung und Verständnis von Corporate Governance ... 23
2.2.2 Änderungen im Revisionsrecht als Katalysator Interner Kontrolle ... 25
2.2.3 Gesetzliche Regulierung der Internen Kontrolle in der Schweiz ... 26
2.3 COSO als Rahmenkonzept der Internen Kontrolle ... 30
2.3.1 Das COSO-Rahmenwerk für interne Kontrollsysteme ... 30
2.3.2 Der COSO-Würfel ... 31
2.3.3 Kontrollumfeld ... 32
2.3.4 Risikobeurteilung ... 34
2.3.5 Kontrollmassnahmen ... 35
2.3.6 Information und Kommunikation ... 36
2.3.7 Überwachung ... 36

3. Umsetzung und Prüfung des IKS ... 37
3.1 Elemente, Gestaltung und Erfolgsfaktoren Interner Kontrollen ... 39
3.1.1 Konzeptpapier als erster Schritt ... 39
3.1.1.1 Ausgangslage ... 39
3.1.1.2 IKS-Definition ... 41
3.1.1.3 Ziele ... 42
3.1.1.4 Organisation ... 43
3.1.1.5 Auswahlverfahren der Schlüsselprozesse ... 44
3.1.1.6 Verantwortung und Überwachung ... 44
3.1.2 Kontrollen auf Unternehmensebene ... 45
3.1.2.1 Unternehmenskultur als Bedingung für die Wirksamkeit von Kontrollen auf der Unternehmensebene ... 45
3.1.2.2 Verhaltenskodex (Code of Conduct) als Beispiel für eine indirekte Kontrolle auf der Unternehmensebene ... 49
3.1.2.3 Budgetkontrolle als Beispiel für eine direkte Kontrolle auf der Unternehmensebene ... 53
3.1.3 Prozesskontrollen ... 54
3.1.3.1 Risiken in der finanziellen Berichterstattung ... 56
3.1.3.2 Ziele der finanziellen Berichterstattung ... 57
3.1.3.3 Festlegung des Wirkungsbereichs des Kontrollsystems ... 57
3.1.3.4 Identifikation von Schlüsselrisiken und Risikobeurteilung ... 58

3.1.3.5 Risiko-Kontroll-Matrix ... 59
3.1.3.6 Dokumentation von Schlüsselkontrollen ... 60
3.1.3.7 Zielsetzung einer Dokumentation ... 60
3.1.3.8 Attribute einer Schlüsselkontrolle ... 62
3.1.4 IT-gestützte Kontrollen ... 63
3.1.4.1 IT-Kontrollen auf Unternehmensebene ... 64
3.1.4.2 Generelle IT-Kontrollen ... 64
3.1.4.3 Applikationskontrollen ... 66
3.1.4.4 Überlegungen beim Outsourcing von IT-Prozessen oder IT-Dienstleistungen ... 67
3.1.4.5 Rahmenwerke, die bei der Einführung und Konzeption der IT-Kontrollen helfen ... 67
3.1.4.6 Gestaltung eines Berechtigungskonzepts ... 68
3.1.5 Verhinderung deliktischer Handlungen ... 69
3.1.5.1 Eigenschaften von Fraud-Risiken ... 69
3.1.5.2 Schlüsselfaktoren für Fraud – Das Fraud-Triangle ... 70
3.1.5.3 Anti-Fraud-Aktivitäten ... 71
3.1.5.4 Schlussbemerkung zur Fraud-Thematik ... 72
3.2 Prüfung der Existenz eines Internen Kontrollsystems ... 72

4. Fallstudien zur Internen Kontrolle ... 77
4.1 Fallstudie Alpha AG ... 78
4.1.1 Ausgangslage ... 78
4.1.2 Das Kontrollumfeld als Basis des IKS ... 80
4.1.3 Erkenntnisse aus Interviews und Dokumentenanalyse ... 81
4.1.4 Kontrollen auf Prozessebene ... 85
4.1.5 IT-Aspekte des internen Kontrollsystems ... 89
4.1.6 Lösungsansatz «Kontrollumfeld» ... 91
4.1.7 Lösungsansatz «IKS auf Prozessebene» ... 96
4.1.8 Lösungsansatz «IT-Aspekte des IKS» ... 100
4.2 Fallstudie Metallix AG ... 101
4.2.1 Das IKS auf Konzernebene der Metallix AG ... 102
4.2.2 Das Auswahlverfahren der relevanten Tochtergesellschaften ... 103
4.2.3 Das Auswahlverfahren auf Ebene der Jahresrechnung einer Tochtergesellschaft ... 104
4.2.4 Die Bestimmung der Schlüsselprozesse ... 107
4.2.5 Risiken und Kontrollen des IKS-Prozesses «Verkauf gegen Rechnung» ... 107
4.2.6 Lösungsansatz «IKS auf Konzernebene» ... 109
4.2.7 Lösungsansatz «Auswahlverfahren der Tochtergesellschaften» ... 109
4.2.8 Lösungsansatz «Auswahlverfahren auf Ebene der Jahresrechnung» ... 110
4.2.9 Lösungsansatz «Bestimmung der relevanten IKS-Prozesse» ... 112
4.2.10 Lösungsansatz «IKS-Prozess Verkauf gegen Rechnung» ... 113

5. IKS aus unterschiedlichen Perspektiven ... 115
5.1 IKS aus internationaler Perspektive ... 116
5.1.1 Überblick und Anwendungsbereiche des Sarbanes-Oxley Act (SOX) ... 117
5.1.2 Interne Kontrolle gemäss SOX 404 ... 119
5.2 IKS in KMU ... 121
5.2.1 IKS als nutzenstiftendes Führungsinstrument in KMU ... 123
5.2.1.1 IKS soll nicht als Pflichtübung verstanden werden ... 123
5.2.1.2 Kompensierende Kontrollen für die mangelnde Funktionentrennung ... 124

5.2.1.3 Ein ausgeprägtes Kontrollumfeld als Chance für KMU ... 125
5.2.1.4 Einsatz von Standard-Software ... 126
5.2.2 Fazit ... 127
5.3 Interne Kontrolle in der öffentlichen Verwaltung ... 127
5.3.1 IKS auf Bundesebene ... 128
5.3.2 IKS auf Kantonsebene ... 130
5.3.3 IKS auf Gemeindeebene ... 130
5.3.4 IKS für staatlich finanzierte Nonprofit-Organisationen ... 131
5.3.5 Fazit ... 133
5.4 Generelle Aspekte zum IKS in Stiftungen ... 134
5.4.1 Kontrolldefizite in Stiftungen ... 134
5.4.2 Typische Interne Kontrolldefizite in Stiftungen ... 135
5.5 IKS in Pensionskassen ... 136
5.5.1 Gesetzliche Anforderungen ... 136
5.5.2 IKS-Betrieb in Vorsorgeeinrichtungen ... 137

6. Schlussbetrachtung und Ausblick ... 141

Literaturverzeichnis ... 145

Abbildungsverzeichnis ... 147

Anhang: Schweizer Prüfungsstandard (PS 890) ... 149

Autoreninformationen ... 173

Stichwortverzeichnis ... 175

1. Einleitung

1. Einleitung

Die Interne Kontrolle gilt allgemein als ein Führungsinstrument, welches dabei behilflich sein kann, die Ziele einer Unternehmung besser und sicherer zu erreichen. Vor allem durch die spektakulären Bilanzskandale grosser börsennotierter Konzerne in den USA hat das Thema der Internen Kontrolle international einen hohen Bedeutungszuwachs erhalten, der anschliessend mit dem US-amerikanischen Sarbanes-Oxley Act sowie zahlreichen weiteren Regulierungen in den Folgejahren auch die Schweizer Unternehmen erreichte. Längst ist unbestritten, dass aus Sicht eines funktionierenden Kapitalmarktes effiziente Corporate-Governance-Strukturen sowie eine wirksame Interne Kontrolle durch neue gesetzliche Richtlinien in vielen Ländern Europas gefordert sind.

In der Schweiz gilt mit der Revision des Obligationenrechts für alle Jahresabschlüsse seit dem 1.1.2008, dass die externe Revision die Existenz eines Internen Kontrollsystems (IKS) überprüfen muss, sofern es sich um ein Unternehmen handelt, das der ordentlichen Revision unterliegt. Seither liegen zahlreiche Veröffentlichungen zum Thema IKS vor, die sich aus unterschiedlicher Perspektive mit der Umsetzung eines IKS im Unternehmen befasst haben und den Unternehmen Handlungsempfehlungen abgeben.

Bei der Umsetzung der Internen Kontrolle innerhalb von Schweizer Unternehmen und Konzernen bestehen allerdings noch immer Grauzonen, die ihre Ursache darin haben, dass der Gesetzgeber keine Aussagen zur inhaltlichen Ausgestaltung Interner Kontrollsysteme gemacht hat, sondern dieses der Revisionsbranche überlassen hat. Dies hat dazu geführt, dass für die meisten Unternehmen der Schweizer Prüfungsstandard 890 zur wesentlichen Informationsquelle hinsichtlich der geforderten Existenz-Prüfung von Internen Kontrollsystemen geworden ist. Unklare Anforderungen haben denn auch manche Unternehmen verunsichert, ein IKS zu konzipieren, das den Erwartungen des Gesetzgebers entspricht.

Eine Studie an der Hochschule Luzern im 2009 hat deutlich gemacht, dass zahlreiche Unternehmen, insbesondere die Klein- und Mittelunternehmen, die Gesetzespflicht zur Einführung und zum Betrieb eines IKS zu Beginn als aufwendige, kostenintensive und wenig sinnvolle Last eingeschätzt haben, was nach der Einführung wieder deutlich korrigiert wurde. Diese Denkhaltung ist im Zusammenhang mit neuen Gesetzespflichten keineswegs neu, allerdings ist gerade mit dem Internen Kontrollsystem ein wirksames Instrument vorhanden, mit dem im Idealfall nicht nur die Risiken im Bereich der Buchführung und finanziellen Berichterstattung, sondern auch in den operativen Geschäftsprozessen sowie im Bereich der Rechtskonformität beherrscht werden können.

Damit ist das IKS dann auch keine lästige Übung, die Unternehmen im Zusammenhang mit der Prüfung des Jahresabschlusses leisten müssen, sondern trägt zur Sicherung der Unternehmensexistenz bei. Mithin gilt ein effektives Interne Kontrollsystem (IKS) nicht nur als Bedingung, sondern zugleich als Erfolgsfaktor für eine nachhaltige Unternehmensführung.

Das vorliegende Buch will seinen Lesern einen umfasssenden und zugleich kompakten Überblick über die wesentlichen Bereiche und Erfolgsfaktoren eines Internen Kontrollsystems geben. Hierzu werden zusätzlich den konzeptionellen Grundlagen mehrere praxisorientierte Fallgestaltungen sowie unterschiedliche Branchenanforderungen dargestellt. Es will daher vor allem eine Lücke schliessen zwischen handlungs- und praxisorientierten Ratgebern zu Internen Kontrolle und rein theoretisch bzw. wissenschaftlich orientierten Arbeiten.

Im ersten Teil des Buches werden zunächst die Grundlagen der Internen Kontrolle dargestellt, um die grundlegenden Begriffe sowie die Abgrenzung der Internen Kontrolle zu nahestehenden Konzepten im Unternehmen, wie z. B. das Qualitätsmanagement oder das Risikomanagement, zu verstehen. Ebenso wird die Stellung der Internen Kontrolle im Zusammenhang mit der Corporate Governance deutlich gemacht und das international am stärksten verbreitete und beachtete Rahmenkonzept «COSO Internal Control» vorgestellt.

Der zweite Teil des Buches befasst sich hieran anschliessend mit der Umsetzung und Prüfung des IKS. Hierbei wird vor allem auf die relevanten Kontrollebenen Bezug genommen: Unternehmensebene, Prozess- und allgemeine IT-Ebene. Ein weiteres Anliegen ist die für Schweizer Unternehmen relevante Revisionspraxis gemäss dem Schweizer Prüfungsstandard 890 vorzustellen, welche im Zusammenhang mit dem revidierten Revisionsrecht zu sehen ist.

Im dritten Teil des Buches werden Fallstudien zur Internen Kontrolle genutzt, um die Leser ergänzend zur konzeptionellen Darstellung auch anwendungs- und praxisorientiert im Hinblick auf die Umsetzung eines IKS zu orientieren.

Im vierten und letzten Teil des Buches wird das Thema IKS aus unterschiedlichen Perspektiven behandelt, womit in erster Linie die divergierenden Branchenerfordernisse deutlich gemacht werden sollen.

2. Grundlagend er Internen Kontrolle

2.1 Definition und Abgrenzung der Internen Kontrolle 10
2.1.1 Zuständigkeiten und Verantwortungsbereiche 14
2.1.2 Abgrenzung und Synergien zum Qualitätsmanagement, Risikomanagement und Compliance Management 14
2.1.2.1 Synergien zum Risikomanagement 15
2.1.2.2 Betrieb von IKS und Risikomanagement 17
2.1.2.3 Konzept und Kontrollumfeld 17
2.1.2.4 Identifikation, Bewertung und Bewältigung 18
2.1.2.5 Synergien zum QMS 20
2.1.2.6 Schlussfolgerungen 21

2.2 Corporate Governance als Rahmenbedingung Interner Kontrolle 23
2.2.1 Entwicklung und Verständnis von Corporate Governance 23
2.2.2 Änderungen im Revisionsrecht als Katalysator Interner Kontrolle 25
2.2.3 Gesetzliche Regulierung der Internen Kontrolle in der Schweiz 26

2.3 COSO als Rahmenkonzept der Internen Kontrolle 30
2.3.1 Das COSO-Rahmenwerk für Interne Kontrollsysteme 30
2.3.2 Der COSO-Würfel 31
2.3.3 Kontrollumfeld 32
2.3.4 Risikobeurteilung 34
2.3.5 Kontrollmassnahmen 35
2.3.6 Information und Kommunikation 36
2.3.7 Überwachung 36

2. Grundlagen der Internen Kontrolle

2.1 Definition und Abgrenzung der Internen Kontrolle

Ein Internes Kontrollsystem (IKS) gilt nach dem aktuellen Verständnis einer funktionierenden Corporate Governance in der Schweiz als Pflichtelement jeder Unternehmensführung, welches in der kollektiven Verantwortung von Aufsichtsorgan und Geschäftsleitung liegt. Durch die im Obligationenrecht neu eingefügten Artikel 728a OR sowie 728b OR wurde zudem die Verantwortung für die Existenzprüfung und Berichterstattung zum IKS der externen Revision übertragen. Demnach müssen sich seit dem 1. Januar 2008 vor allem Organisationen, die einer ordentlichen Revision unterliegen, mit der Frage auseinandersetzen, wie ein IKS ausgestaltet sein soll damit es zumindest die Anforderungen der externen Revision erfüllt. Über die Voraussetzungen für eine Existenzbestätigung durch den Abschlussprüfer besteht weitgehend Einigkeit. Es gilt, dass das vom Aufsichtsorgan definierte IKS nicht nur schriftlich dokumentiert ist, sondern auch im Tagesgeschäft der Organisation seine Anwendung findet und den Mitarbeitenden bekannt ist. Zudem muss das IKS den jeweiligen Geschäftsrisiken und dem Umfang der Geschäftstätigkeit angepasst und ein Kontrollbewusstsein im Unternehmen vorhanden sein.

Trotz intensiver Beschäftigung und Auseinandersetzung mit dem Thema IKS in Forschung und Praxis besteht keine durchgängige Einigkeit darüber, was unter einem IKS zu verstehen ist, respektive welche Ziele mit einem IKS verfolgt werden sollen. Ein relativ breit akzeptiertes IKS-Verständnis rührt aus dem 1992 in den USA publizierten COSO-Rahmenwerk. Das vom Committee of Sponsoring Organizations of the Treadway Commission (COSO) geschaffene Rahmenwerk dient Unternehmen als Unterstützung bei der Bewertung und Verbesserung der Internen Kontrollen. Zusammenfassend zielt die Interne Kontrolle gemäss COSO darauf ab, eine angemessene Sicherheit bezogen auf folgende Aspekte zu erreichen:

- Effizienz und Effektivität der Geschäftstätigkeiten;
- Verlässlichkeit der finanziellen Berichterstattung;
- Einhaltung der Gesetze und Verordnungen (Compliance);
- ein Umfeld zu schaffen, welches betrügerisches Verhalten verhindern oder zumindest vermindern kann.

Interpretiert man diese IKS-Definition, wird offensichtlich, wie umfassend ein Kontrollsystem gemäss COSO ausgestaltet sein muss. Am Beispiel des ersten Aspektes – Effizienz und Effektivität der Geschäftstätigkeit – kann das verdeutlicht werden. Hier rückt das gesamte Geschäftsmodell in den Fokus; das heisst alle Kern- und Supportprozesse müssten hinsichtlich Risiken, Optimierungspotenzial sowie Qualitätsaspekten untersucht und mit entsprechenden Kontrollen versehen werden.

Eine derart weitreichende Neuregelung war offensichtlich nicht in der Absicht des Schweizer Gesetzgebers, so dass alt Bundesrat Blocher in der Wintersession 2005 den Geltungsbereich des IKS auf die Sicherstellung einer verlässlichen und wahrheitsgetreuen finanziellen Berichterstattung eingeschränkt hat.[1] In diesem Zusammenhang regelt der Schweizer Prüfungsstandard (PS) 890, der vom Vorstand der Treuhand-Kammer am 17. Dezember 2007 verabschiedet wurde, welche Massstäbe für die Prüfung der von Organisationen dokumentierten Internen Kontrollen anzulegen sind. Aus dieser Einschränkung bezüglich des Wirkungsbereichs des IKS ergibt sich ein anderer Fokus der IKS-Definition:

«Der Begriff ‹Internes Kontrollsystem› wird […] nicht in der üblichen Form verwendet, sondern inhaltlich eingegrenzt. Das IKS […] umfasst nur jene Vorgänge und Massnahmen in einer Unternehmung, welche eine ordnungsmässige Buchführung und finanzielle Berichterstattung sicherstellen.»[2]

Zusammenfassend lässt sich feststellen, dass in den neuen Bestimmungen im Schweizer Gesetz keine klare Aussage gemacht wird, wie ein IKS konkret auszugestalten ist. Die Legislative überlässt es den Organisationen, zu entscheiden, welches Kontrollsystem oder welche Kontrollmechanismen sie für ihre Situation als angemessen betrachten. Im Vordergrund für diese Entscheide stehen jedoch die Faktoren wie Grösse des Unternehmens, Komplexität der Geschäftstätigkeit und Art der Risiken. Das IKS soll durch Massnahmen und Methoden in die betrieblichen Arbeitsabläufe integriert werden. Das heisst, dass die Kontrollen arbeitsbegleitend erfolgen oder dem Arbeitsvollzug unmittelbar vor- oder nachgelagert sind. Dazu gehören nebst den Kontrolltätigkeiten auch Aktivitäten zur Steuerung und Planung jeder Organisation. Die nachfolgende Abbildung zeigt, welche Massnahmen einer Organisation zur Verfügung stehen, um ein IKS umzusetzen.

1 In der Wintersession des Ständerates am 1. Dezember 2005 hat Herr Bundesrat Christoph Blocher mit folgendem Statement für Klarheit gesorgt: «Wenn im neuen Revisionsrecht vom Internen Kontrollsystem gesprochen wird, dann nur in Bezug auf die Buchführung und Rechnungslegung. Andere Bereiche, wie die Geschäftsführung oder die Compliance, werden von der Vorlage – soweit keine Auswirkungen auf die Jahresrechnung bestehen – nicht berührt.

2 Vgl. Treuhand-Kammer (2007), S. 3.

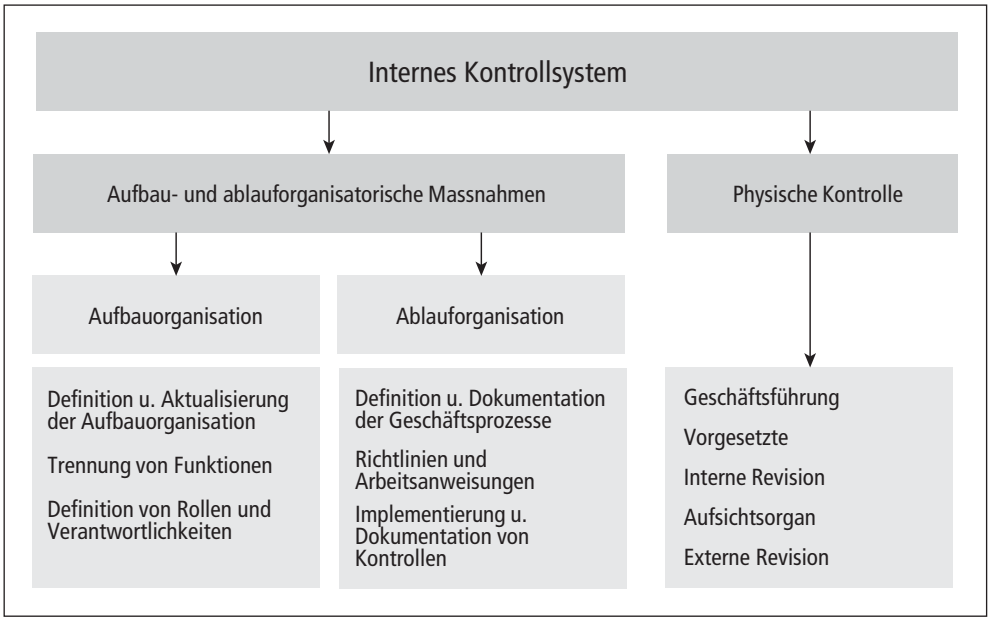

Abbildung 1: Elemente zur Unterstützung der Internen Kontrolle.[3]

Im Bereich der aufbauorganisatorischen Massnahmen ist – nebst der Definition und Aktualisierung der Aufbauorganisation (Organigramm) – die Funktionentrennung ein zentraler Grundsatz eines jeden Kontrollsystems. Beispielsweise sollen die Funktionen Genehmigung, Durchführung, Verbuchung und Kontrolle von Geschäftsvorfällen nicht von der gleichen Person durchgeführt werden. Durch eine angemessene Funktionentrennung kontrollieren sich die verantwortlichen Personen – etwa im Bereich des Rechnungswesens – stärker gegenseitig. Diese Massnahme erhöht die Verlässlichkeit der Rechnungslegung und unterstützt den Schutz des Geschäftsvermögens.[4]

Schliesslich gehört zu den aufbauorganisatorischen Massnahmen innerhalb einer Organisation, bestimmten Rollen oder Personen definierte Verantwortlichkeiten zuzuweisen. Welche Rollen definiert werden, hängt vom Ausschnitt der Organisation ab, den man betrachten möchte. So können Rollen etwa für das Gesamtunternehmen, für eine Abteilung oder ein Projekt festgelegt werden. Für die Definition der Verantwortlichkeiten sollen normierte Begriffe verwendet werden, die eine differenzierte Betrachtung erlauben, wer welche Verantwortung – beispielsweise bezüglich des IKS-Projekts – in welcher Ausprägung übernimmt. Die Aufgaben und Kompetenzen einzelner Stellen werden insbesondere in Stellenbeschreibungen und Funktionendiagrammen festgehalten. Spezifische Befugnisse und Vollmachten der Führungsebene sollen dokumentiert werden.

3 Vgl. von Malottke (2010).

4 Vgl. zum Folgenden Klinger und Klinger (2000), S. 13 ff.

Zu den ablauforganisatorischen Sicherungsmassnahmen gehört auch die Regelung und Beschreibung der Arbeitsabläufe und Arbeitsrichtlinien. Sich wiederholende Tätigkeiten sollen durch verständliche und detaillierte Arbeits- und Organisationsanweisungen geregelt werden. Für die wesentlichen Geschäftsfälle müssen Bewilligungsverfahren definiert werden; administrative Abläufe sollen geregelt werden, damit geschäftsschädigende Handlungen minimiert werden können. Empfehlenswert ist die Dokumentation der wesentlichen Abläufe beispielsweise mit Flussdiagrammen, damit die Transparenz erhöht wird und die Nachvollziehbarkeit von Geschäftstransaktionen ermöglicht wird. Zudem können die visualisierten Geschäftsprozesse die Basis der Risiko- und Kontrolldokumentationen im IKS sein.

Kernstück jedes Kontrollsystems sind systematisch eingebaute Kontrollen. Dies kann bei IT-gestützten Abläufen zum Beispiel durch Plausibilisierungsprüfungen, Vollständigkeitskontrollen, Summenabgleiche und Versionierung von Veränderungen an Daten erreicht werden. Bei vorwiegend manuellen (Teil-)Prozessen kann eine Kontrollautomatik durch das Vier-Augen-Prinzip, klassische Unterschriftenregelungen, Genehmigungsverfahren (z. B. Investitionshandbuch) wie auch durch angeordnete Arbeitswiederholungen erreicht werden. Aus Effizienzüberlegungen ist der präventive, IT-gestützte Kontrolltyp allen anderen Kontrollen vorzuziehen. Es kann also durchaus Sinn machen, ein bestehendes Kontrollsystem darauf hin zu prüfen, ob manuelle, detektive (dem Teilprozess nachgelagerte) Kontrollen nicht durch einen wirtschaftlicheren und sicheren Kontrolltyp ersetzt werden können.

Nebst aufbau- und ablauforganisatorischen Massnahmen wird das IKS wesentlich durch physische Kontrollen unterstützt. Zentral ist das Vorleben einer angemessenen Einstellung zur Internen Kontrolle (Kontrollkultur) durch die Geschäftsleitung. Nur ein intern regelmässiges, kommuniziertes Bekenntnis zum IKS durch die Führungsebene ermöglicht den dauerhaften, erfolgreichen Betrieb eines IKS. Die Mitarbeitenden müssen über die Wichtigkeit der Internen Kontrolle laufend informiert werden, sie müssen das IKS akzeptieren und es als Unterstützung (und eben nicht als notwendiges Übel) ihrer Aufgaben verstehen. Vorgesetzte müssen zudem Arbeitsabläufe laufend beaufsichtigen. Dazu müssen sie die Tätigkeiten der Mitarbeitenden und mögliche Fehlerquellen kennen. Gerade in kleineren Organisationen kennt die Geschäftsleitung die Arbeitsabläufe und deren inhärenten Risiken in der Regel sehr gut und übernimmt so eine zentrale Überwachungs- und Kontrollfunktion im IKS. Neben der Überwachung der Mitarbeitenden müssen auch die angewandten Organisationsmittel auf deren Manipulationssicherheit geprüft werden. Das Aufsichtsorgan kann zusätzlich die Interne Revision, die Geschäftsleitung und / oder Fachpersonen der Wirtschaftsprüfung mit der Überwachung beauftragen. Wichtig ist aber, dass die Geschäftsleitung dadurch nicht von ihrer Kontrollverpflichtung befreit werden kann.

2.1.1 Zuständigkeiten und Verantwortungsbereiche

Beim IKS kann zwischen den Zuständigkeiten des Aufsichtsorgans, der Geschäftsleitung und der Revisionsstelle unterschieden werden. Das Aufsichtsorgan trägt die Gesamtverantwortung für das IKS. Es ist dafür zuständig, dass ein IKS im Unternehmen eingeführt und aufrechterhalten wird. Dazu gehört, dass das Aufsichtsorgan strategische Entscheidungen genehmigt und überprüft sowie die Einführung von Massnahmen im Zusammenhang mit dem IKS sicherstellt. Zusätzlich ist es dafür verantwortlich, dass die Wirksamkeit des IKS von der Geschäftsleitung kontrolliert wird. Das Aufsichtsorgan muss somit regelmässig die Effektivität der Massnahmen aus dem IKS mit der Geschäftsleitung erörtern und die Bewertung des IKS beurteilen. Wurden Mängel im IKS festgestellt, so ist das Aufsichtsorgan dafür verantwortlich, geeignete Korrekturmassnahmen anzuordnen und zu überwachen. Als Unterstützung bei den Aufgaben zum IKS kann das Aufsichtsorgan einen Prüfungsausschuss und/oder eine externe Kontrolle einsetzen. Allerdings kann es dadurch die Oberverantwortung über das IKS nicht delegieren.

Die Geschäftsleitung ist dafür verantwortlich, das IKS nach den strategischen Vorgaben und Geschäftsgrundsätzen des Aufsichtsorgans zu gestalten und umzusetzen. Dazu sollen zweckmässige Prozesse zur Identifikation, Messung, Kontrolle und Überwachung der eingegangenen Risiken festgelegt werden. Zusätzlich identifiziert und überwacht die Geschäftsleitung Schlüsselkontrollen im Unternehmen. Sie ist verantwortlich für die Aufrechterhaltung und Dokumentation der Verantwortlichkeiten, Kompetenzen und Informationsflüsse in der Organisationsstruktur.

Weiter soll die Geschäftsführung das IKS dokumentieren und überprüfen. Im Zusammenhang mit diesen Zuständigkeiten stellt sie ausserdem sicher, dass genügend personelle Ressourcen mit der benötigten Ausbildung und Erfahrung im Unternehmen vorhanden sind. Eine weitere Aufgabe der Geschäftsleitung ist die periodische Berichterstattung über die Wirksamkeit des IKS an das Aufsichtsorgan.

2.1.2 Abgrenzung und Synergien zum Qualitätsmanagement, Risikomanagement und Compliance Management

Die folgende Abbildung steht schematisch für die verschiedenen Managementsysteme, die regelmässig in mittleren und grösseren Unternehmen implementiert sind. Orientiert man sich an den grundlegenden Kontrollzielen, mit denen ein Unternehmen konfrontiert wird, so können Ziele in den Bereichen Strategie, Geschäftstätigkeit (Operational Objectives), wahrheitsgetreue finanzielle Berichterstattung (Financial Reporting Objectives) sowie Regel- und Normenkonformität (Compliance) unterschieden werden. Dieselben Kontrollziele finden sich auch im Rahmenwerk COSO ERM[5], welches 2004 veröffentlich wurde. In diesem Beitrag wird davon ausgegangen, dass ein Unternehmen sich nicht an

5 Im Jahr 2004 hat das Committee of Sponsoring Organizations of the Treadway Commission (COSO) eine Ergänzung zu seinem ursprünglichen Modell von 1992, das COSO ERM – Enterprise Risk Management Framework publiziert.

einem IKS-Minimalstandard orientiert, sondern aus Überlegungen von Effizienz- und Synergiepotentialen einen ganzheitlichen Projektansatz wählt, der ebenfalls Bereiche aus der operativen Geschäftstätigkeit sowie Compliance-Risiken miteinbezieht. Wenn von einem ganzheitlichen Ansatz gesprochen wird, kann das COSO ERM als Referenz herangezogen werden. Die folgenden Erläuterungen beziehen sich auf die Abbildung 2, wo schematisch mögliche Überlappungen einzelner, nicht integrierter Aktivitäten aufgezeigt sind.

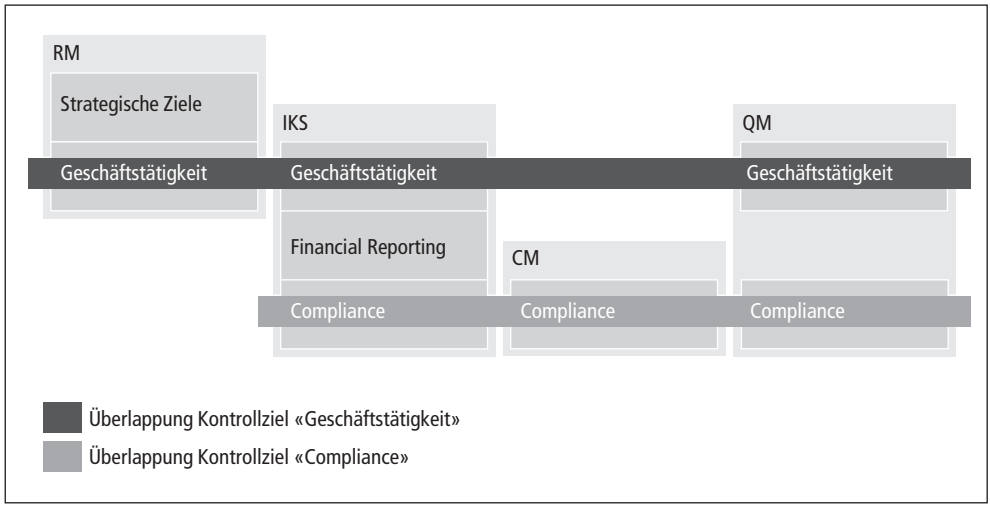

Abbildung 2: Managementsysteme und deren Abdeckung verschiedener Kontrollziele

2.1.2.1 Synergien zum Risikomanagement

Einigkeit besteht heute darin, dass Risikomanagement und Internes Kontrollsystem mindestens Schnittstellen und wesentliche Gemeinsamkeiten und Wechselwirkungen zueinander aufweisen; der Versuch jedoch, eine genaue konzeptionelle Einordnung und Abgrenzung der beiden Konzepte vorzunehmen, fehlt bislang weitgehend. Wertet man die bestehende Literatur aus, findet man unterschiedliche Ansätze, Risikomanagement und Internes Kontrollsystem in Relation zu stellen. Aus Sicht der Autoren bleibt nach wie vor hoher Klärungsbedarf, inwiefern sich diese beiden Konzepte decken oder eben in ihrer Art und Ausprägung unterscheiden. Ohne Zweifel beschäftigen sich sowohl IKS als auch das Risikomanagement mit Risiken, Massnahmen und Kontrollen. Dennoch wäre es falsch, von gleichen oder ähnlichen Führungs- und Managementsystemen zu sprechen.

Angefangen beim Vergleich eines Risikomanagements mit einem IKS lassen sich wesentliche Schnittstellen im Bereich der operativen Gefahren (Geschäftstätigkeit) finden. Ein operationelles Risikomanagement (ORM) adressiert teilweise dieselben Risiken wie ein IKS, falls das Risk Assessment unabhängig durchgeführt wird. So fokussiert dass IKS im Wesentlichen auf Risiken im Hinblick auf die finanzielle Berichterstattung oder allgemeine finanzielle Risiken, die aus der Geschäftstätigkeit hervorgehen. Im Rahmen der Risiko-

identifikation wird versucht, die Schnittstellen von den operativen Geschäftsprozessen zum finanziellen Rechnungswesen herzuleiten, um somit IKS-relevante Risiken zu erfassen. Beim Risikomanagement werden somit mindestens teilweise dieselben Risiken identifiziert, bewertet, überwacht und rapportiert. Es ist offensichtlich, dass durch unabhängige Assessments so eine mehrfache und, daraus folgend, ineffiziente Risikoabdeckung durch die beiden Systeme generiert wird. Ein Beispiel lässt sich aus dem Kreditorenmanagement aufführen. Grundsätzlich stellt der Verkauf an neue Kunden ein Risiko dar. Das Risiko besteht in der Gefahr, dass neue Kunden nicht genügend solvent sind – eine Bonitätsprüfung im Sinne einer Massnahme zur Risikoreduzierung ist also nötig und wird vom IKS und vom operationellen RM eventuell doppelt abgedeckt. Ein anderes Beispiel resultiert aus der risikoorientierten Analyse des Einkaufsprozesses. Im Rahmen des Scopings für das IKS wird dieser Prozess mit Sicherheit als relevant eingeschätzt, da beispielsweise die falsche Erfassung von Einkaufspreisen im System direkt auf die finanzielle Berichterstattung durchschlägt. Mit hoher Wahrscheinlichkeit wurde dieses Risiko schon früher im Rahmen eines Risk Assessments im operationellen Risikomanagement erkannt, bewertet, dokumentiert und entsprechende Massnahmen implementiert. Auch hier besteht die Gefahr einer doppelten Abdeckung durch das ORM und IKS.

Möglicherweise werden einige Risiken weder vom RM noch vom IKS adressiert – es entstehen Abdeckungslücken. Einerseits muss man bedenken, dass sich das Risikomanagement primär den wesentlichen Aufgaben der Identifizierung, Bewertung und Ableitung von Massnahmen zur Reduzierung von **bedeutenden** (Netto-Risiken mit einer gewissen Materialität) strategischen wie auch operationellen Risiken annimmt. Im Allgemeinen werden somit vom Risikomanagement nur solche Risiken adressiert, welche auf sehr hohem Niveau mit **unmittelbarem Bezug zu den Unternehmenszielen** stehen. Andererseits bezieht sich das IKS meistens auf Prozessrisiken mit direktem finanziellem Bezug; d. h. auf Finanzprozesse oder auf Prozesse der Jahresabschlusserstellung. Somit werden tendenziell Risiken weder vom IKS noch vom RM adressiert, die eine gewisse Materialität unterschreiten oder nicht in direktem Bezug zu Finanzprozessen stehen.

Da sich im schnell ändernden Marktumfeld Risiken verändern oder neue Risiken dazukommen und sich dadurch die Rahmenbedingungen zur Erreichung der Unternehmensziele immer neu gestalten, muss die Risikobeurteilung im klassischen Risikomanagement periodisch oder zumindest einmal jährlich neu erfolgen. Im operationellen, vorwiegend prozessorientierten Bereich reicht meist eine ereignisgesteuerte Risikobeurteilung, d. h. einmal zu Beginn im Rahmen der erstmaligen Implementierung eines IKS und anschliessend bei sich verändernden Prozessen oder nach einem Business Process Reengineering. Da operationelle Risiken in der Regel durch Kontrollaktivitäten gemanagt werden können, besteht in diesem Bereich eine erhebliche Schnittstelle zum IKS. Die Definition und Dokumentation von Kontrollaktivitäten in Prozessen oder auch auf Unternehmensebene ist ganz klar dem IKS zuzuordnen und vom Risikomanagement abzugrenzen. Auch auf strategischer Ebene bestehen aber durchaus Schnittstellen zum klassischen Risikomanagement. Obwohl die Massnahmen zur Reduzierung dieser Risi-

ken auf ein tragbares Risiko vom Risikomanagement definiert und überwacht werden, trägt hier das Interne Kontrollsystem dazu bei, mittels Kontrollaktivitäten sicher zu stellen, ob diese Massnahmen auch tatsächlich umgesetzt werden.

2.1.2.2 Betrieb von IKS und Risikomanagement

Orientiert man sich bei der Gegenüberstellung von IKS und Risikomanagement dem klassischen Regelkreislauf der Identifikation, Bewertung, Bewältigung und Überwachung von Risiken, können wie in der folgenden Abbildung Merkmale beider Konzepte herausgearbeitet werden. Bei der Analyse der Abhängigkeiten wird auch versucht, Möglichkeiten und Grenzen von Aspekten der Integration eines IKS ins bestehende Managementsystem aufzuzeigen.

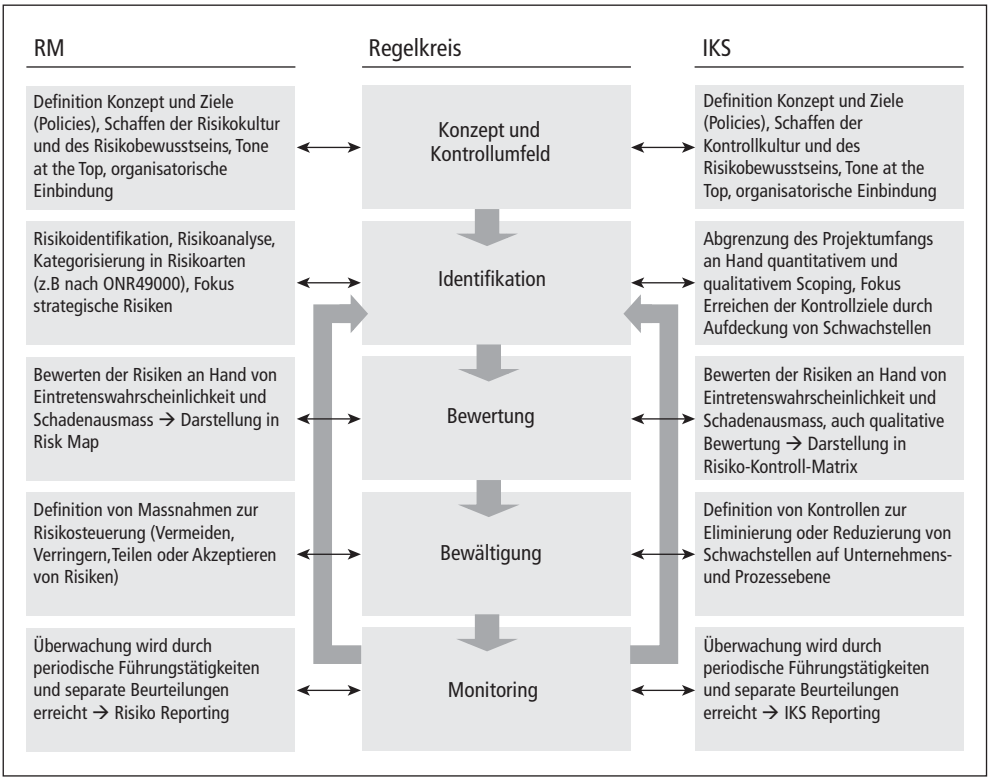

Abbildung 3: Regelkreis RM und IKS

2.1.2.3 Konzept und Kontrollumfeld

Selbstverständlich ist das Kontrollumfeld und die damit verbundenen Elemente einer gesunden Kontrollkultur und eines ausgeprägten Kontrollbewusstsein im Unternehmen eine zentrale Voraussetzung beider darauf aufbauender Managementsysteme. Im Rahmen des Kontrollumfelds werden die Unternehmensorganisation, das Weisungswesen, die Kompetenzverteilung und weitere Aspekte guter Corporate Governance definiert. Als

Kontrollumfeld, welches grundsätzlich als das interne Arbeitsklima und Arbeitsumfeld bezeichnet werden kann, wird als zentrales Element die Einstellung und das Vorleben des Managements im Hinblick auf Kontrollen und Sanktionen bezeichnet (Tone at the Top). Integrität und ethische Werte, Kompetenzen und Verantwortlichkeit, Personal- und Beförderungspolitik sowie Fachkompetenzen sind Bestandteile des internen Arbeitsumfeldes und tragen indirekt dazu bei, beispielsweise deliktische Handlungen (Fraud) zu minimieren. Um einem integrativen Ansatz gerecht zu werden, kann es Sinn machen, die vom Verwaltungsrat oder Audit Committee definierten Richtlinien (Policy) bezüglich IKS und RM in einem zentralen Dokument vereint festzuhalten.

Bei der konzeptionellen Gestaltung des RM muss bei einem integrativen Ansatz beispielsweise berücksichtig werden, dass die Rollen und Verantwortlichkeiten bezüglich RM und IKS eindeutig bestimmt werden und idealerweise ein neues, gesamtheitliches Rollen- und Verantwortlichkeitskonzept geschaffen wird. Dies setzt voraus, dass die Begriffe Enterprise Risk Management, operationelles Risikomanagement sowie IKS klar definiert und Synergien als auch wesentliche Schnittstellen aufgezeigt werden. In der Regel ist das Risikomanagement eine zentrale Instanz im Unternehmen, die entweder direkt bei der Geschäftsleitung angesiedelt ist oder einem Risikoverantwortlichen übertragen wird. Diesem obliegen beispielsweise die Konzeption, Dokumentation und Unterhalt des Risikomanagementsystems sowie die Informationsversorgung und Unterstützung der Risikoverantwortlichen in den Unternehmensbereichen und -prozessen oder auch die Risikoberichterstattung und Ad-hoc-Reporting. Im Rahmen des integrativen Ansatzes erfordert die Einbindung des IKS organisatorische Anpassungen wie etwa die Vereinheitlichung des IKS- und RM-Reports an den Verwaltungsrat oder das Audit Committee. Synergien entstehen jedoch dadurch, dass die bestehende Reportingstruktur angewendet werden kann. Beachtet werden muss allerdings, dass ergänzend die Definition des Reportings über die Existenz des IKS insbesondere bezüglich der finanziellen Berichterstattung gefordert wird.

2.1.2.4 Identifikation, Bewertung und Bewältigung

Aus Überlegungen bezüglich der Effizienz und Nutzung von Synergien zwischen beiden Konzepten soll ein integrativer Ansatz aufgezeigt werden; das heisst, IKS-Elemente sollen sukzessive in das Risikomanagement-System eingearbeitet werden. Als Ausgangspunkt und Basis zur Implementierung eines Risikomanagement-Systems als auch eines IKS kann die unternehmensweite Risikoidentifikation gesehen werden. Im Rahmen des klassischen Risikomanagement-Prozesses werden in einem ersten Schritt die Geschäftsrisiken hinsichtlich der finanziellen Berichterstattung, den Unternehmens- und Leistungszielen, der Wirksamkeit der Prozesse, den Gefahren deliktischer Handlungen sowie den Compliance-Anforderungen identifiziert und analysiert. Diese beiden grundlegenden Prozesse stellen die Basis beider Konzepte dar und sollten keinesfalls voneinander isoliert durchgeführt werden. Daher soll das im Unternehmen vorhandene Know-how bezüglich operationeller Risiken genutzt werden und mit den IKS-relevanten Risiken ab-

gestimmt werden, damit Redundanzen oder schlimmstenfalls Kontrolllücken vermieden werden können. Üblicherweise sind aber Kenntnisse über die Schnittstellen von Prozessaktivitäten zur finanziellen Berichterstattung in den Kernprozessen nur ungenügend vorhanden; d. h. Risiken in operativen Prozessen werden vom ORM möglicherweise nicht erkannt, hier wird aus Sicht eines IKS spezifisches Augenmerk verlangt.

Im Gegensatz zu einem ERM wird der Umfang eines IKS-Projektes (Scoping) anders definiert. Die Festlegung des Wirkungsbereichs des IKS orientiert sich auf Basis der finanziellen Berichterstattung, d. h. Positionen der Jahresrechnung werden nach quantitativen und qualitativen Kriterien ausgewählt. In einem weiteren Schritt erfolgt die Identifikation derjenigen Geschäftsprozesse, welche Einfluss auf die wesentlichen Positionen der Jahresrechnung haben. Dabei sollen auch IT-Prozesse, welche die Verarbeitung von Transaktionen unterstützen oder sonst Einfluss auf die Ziele der Berichterstattung ausüben, erfasst werden.

Als Ergebnis der Analyse der Materialität von Unternehmenseinheiten und Positionen der Jahresrechung sowie der Risk Assessments durch das ORM liegt nun ein Inventar mit allen relevanten Risiken vor, denen anschliessend eine Wahrscheinlichkeit des Eintretens wie auch das potenzielle Schadensausmass zugeordnet werden. Aus Überlegungen der Integration empfiehlt es sich hier, eine Kategorisierung der Risiken vorzunehmen, die den Ansprüchen aus dem RM und IKS gleichzeitig genügen. Folgende Abbildung zeigt einen Vorschlag, wie eine solche Kategorisierung aussehen kann.

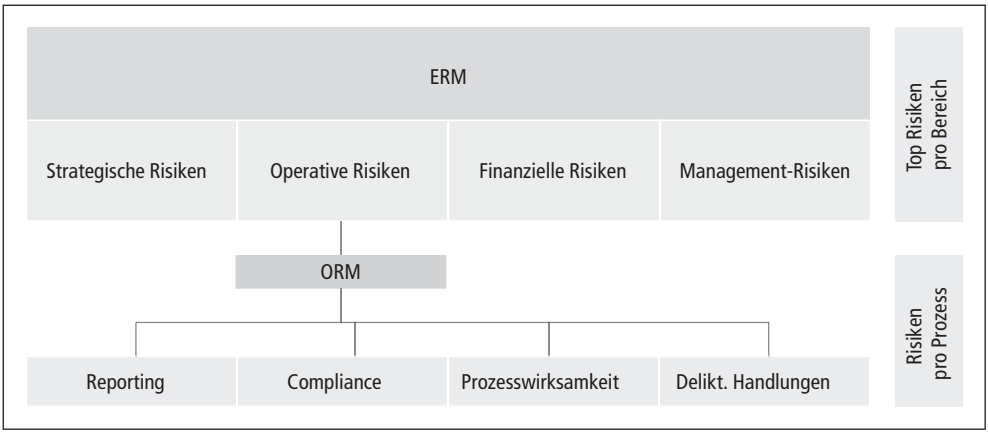

Abbildung 4: Risikokategorisierung

Eine zentrale Aufgabe des Risikomanagements sind die im Rahmen der definierten Risikostrategie bestimmten Risiken, die auf Grund ihrer hohen Komplexität nicht alleine durch Kontrollen zu bewältigen sind, sondern ausgewählter Massnahmen bedürfen. An dieser Stelle kann eine Abgrenzung zum IKS hergestellt werden – die allgemein bekannten Massnahmen der Risikobewältigung (Instrumente zur Risikosteuerung: Vermeiden,

Verringern, Teilen oder Akzeptieren von Risiken mit dem Ziel, ein Bündel von Massnahmen zum Anpassen der Risiken an den Risikoappetit der Organisation festzulegen) sind dem Risikomanagement-Prozess zuzuordnen. Da solche Massnahmen im Allgemeinen strategische oder finanzielle Risiken mit hoher Komplexität und Materialität adressieren, kann grundsätzlich gesagt werden, dass ein Internes Kontrollsystem sich primär nicht mit strategischen Risiken beschäftigt, sondern vorwiegend im operationellen Risikobereich anzusiedeln ist. Ein IKS fokussiert somit auf Risiken in Prozessen mit Auswirkung auf die finanzielle Berichterstattung, die durch geeignete – idealerweise automatisierte – Kontrollen behoben werden können. Möglicherweise kann aber ein unter IKS definiertes Risiko nach erneuter Beurteilung der Materialität nicht mehr alleine durch Kontrollen adäquat gemanagt werden und mutiert so zu einem Risiko, dass dem Risikomanagement gemeldet werden muss und geeigneter Massnahmen bedarf.

Alle Risiken, die ein im IKS-Projektumfang definiertes Kontrollziel (Reporting, Compliance; Prozesswirksamkeit) negativ beeinflussen können, müssen als IKS-relevant deklariert werden. Aus gesetzlicher Sicht müssen mindestens alle Risiken berücksichtigt werden, die eine wahrheitsgetreue, finanzielle Berichterstattung gefährden. Falls der IKS-Projektumfang auch die Einbeziehung von Compliance-Risiken vorsieht, ist ein Abgleich mit dem Compliance Management zwingendermassen nötig, um auch hier Doppelspurigkeiten oder Kontrolllücken zu vermeiden. Ob solche Risiken auch für das RM relevant sind, entscheidet die in der Risikopolitik definierte Toleranzgrenze der Materialität. So muss beispielsweise ein unter IKS definiertes Risiko dem RM gemeldet werden, falls das Netto-Risiko eine Million CHF übersteigt und nicht adäquat durch eine Kontrolle abgedeckt werden kann.

Aus Sicht des Existenznachweises eines IKS sind im Gegensatz zum RM zusätzliche Anforderungen an die Dokumentation zu erfüllen. Massnahmepläne und Kontrollinventare aus dem RM reichen dazu nicht. Hierbei ist die Risiko-Kontroll-Matrix ein wichtiges zusätzliches Instrument für die Dokumentation des IKS und somit ein Hilfsmittel gegenüber dem Abschlussprüfer, das IKS nachzuweisen. Die Risiko-Kontroll-Matrix wird als umfassendes Dokument im Sinne eines Risikoinventars bezüglich Kontrollen auf Unternehmensebene, Kontrollen auf der Prozessebene und generellen IT-Kontrollen erstellt.

2.1.2.5 Synergien zum QMS

Ein wesentlicher Bestandteil eines ausgereiften Qualitätsmanagement (z. B. ISO 9001) stellt der Kontinuierliche Verbesserungsprozess (KVP) dar. Der KVP bezieht sich nicht nur auf die Dienstleistungs- und Produktqualität, sondern auch auf die interne Prozessqualität. Das Ziel des KVP ist es, in fortwährender Teamarbeit stetig kleine Verbesserungsschritte zu erreichen, in dem nach der Analyse des definierten Problems Massnahmen abgeleitet, umgesetzt und überprüft werden. Ergebnisse eines KVP sind unter anderem die Entdeckung von Ressourcen und Synergien, optimierte Prozessabläufe und die Reduzierung von Ressourcenverschwendung und dadurch Einsparung von Kosten. Der KVP im Rahmen eines Qualitätsmanagements betrifft die gesamten Prozessabläufe

im Unternehmen, somit auch die Regelkreise des RM und IKS. Zudem stellt die Qualitätssicherung – ebenfalls Bestandteil des Qualitätsmanagements – sicher, ob die vom Qualitätsmanagement definierten Massnahmen effektiv und effizient sind.

Die im Laufe eines IKS-Projektes oder auch durch die interne oder externe Revision identifizierten Risiken, Schwachstellen und Kontrollabläufe in Prozessen müssen ebenfalls ständig aktualisiert und angepasst werden. Die bereits vorhandenen Prozesse im Rahmen der Qualitätssicherung können hierbei wertvolle Hinweise über vorhandene Schwachstellen liefern und sollten bei der IKS-Evaluation miteinbezogen werden. Die Synergien lassen sich vor allem im Bereich der operativen Effizienz (Kernprozesse) erreichen, da die Schnittstellen zum finanziellen Rechnungswesen vom Qualitätsmanagement weitgehend ausgeklammert werden. In der Sprache des COSO-Modells entspricht das IKS-Kontrollziel «operative Effizienz» in vielen Belangen dem Ziel des Qualitätsmanagements, da die Optimierung der Prozesse und Aktivitäten mit dem Ziel eine effektive und effiziente, aber trotzdem sichere und fehlerfreie Arbeitsweise zu ermöglichen Gegenstand beider Managementsysteme ist. Da das Interne Kontrollsystem wie auch die Qualitätssicherung die Massnahmen und Kontrollen zur Optimierung von Prozessen zur Aufgabe haben, ist eine Abstimmung beider Systeme sinnvoll.

Die Überprüfung und Anpassung von Prozessen erfolgt oft ereignisgesteuert, beispielsweise auf Grund von personellen Wechseln, erforderlichen Qualitätsoptimierungen oder Reorganisationsprojekten. Anpassungen in Prozessen ziehen eine notwendige Aktualisierung der bestehenden Internen Kontrollen nach sich, insbesondere auch im Schnittstellenbereich zwischen Support- und Kernprozessen. Dies erfordert ein ausgereiftes Change Management, welches in bestehenden Qualitätsmanagementsystemen vorhanden ist und genutzt werden sollte. Schliesslich kann das IKS auf bestehende Prozesse aus dem Qualitätsmanagement zurückgreifen und Kontrollen in den einzelnen Prozessschritten im Sinne eines integrativen Ansatzes definieren.

2.1.2.6 Schlussfolgerungen

Ein zentrales Element beim IKS ist sicherlich die sorgfältige Dokumentation der Kontrollaktivitäten. Im Rahmen der Existenzprüfung des IKS durch die externe Revisionsstelle sind Unternehmen gezwungen, Kontrollaktivitäten schriftlich nachzuweisen. Diese Kontrollaktivitäten beziehen sich in erster Linie auf operationelle Risiken, da diese im Allgemeinen auf Grund ihres eher niedrigen Komplexitätsgrades durch Kontrollen zu bewältigen sind. Auf strategischer Ebene stellt das IKS Kontrollaktivitäten bereit, um die im Risikomanagement definierten Massnahmen zur Steuerung der Risiken zu überprüfen. IKS, Risikomanagement, Compliance Management und Qualitätsmanagement sind zweifelsohne nicht als isolierte Systeme zu betrachten, sondern weisen starke gegenseitige Wechselbeziehungen zueinander auf. Ein Internes Kontrollsystem bezieht sich schwerpunktmässig auf Kontrollen hinsichtlich Schadensbegrenzung der im Projektumfang definierten Prozesse, wobei das Risikomanagement Instrumente zur Bewertung und Steuerung von Risiken bereitstellt.

Wechselbeziehungen zwischen allen Systemen und daraus resultierendem Abbau von Redundanzen sind aus Kosten/Nutzen-Überlegungen wünschenswert und werden durch die aufeinander abgestimmten Risiko-Assessments, Definitionen von Risiko- und Kontrollprozessen sowie Reportingprozessen erreicht. Abbildung 5 zeigt auf, dass sowohl der Regelkreislauf der verschiedenen Systeme wie auch die Zuordnung von Rollen und Verantwortlichkeiten aufeinander abgestimmt werden sollten.

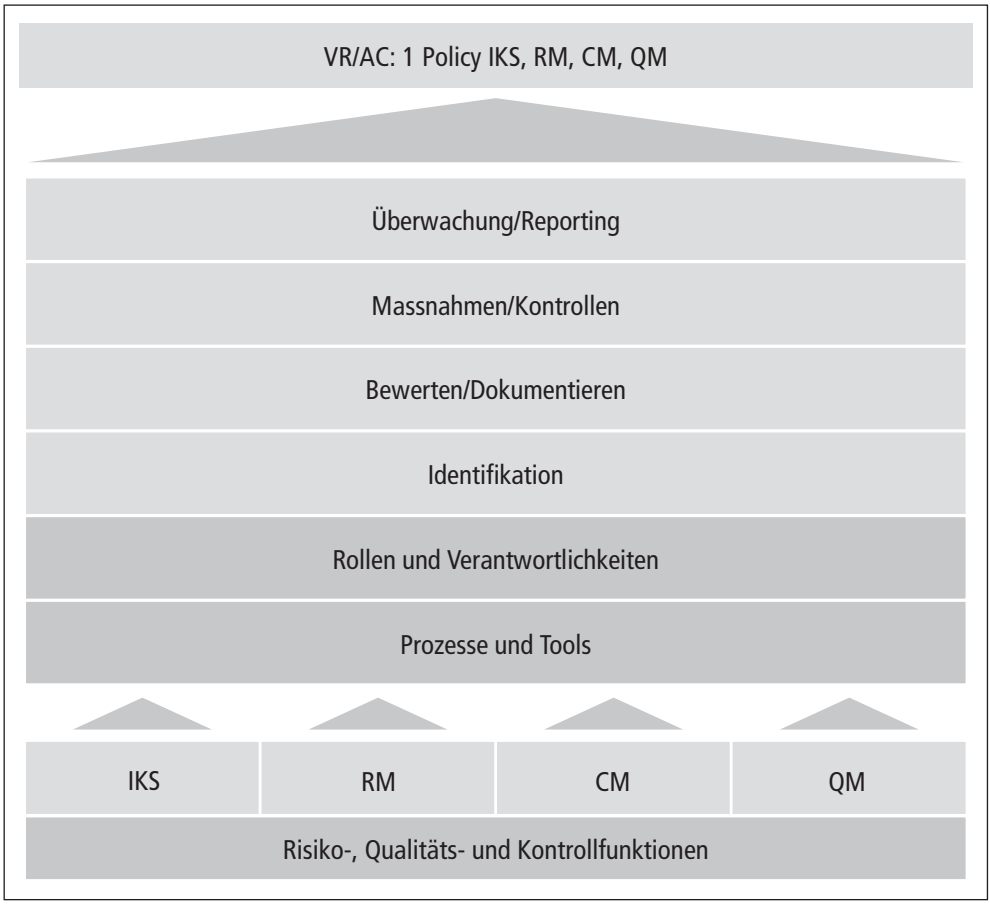

Abbildung 5: Integrierter Ansatz zur Nutzung von Synergien

Ziel ist es, organisatorische wie auch systematische Synergien zwischen den einzelnen Managementsystemen zu erreichen. Dies wird durch die Anwendung konsistenter Methoden, einer transparenten und integrierten Berichterstattung an den VR oder das Audit Committee, das Zusammenfassen der verschiedenen Policies in einem abgestimmten, zentralen Dokument sowie der Nutzung bestehender Prozessdokumentationen erreicht.