DIIR

Revision des Internen Kontrollsystems

Prüfungsleitfäden zu Funktion und Wirksamkeit

Herausgegeben vom DIIR – Deutsches Institut für Interne Revision e. V.
Erarbeitet von Sami Abbas, Sabine Bohlenz, Martin Guder, Clemens Jung, Stefan Kullmann, Claudia Lazarz, Matthias Meyer, Wulf-Matthias Nolte, Ilja Papas, Christoph Tennstedt und Oliver Wiesehahn

60

DIIR-Schriftenreihe • DIIR – Deutsches Institut für Interne Revision e. V.

ESV ERICH SCHMIDT VERLAG

ESV ERICH SCHMIDT VERLAG

DIIR-SCHRIFTENREIHE

Band 60

Revision des Internen Kontrollsystems

Prüfungsleitfäden zu Funktion und Wirksamkeit

Herausgegeben vom DIIR – Deutsches Institut für Interne Revision e. V.

Erarbeitet von Sami Abbas, Sabine Bohlenz, Martin Guder, Clemens Jung, Stefan Kullmann, Claudia Lazarz, Matthias Meyer, Wulf-Matthias Nolte, Ilja Papas, Christoph Tennstedt und Oliver Wiesehahn

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 16659 6

Gedrucktes Werk: ISBN 978 3 503 16658 9
eBook: ISBN 978 3 503 16659 6

Satz: multitext, Berlin

Vorwort

Das Interne Kontrollsystem eines Unternehmens soll mittels wirksamen Überwachungsinstrumenten/-mechanismen sicherstellen, dass die wesentlichen Geschäftsprozesse und -aktivitäten effektiv, effizient und möglichst fehlerfrei abgewickelt und dabei interne und externe Vorgaben eingehalten werden. Die Qualität des Internen Kontrollsystem ist in diesem Sinne ein wichtiger Erfolgsfaktor für die ordnungsmäßige Finanzberichterstattung.

Die Verantwortung für ein funktionierendes und wirksames Internes Kontrollsystem obliegt dabei der Unternehmensführung. Diese bedient sich u.a. der Internen Revision, um die Wirksamkeit des Internen Kontrollsystems sicherzustellen. Die Interne Revision prüft die Funktionsweise und Wirksamkeit des Internen Kontrollsystems und beurteilt somit die prozessbezogenen Steuerungs- und Kontrollaktivitäten des Managements bezüglich der o.a. Aspekte.

Ziel der in diesem Band enthaltenen Prüfungsleitfäden ist es, inhärente Risiken von Unternehmensprozessen aufzuzeigen, die geeigneten prozessbezogenen Steuerungs- und Kontrollaktivitäten zu identifizieren – ohne dass hierbei ein Anspruch auf Vollständigkeit erhoben werden kann – und die jeweils zu empfehlende Methodik zur Prüfung der Funktion und Wirksamkeit des Internen Kontrollsystems durch die Interne Revision darzustellen.

Der DIIR-Arbeitskreis „Revision des Finanz- und Rechnungswesens“ kommt dem anspruchsvollen Ziel mit diesem Band in umfangreicher und fachlich fundierter Art und Weise nach. Durch die risikoorientierte Betrachtung der prozessbezogenen Steuerungs- und Kontrollaktivitäten entlang der jeweiligen Prozessablaufkette und Darstellung der Methoden zur Überprüfung auf Wirksamkeit des Internen Kontrollsystems durch die Interne Revision können die Leitfäden auch als ein Baustein für die Überprüfung der Wirksamkeit des Risikomanagementsystems herangezogen werden.

Den Mitgliedern des DIIR-Arbeitskreises, die die Prüfungsleitfäden erarbeitet haben, sprechen wir unseren Dank und unsere Anerkennung aus. Das Autorenteam unter der Leitung von Herrn

Sami Abbas, Wiesbaden

bestand aus

Sabine Bohlenz, Gelsenkirchen
Martin Guder, Wolfsburg
Clemens Jung, Solingen
Dr. Stefan Kullmann, Essen
Claudia Lazarz, Berlin
Matthias Meyer, Wolfsburg
Wulf-Matthias Nolte, Mannheim
Ilja Papas, Neuss
Christoph Tennstedt, Neckarsulm
Oliver Wiesehahn, Haiger.

Wir danken auch den Unternehmen, die durch die Mitwirkung ihrer Mitarbeiter die Erarbeitung dieses Prüfungsleitfadens ermöglicht haben.

Frankfurt am Main, im Januar 2020

DIIR – Deutsches Institut für Interne Revision e.V.

Bernd Schartmann
(Sprecher des DIIR-Vorstandes)

Ralf Herold
(Mitglied des DIIR-Vorstandes)

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
ABS	Asset-backed Securities
ADR	Accord européen relatif au transport international
AEO	Authorised Economic Operator
AEO-Zertifikats	Authorised Economic Operator-Zertifikat
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
AO	Abgabenordnung
A. T. A.	admission temporaire/temporary admission („vorübergehende Einfuhr“)
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BANF	Bestellanforderung
BilMoG	Bilanzrechtsmodernisierungsgesetz
BMF	Bundesministerium der Finanzen
bspw.	beispielsweise
BVL	Bundesvereinigung Logistik
bzgl.	bezüglich
bzw.	beziehungsweise
CAPEX	Capital Expenditure
CFaR	Cashflow at Risk
CMS	Compliance Management System
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COSO-ERM	COSO-Enterprise Risk Management
COSO-IC/ COSO I	COSO Internal Control
CP	Commercial Paper
DCGK	Deutscher Corporate Governance Kodex
d.h.	das heißt
diesbezgl.	diesbezüglichen
DIIR	Deutsches Institut für Interne Revision e.V.

DIN	Deutsches Institut für Normung e.V.
DIN EN ISO/ IEC 17025	Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien
DMS	Dokumentenmanagementsystem
DOK	Dokument
DV	Datenverarbeitung
eANV	elektronisches Abfallnachweisverfahren
ebd.	ebenda
EBIT	Earnings Before Interest and Taxes
EDI	electronic data interchange
EDV	Elektronische Datenverarbeitung
EfbV	Entsorgungsfachbetriebeverordnung
EK	Einkauf
EMIR	European Market Infrastructure Regulation
ERM	Enterprise Risk Management
ERP	Enterprise-Resource-Planning
EStG	Einkommensteuergesetz
et al.	et alii (und andere)
etc.	et cetera (und so weiter)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUR	Euro
e.V.	eingetragener Verein
f.	folgend
ff.	fortfolgend
F&E	Forschung und Entwicklung
FFM	Fremdfirmenmanagement
FR	Frankreich
FRA	Forward Rate Agreements
ggf.	gegebenenfalls
GmbH	Gesellschaften mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoB	Grundsätze ordnungsmäßiger Buchführung

GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
GuV	Gewinn- und Verlustrechnung
GZ	Geschäftszeichen
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
IIA	Institute of Internal Auditors
IAS	International Accounting Standards
IC	Intercompany
i.d.R.	in der Regel
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IFRS	International Financial Reporting Standards
i.H.v.	in Höhe von
IKS	Internes Kontrollsystem
inkl.	inklusive
Intrastat	Intrahandelsstatistik
IPO	Initial Public Offering
i.S.	im Sinne
IT	Informationstechnologie
i.V.m.	in Verbindung mit
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator
KrW-/AbfG	Kreislaufwirtschafts- und Abfallgesetz
lit.	littera (Buchstabe)
LME	London Metal Exchange
LuL	Lieferung und Leistung
MaRisk	Mindestanforderungen an das Risikomanagement
Mio.	Millionen
Mrd.	Milliarden
MS-Excel	Microsoft Excel
MTN	Medium Term Notes
NachwV	Nachweisverordnung
n.F.	neue Fassung

Nr.	Nummer
Nutzer-ID	Nutzeridentifizierung
NY	New York
o. a.	oben angeführt
OMB	Office of Management and Budget
OWiG	Ordnungswidrigkeitengesetz
PS	Prüfungsstandard
rd.	rund
REACH	Registration, Evaluation, Authorisation and Restriction of Chemicals
RFID	radio-frequency identification
RHB	Roh-, Hilfs- und Betriebsstoffe
RMS	Risikomanagementsystem
Rn.	Randnummer
Rs.	Rechtssache
ROI	Return-on-Investment
S.	Seite
SAP-CO/PS	SAP-Module Controlling, Projektsystem
SAP-MM	SAP-Modul Materials Management
SEC	Securities and Exchange Commission
Slg.	Sammlung
sog.	sogenannt
SOX	Sarbanes-Oxley Act
SvEV	Sozialversicherungsentgeltverordnung
TAN	Transaktionsnummer
TEUR	Tausend Euro
TgV	Transportgenehmigungsverordnung
Tz.	Textziffer
u. a.	unter anderem
u. U.	unter Umständen
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer
U. S.	United States (of America)
USA	United States of America
US-GAAP	United States Generally Accepted Accounting Principles

USt	Umsatzsteuer
UStG	Umsatzsteuergesetz
UZK	Unionszollkodex
v.	von
VDR	Verband Deutsches Reisemanagement e. V.
verb.	verbundene
vgl.	vergleiche
VK	Verkaufspreis
vs.	versus
VSt	Vorsteuer
WE	Wareneingang
WP	Wirtschaftsprüfer
WTU	Werttransportunternehmen
z. B.	zum Beispiel
zzgl.	zuzüglich

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Praxisleitfäden zur Revision des Internen Kontrollsystems richtet sich an Revisorinnen und Revisoren, die Prüfungen der Internen Revision zur Wirksamkeit des Internen Kontrollsystems (IKS) im Unternehmen durchführen. Im Vordergrund stehen die Prozesse und Teilprozesse eines Unternehmens, deren Risiken, die prozessbezogenen Steuerungs- und Kontrollaktivitäten sowie beispielgebende Prüfungshandlungen für die Interne Revision, um die Wirksamkeit der Aktivitäten und somit des IKS zu überprüfen und ggf. nachhaltig zu verbessern.

1.1 Vorbemerkung

Nachdem bereits mehrere Vorschriften auf nationaler Ebene die gesetzlichen Vertreter von Kapitalgesellschaften zur Einführung eines wirksamen und funktionsfähigen IKS verpflichteten,[1] richtete sich das Bilanzrechtsmodernisierungsgesetz (BilMoG) im Jahr 2009 schließlich auch an die betreffenden Aufsichtsorgane.

Das BilMoG konkretisierte die Aufgaben eines Aufsichtsrats im Hinblick auf die Beurteilung der Wirksamkeit des IKS, des Risikomanagementsystems (RMS) und des Internen Revisionssystems und fand in § 107 Abs. 3 des Aktiengesetzes (AktG) entsprechende Berücksichtigung. Gemäß § 91 Abs. 2 AktG obliegt es allerdings dem Vorstand, geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen hinreichend frühzeitig erkannt werden. Diese aktienrechtliche Regelung hat Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer anderer Gesellschaftsformen, insbesondere für mittlere und große GmbHs je nach Größe und Komplexität ihrer Struktur.[2]

Der Gesetzgeber verzichtete indes auf eine nähere Definition der Begriffe und führte im BilMoG nicht aus, wie die Systeme auszugestalten sind oder wie eine Prüfung der Wirksamkeit durchzuführen ist.

Vor diesem Hintergrund kommt dem Rahmenwerk „Internal Control – Integrated Framework“ (COSO-IC Modell oder auch COSO I) des Committee of Sponsoring Organizations of the Treadway Commission (COSO) besondere Bedeutung zu, da es durch die U. S. Securities and Exchange Commission (SEC) als ein mögliches Rahmenkonzept zur Einrichtung und Dokumentation

1) Vgl. Bungartz, Oliver, Handbuch Interne Kontrollsysteme (IKS), 5., neu bearbeitete und erweiterte Auflage, Berlin 2017, S. 41 ff.

2) Vgl. Deutscher Bundestag, 13. Wahlperiode, Drucksache 13/9712, Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), 28. 01. 1998, S. 15, Abs. 7.

eines IKS zur Umsetzung des Sarbanes-Oxley Act (SOX), Section 404, anerkannt wurde. Die Orientierung am COSO-IC Modell bei der Prüfung der Wirksamkeit eines IKS durch die Interne Revision ist insofern angebracht und zweckmäßig.

Bei der Beurteilung des IKS ist auf die Angemessenheit (Aufbauprüfung) und auch auf die Wirksamkeit (Funktionsprüfung) einzugehen.

Die Angemessenheit des IKS ist gegeben, wenn die Maßnahmen der Geschäftsleitung, des Überwachungsorgans oder anderer Stellen geeignet sind, die Risiken angemessen zu steuern und die Wahrscheinlichkeit erhöhen, dass die Ziele der Organisation erreicht werden.

Von einer Wirksamkeit des IKS ist auszugehen, wenn die aufeinander aufbauenden IKS-Elemente (Kontrollumfeld, Risikobeurteilung, Kontrollaktivitäten, Information und Kommunikation, Überwachungsaktivitäten) ordnungsgemäß durchlaufen werden, sodass die Erreichung der unternehmerischen Ziele mit ausreichender Wahrscheinlichkeit sichergestellt wird.

Zu beachten ist, dass in der Regel durch die Interne Revision einzelne Geschäftsprozesse geprüft werden. Soll das Prüfungsergebnis eine Aussage zur Wirksamkeit des IKS enthalten, sollte ersichtlich sein, für welchen Geschäftsprozess die IKS-Elemente überprüft wurden.

Die vorliegenden Praxisleitfäden legen den Schwerpunkt auf die prozessbezogenen Steuerungs- und Kontrollaktivitäten und die Schritte zur Prüfung der Wirksamkeit. Die betrachteten Teilprozesse können einzelnen IKS-Elementen zugeordnet werden. Die Prüfung der Wirksamkeit bezieht sich somit auf diese IKS-Elemente. Eine Aussage zur Wirksamkeit des IKS für einen vollständigen Geschäftsprozess ist nur möglich, wenn alle Kriterien der aufeinander aufbauenden IKS-Elemente erfüllt sind.

1.2 Prüfungsleitfaden zur Prüfung der Funktionsweise und Wirksamkeit des Internen Kontrollsystems

Für die einzelnen Prozessabläufe/-schritte sind in diesem Band der betreffende (Haupt-)Prozess, das inhärente Risiko, die jeweilige(n) beispielhafte(n) prozessbezogene(n) Steuerungs- und Kontrollaktivität(en) innerhalb des IKS sowie die zu empfehlende Methodik bei der Prüfung der Wirksamkeit durch die Interne Revision tabellarisch für die einzelnen Themenbereiche aufgeführt.

Die aufgezeigten Steuerungs- und Kontrollaktivitäten umfassen dabei die gesamte Prozessablaufkette für den betreffenden (Haupt-)Prozess, ohne dabei den Anspruch auf Vollständigkeit zu erheben. Die empfohlenen Aktivitäten sind bewusst zusammengefasst aufgeführt, da sie nur ganzheitlich ein angemessenes und wirksames IKS gewährleisten. Eine Fragmentierung in einzelne IKS-Punkte würde zwar eine einfachere Bearbeitung sowohl für den jewei-

ligen IKS-Verantwortlichen wie auch für die Prüfung der Wirksamkeit durch die Interne Revision bedeuten, allerdings mit der Gefahr, dass nur auf die aus dem Gesamtzusammenhang gerissene Funktionsweise der einzelnen Kontrolle abgestellt würde. Selbige stellt per se allein nicht bzw. nur eingeschränkt ein angemessenes IKS sicher.

Je nach Geschäft, Branche, Größe und organisatorischer Ausgestaltung des Unternehmens sind unterschiedliche Abläufe und IKS-Mechanismen in unterschiedlicher Ausprägung vorhanden, die jeweils für eine sichere, effiziente und effektive Abwicklung der einzelnen Aktivitäten geeignet sein können. Primär führt der „Weg zum «richtigen» IKS … bei Unternehmen jeder Art und Größe über den risikogerechten Bedarf",[3] wobei ggf. IKS-Mechanismen aufgrund bestehender externer regulatorischer Anforderungen für einzelne Branchen etc. (z.B. Banken, Versicherungen, öffentlich-rechtliche Unternehmen) zusätzlich zu berücksichtigen sind.

Insofern gilt es immer, den jeweiligen Prozessablauf und die implementierten Steuerungs- und Kontrollaktivitäten vorab aufzunehmen und nachfolgend gegen die in dem Prüfungsleitfaden aufgeführten prozessbezogenen Steuerungs- und Kontrollaktivitäten unter Einbeziehung ggf. bestehender regulatorischer Anforderungen zu spiegeln. Daneben sind ggf. die Konsistenz und vermeintlich existierende Abweichungen auf deren Sinnhaftigkeit und Angemessenheit unternehmensspezifisch zu hinterfragen (Customizing des Prüfungsleitfadens auf das vorliegende Prüfungsobjekt). Nur dann kann auf dieser Basis eine angemessene und hinreichende risikoorientierte Prüfung der Wirksamkeit des IKS mittels der nachfolgend empfohlenen Methoden sichergestellt werden.

1.3 Exkurs

Die Mitglieder des DIIR-Arbeitskreises „Revision des Finanz- und Rechnungswesens" kommen aus Unternehmen unterschiedlicher Branchen, Unternehmensformen und Größe. Diskussionen im Arbeitskreis während der Erarbeitung des Praxisleitfadens zeigten die Notwendigkeit, auf wesentliche Aspekte des IKS und des RMS zur Sicherstellung eines einheitlichen Verständnisses des Leitfadens einleitend einzugehen. Zur Vertiefung der grundlegenden Kenntnisse zum IKS und zum RMS wird auf die einschlägigen Rahmenwerke verwiesen.[4]

3) Vgl. Leibundgut, Heinz, IKS – Zwischen Zwang und Bedarf, in: Der Schweizer Treuhänder, Heft 11/2006, S. 838.

4) Für das grundlegende Verständnis des IKS siehe insbesondere Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control – Integrated Framework, Jersey NY, September 1992 und Mai 2013; und des Risikomanagementsystems siehe im Einzelnen COSO, Enterprise Risk Management – Integrated Framework, Jersey NY, September 2004.

1.3.1 Begriff des Internen Kontrollsystems

Bei dem Begriff des „Internen Kontrollsystems“ handelt es sich um eine unvollständige und deshalb oft missverstandene Übersetzung des englischen „Internal Control Systems“. Im Vordergrund des „Internal Control Systems“ steht nicht die Kontrolle, wie die oftmals zu kurz gegriffene deutsche Übersetzung/Interpretation vermuten lässt.

Die Notwendigkeit zur Einrichtung eines „Internal Control Systems“ wurde in den USA bereits Mitte des letzten Jahrhunderts erkannt, insbesondere um Betrug, Verschwendung und Missbrauch von Regierungsmitteln entgegenzutreten. Im „Accounting and Auditing Act“ von 1950 forderte der US-amerikanische Gesetzgeber die Einrichtung eines angemessenen „systems of internal control“ durch das Management. In den nachfolgenden Jahren präzisierte die Legislative die Inhalte und bezog sich auf erste „internal control standards“.[5] In diesen wird u. a. beschrieben, dass die „internal control systems“ sicherstellen sollen, dass die Ziele der Organisation erreicht werden.[6] Die grundsätzlichen Aussagen wurden von dem 1985 gegründeten Committee of Sponsoring Organizations of the Treadway Commission (COSO) aufgegriffen und in den Folgejahren weiterentwickelt. Das Rahmenwerk „Internal Control – Integrated Framework“ (COSO-IC Modell oder auch COSO I) aus dem Jahr 1992 gilt als erstes umfassendes Konzept zur Beschreibung und Überprüfung eines „Internal Control Systems“.

COSO bezieht sich in seinem COSO-IC Modell darauf, dass im Allgemeinen „Internal Control“ als ein Prozess definiert wird, der durch die Geschäftsführung, das Management oder andere Mitarbeiter ausgeführt wird und derart ausgestaltet ist, um mit ausreichender Sicherheit die Erreichung der Unternehmensziele für die nachfolgenden Kategorien zu gewährleisten:

- Effektivität und Effizienz der Geschäftsprozesse,
- Verlässlichkeit der Berichterstattung,
- Einhaltung der gültigen Gesetze und Vorschriften.

Dem Begriff „to control“ kommt im Kontext des COSO-IC Modells weniger die Bedeutung des „Kontrollierens“ zu, sondern er stellt vielmehr darauf ab, Risiken bei gleichzeitiger Überwachung der zugehörigen Prozesse zu steuern, um die Unternehmensziele zu erreichen.

5) Vgl. Executive Office of the President, Office of Management and Budget (OMB), OMB Circular A-123 – Management's Responsibility for Internal Control, Washington D. C., S. 1981 ff., in der aktuell gültigen Fassung vom Juli 2015, Abruf vom 22. 07. 2018 via www.whitehouse.gov.

6) Vgl. ebd.

In der deutschen Auflage der „Internationalen Standards für die berufliche Praxis der Internen Revision 2017“ des Institute of Internal Auditors wird „Control“ übersetzt mit „Kontrolle“. Die zugehörige Definition beschreibt jedoch die umfangreichere Bedeutung des Begriffs im Englischen: „Jede Maßnahme der Geschäftsleitung, des Überwachungsorgans oder anderer Stellen, die dazu dient, Risiken zu steuern und die Wahrscheinlichkeit zu erhöhen, dass gesetzte Ziele erreicht werden. Das Management plant, organisiert und steuert die Durchführung ausreichender Maßnahmen, durch die die Zielerreichung soweit wie möglich gewährleistet wird.“[7)]

Auch in diesem Sinne wäre „Risikosteuerung“ eine zutreffende Übersetzung des Begriffs „control“. Dementsprechend ließe sich der Begriff „Internal Control System“ nicht nur als „Internes Kontrollsystem“ deuten, sondern vielmehr als „Internes Risikosteuerungssystem“ interpretieren. Eine Nähe zum RMS ist erkennbar.

1.3.2 Das Interne Kontrollsystem in Abgrenzung zum Risikomanagementsystem

Das BilMoG unterscheidet zwischen der Beurteilung der Wirksamkeit des IKS und der Beurteilung der Wirksamkeit des RMS. Da das IKS der Bedeutung entsprechend auch als Internes Risikosteuerungssystem bezeichnet werden könnte und Schnittmengen mit dem RMS bestehen, ist eine Betrachtung der beiden Systeme zur richtigen Ausgestaltung der Prüfungsaufträge für die Interne Revision zwingend erforderlich.

Das dreidimensionale COSO-IC Modell beschreibt in dem sog. COSO-Würfel in der ersten Ebene die drei Unternehmenszielkategorien (Betrieblich, Berichterstattung, Regeleinhaltung) und definiert in der zweiten Dimension die Inhalte eines IKS mittels der fünf folgenden Komponenten:

1. Kontrollumfeld,
2. Risikobeurteilung,
3. Kontrollaktivitäten,

7) Vgl. DIIR – Deutsches Institut für Interne Revision e.V., Frankfurt am Main, Institut für Interne Revision Österreich (IIA Austria), Wien, Schweizerischer Verband für Interne Revision (IIA Switzerland), Zürich (Hrsg.), Internationale Standards für die berufliche Praxis der Internen Revision 2017 – Mission, Grundprinzipien, Definition, Ethikkodex, Standards, Frankfurt am Main 10. Januar 2018 (Version 6.1), S. 59.

4. Information und Kommunikation,
5. Überwachung.[8)]

Die dritte Dimension beschreibt die Verankerung der Unternehmenszielkategorien und der IKS-Komponenten in den Unternehmenseinheiten/-aktivitäten. Diese gelten für alle Konzern- oder Unternehmenseinheiten.

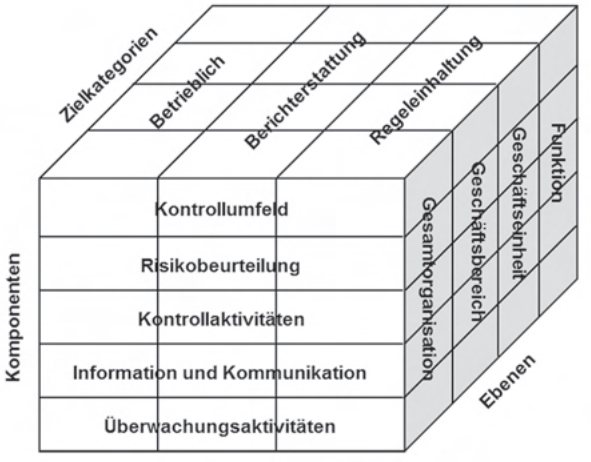

Abbildung 1: Das COSO-IC Modell

Quelle: In Anlehnung an Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. Executive Summary, Mai 2013.[9)]

Im Jahr 2004 veröffentlichte das Committee of Sponsoring Organizations of the Treadway Commission das Rahmenwerk „Enterprise Risk Management – Integrated Framework" (COSO-ERM oder auch COSO II).[10)] Bei diesem Rahmenwerk handelt es sich um ein grundlegendes Konzept zur Überprüfung des unternehmensweiten Risikomanagements.

8) Im COSO-Modell aus Mai 2013 wird anstatt des Begriffs „monitoring" der Begriff „monitoring activities" (deutsches Synonym: Überwachungsaktivitäten) verwendet.

9) Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. Executive Summary, Mai 2013, S. 6, verfügbar unter www.theiia.org.

10) Vgl. Institut für Interne Revision Österreich, Deutsche Fassung vom Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework (2004), Wien 2009.

COSO-ERM basiert auf dem COSO-IC Modell und integriert die zuvor beschriebenen Elemente des IKS in das RMS.

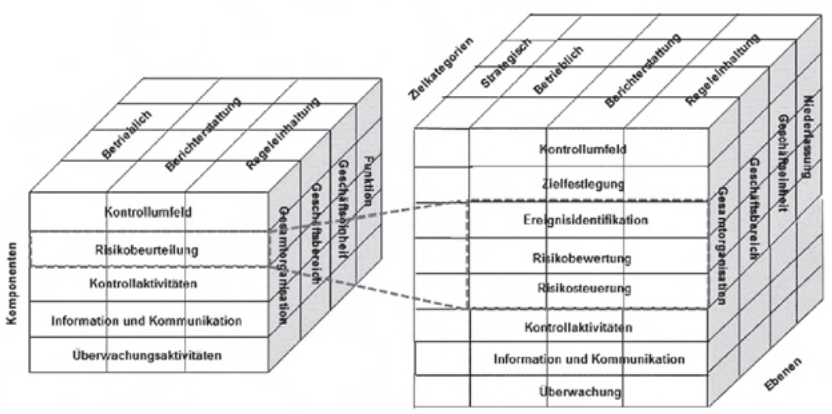

Abbildung 2: Übergang von COSO-IC auf das COSO-ERM Modell

Quelle: Eigene Darstellung in Anlehnung an COSO – Internal Control – Integrated Framework. Executive Summary[11] und COSO – Enterprise Risk Management – Integrated Framework.[12]

Die Unternehmensziele werden in COSO-ERM um eine vierte Kategorie, die strategischen Ziele, ergänzt. Ferner werden die fünf Komponenten des IKS um drei weitere Komponenten ergänzt: Zielfestlegung, Ereignisidentifikation und Risikosteuerung. Die IKS-Komponente „Kontrollumfeld" wurde unter Hinzufügen neuer Aspekte zum „Internen Umfeld" weiterentwickelt. Gemäß COSO-ERM beinhaltet ein RMS die folgenden, aufeinander aufbauenden acht Komponenten:

1. Internes Umfeld,
2. Zielfestlegung,
3. Ereignisidentifikation,
4. Risikobeurteilung,
5. Risikosteuerung,
6. Kontrollaktivitäten,

11) Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, Executive Summary, Jersey NY Mai 2013, S. 6, verfügbar unter www.theiia.org.

12) Vgl. Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework (2004), Deutsche Fassung vom Institut für Interne Revision Österreich, Wien 2009, S. 7.

7. Information und Kommunikation,
8. Überwachung.

Aus Sicht der Internen Revision ist es von Bedeutung, dass die drei neuen Komponenten des COSO-ERM Modells bereits in der Detailbeschreibung des COSO-IC Modells Erwähnung finden. Das COSO-IC Modell beschreibt den Prozess der Zielfestlegung (neue ERM-Komponente Nr. 2) als eine Voraussetzung für die Durchführung der Risikobeurteilung.[13] Der Prozess der Risikoidentifikation (integriert in der neuen ERM-Komponente Nr. 3 Ereignisidentifikation) ist im COSO-IC Modell sogar wesentlicher Bestandteil in der Beschreibung der zweiten IKS-Komponente, der Risikobeurteilung. Es wird betont, dass es sich bei der Risikoidentifikation um einen iterativen Prozess handelt, der eine kritische Komponente eines wirksamen IKS darstellt[14] und der Risikobeurteilung vorangestellt sein muss.[15]

Auch auf die Risikosteuerung (neue ERM-Komponente Nr. 5) wird im COSO-IC Modell bereits eingegangen. COSO-ERM bezeichnet als Risikosteuerungsmaßnahmen die Maßnahmen, die vom Management getroffen werden, um die bewerteten Risiken zu vermeiden, zu reduzieren, zu teilen oder zu akzeptieren.[16] In den Ausführungen zu der Risikobeurteilung im COSO-IC Modell wird betont, dass das Management nach Abschluss der Risikobeurteilung festlegen muss, wie die Risiken zu managen, also zu steuern sind.[17] Es wird allerdings auch explizit darauf hingewiesen, dass im COSO-IC Modell nur die Risikobeurteilung Bestandteil des IKS ist. Die Maßnahmen, die getroffen werden, um den Risiken zu begegnen, sind nach dieser Definition ein Bestandteil der umfassenderen Managementprozesse.[18]

Im Vergleich der in beiden Modellen enthaltenen Komponente Kontrollaktivitäten zeigen sich weitere Unterschiede. Im COSO-ERM Modell dienen die Kontrollaktivitäten dazu, sicherzustellen, dass die Risikosteuerungsmaßnahmen ordnungsgemäß und zeitgerecht durchgeführt werden.[19] Die Kontrollaktivitäten im COSO-IC Modell sind umfassender zu verstehen. Dort wird u. a.

13) Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. Framework, Jersey NY, Mai 1994, S. 33.
14) Vgl. ebd., S. 39.
15) Vgl. ebd., S. 42.
16) Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management – Integrated Framework, Jersey NY, September 2004, S. 55.
17) Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. Framework, Mai 1994, S. 42.
18) Vgl. ebd., S. 43.
19) Vgl. Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework, Jersey NY, September 2004, S. 61.

unterschieden zwischen vorbeugenden, aufdeckenden, manuellen, IT-basierten und Management-Kontrollaktivitäten. Einige beispielhaft aufgezählte Kontrollaktivitäten wären im COSO-ERM Modell den Risikosteuerungsmaßnahmen zuzuordnen (z. B. Funktionstrennung, Zugriffsberechtigungen). Daraus ergibt sich eine Inkonsistenz in der Abgrenzung der Modelle, da die Risikosteuerung unter Umständen Bestandteil des Internen Kontrollsystems ist. Durch die Einführung der Komponente Risikosteuerung im COSO-ERM Modell erfolgte eine genauere Abgrenzung zwischen den Risikosteuerungsmaßnahmen und den Kontrollaktivitäten.

In den „Internationalen Standards für die berufliche Praxis der Internen Revision 2017" wird der Begriff „Kontrolle" als „jede Maßnahme der Geschäftsleitung, des Überwachungsorgans oder anderer Stellen, die dazu dient, Risiken zu steuern und die Wahrscheinlichkeit zu erhöhen, dass gesetzte Ziele erreicht werden …" definiert.[20)]

Auch die Mindestanforderungen an das Risikomanagement[21)] (MaRisk) definieren die Risikosteuerungsprozesse explizit als Bestandteil des IKS (MaRisk AT 4.3 Internes Kontrollsystem). Daneben bezeichnet auch das Institut der Wirtschaftsprüfer (IDW) die Aktivitäten, die geeignet sind, wesentliche Fehler in der Rechnungslegung zu verhindern bzw. aufzudecken und zu korrigieren als Kontrollaktivitäten.[22)]

Festzuhalten ist, dass die neuen Komponenten des COSO-ERM Modells Zielfestlegung und Ereignisidentifikation gemäß dem COSO-IC Modell formal nicht Bestandteil des IKS sind, jedoch von nicht unerheblicher Bedeutung für die Wirksamkeit des IKS sind. Im COSO-ERM Modell werden die Risikosteuerungsmaßnahmen eigenständig hervorgehoben und von den Kontrollaktivitäten abgegrenzt. Die diesbezügliche Auseinandersetzung mit den Risikosteuerungsmaßnahmen und den Kontrollaktivitäten kann das prüferische Verständnis für die Kontrollaktivitäten des COSO-IC Modells, die auch Risikosteuerungsmaßnahmen enthalten können, schärfen und ist insofern zu empfehlen.

---

20) Vgl. DIIR – Deutsches Institut für Interne Revision e. V., Frankfurt am Main, Institut für Interne Revision Österreich (IIA Austria), Wien, Schweizerischer Verband für Interne Revision (IIA Switzerland), Zürich (Hrsg.), Internationale Standards für die berufliche Praxis der Internen Revision 2017 – Mission, Grundprinzipien, Definition, Ethikkodex, Standards, Frankfurt am Main 10. Januar 2018 (Version 6.1), S. 59.

21) Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin); Mindestanforderungen an das Risikomanagement – MaRisk, Rundschreiben 09/2017 (BA) vom 27. 10. 2017.

22) Vgl. Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) (Hrsg.), IDW PS 261 n. F. – Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken, in: Heft 4/2012 der IDW Fachnachrichten sowie dem WPg-Supplement 2/2012, Tz. 49.

Die Tabellen des vorliegenden Praxisleitfadens beinhalten neben der Spalte „Risiko“ die Spalte „Prozessbezogene Steuerungs- und Kontrollaktivität“, um das Zusammenspiel der Risikosteuerungsmaßnahmen und der Kontrollaktivitäten des Fachbereichs zu verdeutlichen.

Die Betrachtung der zugrundeliegenden COSO-Modelle zeigt, dass eine Abgrenzung einer Wirksamkeitsprüfung des IKS und einer Wirksamkeitsprüfung des RMS nicht unerheblich ist. Da das IKS Bestandteil des RMS ist, kann es eine vereinfachende prüferische Alternative sein, dem integrativen Ansatz zu folgen und Prüfungen nach dem COSO-ERM Modell durchzuführen. Wenn die Wirksamkeit der einzelnen, aufeinander aufbauenden Elemente des COSO-ERM Modells durch eine Revisionsprüfung bestätigt werden kann, ist grundsätzlich davon auszugehen, dass sowohl das RMS als auch das IKS wirksam sind.

Der Praxisleitfaden unterstützt beide Ansätze und kann sowohl als Grundlage für die Überprüfung der Wirksamkeit des IKS als auch als ein Baustein für die Überprüfung der Wirksamkeit des RMS herangezogen werden.

1.3.3 Beurteilung der Wirksamkeit des Internen Kontrollsystems

Die Beurteilung der Wirksamkeit des IKS und des RMS durch den Aufsichtsrat beschränkt sich nicht auf den rechnungslegungsbezogenen Teil des Unternehmens, sondern ist umfassend durchzuführen und hat alle wesentlichen Geschäftsprozesse zu berücksichtigen.[23)]

Die Einrichtung eines wirksamen IKS und RMS liegt in der Verantwortung der Unternehmensleitung,[24)] die dadurch selbst ein ureigenes Interesse hat oder zumindest haben sollte, die Wirksamkeit zu überwachen.

Neben dem Abschlussprüfer, dessen Prüfung des Jahresabschlusses gemäß § 317 Abs. 1 S. 1 HGB auch die Beurteilung des rechnungslegungsbezogenen IKS[25)] umfasst, sind insbesondere die unternehmensinternen Überwachungs-

23) Vgl. Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/10067, Entwurf eines Gesetzes zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – Bil-MoG), 30. 07. 2008, S. 102, Abs. 7 ff.

24) Vgl. Bungartz, Oliver, Handbuch Interne Kontrollsysteme (IKS), 4. neu bearbeitete und erweiterte Auflage, Berlin 2014, S. 39 ff.

25) Vgl. Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/10067, Entwurf eines Gesetzes zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – Bil-MoG), 30. 07. 2008, S. 45, Abs. 8; vgl. Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) (Hrsg.), IDW PS 261 n. F. – Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken, Tz 40 ff.

maßnahmen zur Wirksamkeit des IKS bzw. des RMS bezogen auf das Gesamtunternehmen für die Unternehmensleitung von besonderer Bedeutung.

Sowohl das COSO-IC Modell, der IDW-Prüfungsstandard „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken" (IDW PS 261), der DIIR-Prüfungsstandard Nr. 2 „Prüfung des Risikomanagementsystems durch die Interne Revision"[26] als auch das Three Lines of Defense-Modell[27] legen einvernehmlich dar, dass die unternehmensinternen Überwachungsmaßnahmen auf verschiedenen Ebenen zu erfolgen haben. Dabei ist zu berücksichtigen, dass bereits das operative Management, die sog. First Line of Defense, eine Überwachung der eigenen Prozesse sicherzustellen hat. Der IDW PS 261 spricht in diesem Zusammenhang von den prozessintegrierten Überwachungsmaßnahmen.[28] In Bezug auf den im vorherigen Kapitel verwendeten Bezeichnungen des COSO-IC Modells sind darunter die Kontrollaktivitäten zu verstehen.

Diese prozessintegrierte Überwachung durch das operative Management wird durch die prozessunabhängigen Überwachungsmaßnahmen der Einheiten der Second Line of Defense (z. B. Controlling, Risikomanagement) und der Third Line of Defense (Interne Revision) ergänzt. Im COSO-IC Modell entsprechen diese Maßnahmen der IKS-Komponente „Überwachungsaktivitäten".

Im Sinne eines einleitenden Überblicks ist die vorliegende Darstellung des IKS verkürzt. Insofern ist darauf hinzuweisen, dass z. B. auch das operative Management über zusätzliche prozessunabhängige Überwachungsmaßnahmen verfügen kann, z. B. indem innerhalb eines Geschäftsbereichs für besonders relevante Risiken Monitoringaktivitäten unabhängig von der Second bzw. Third Line of Defense an eine nicht direkt im Prozess involvierte Abteilung delegiert werden, die z. B. Key Performance Indikatoren überwacht.

Der Internen Revision kommt bei den unternehmensinternen Überwachungsmaßnahmen eine besondere Rolle zu, als dass sie weitestgehend das einzige Überwachungsinstrument ist, welches einen gesamtheitlichen Blick auf die Unternehmensprozesse hat. Der Fokus der Einheiten der Second Line of De-

26) Vgl. Deutsches Institut für Interne Revision e. V. (DIIR) (Hrsg.), Revisionsstandard Nr. 2 – Prüfung des Risikomanagementsystems durch die Interne Revision, Frankfurt am Main veröffentlicht im August 2014 und geändert im September 2015 (Version 1.1), Tz. 15.

27) Vgl. The Institut of Internal Auditors – IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, Januar 2013, Abruf vom 04. 07. 2018 via www.theiia.org.

28) Vgl. Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) (Hrsg.), IDW PS 261 n. F. – Feststellung und Beurteilung von Fehler-risiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken, in: Heft 4/2012 der IDW Fachnachrichten sowie dem WPg-Supplement 2/2012, Tz 20 und 34.

fense ist hingegen viel stärker auf einzelne Prozesse ausgerichtet. Für eine umfassende Aussage zur Wirksamkeit des IKS und des RMS des Gesamtunternehmens ist die Interne Revision deshalb die prädestinierte Instanz.

Das IKS und das RMS sollten so aufgebaut sein, dass sie sich fortlaufend selbst beurteilen, indem die Prozessverantwortlichen der First Line of Defense alle Komponenten des IKS oder RMS ordnungsgemäß durchführen und eigenständig Störungen im System erkennen und ohne Einwirkung Dritter Korrekturen veranlassen. Grundsätzlich sollte die Wirksamkeit der Systeme nicht von der Second bzw. Third Line of Defense abhängig sein.

2 Prüfung der Funktionsweise und Wirksamkeit des Internen Kontrollsystems

2.1 Beschaffungs-/Einkaufsmanagement

2.1.1 Beschaffung / Einkauf

Die Begriffe „Beschaffung" und „Einkauf" stehen in der betrieblichen Praxis im Kontext mit den Begriffen „Logistik" und „Materialwirtschaft" für bestimmte Funktionen und Aufgaben und sind in jedem Unternehmen aufgrund unterschiedlichster zugrundeliegender Strukturen oftmals mit verschiedenen Inhalten besetzt. Der Begriff der „Materialwirtschaft" wird indes dabei grundsätzlich als Oberbegriff für sämtliche Aktivitäten der Materialversorgung verwendet.[29)]

In der einschlägigen Literatur wird die Einkaufsfunktion (z. B. mit den Aufgaben Marktforschung, Angebotsvergleich, Lieferantenauswahl, Preisverhandlungen) grundsätzlich als ein Teil des Beschaffungsprozesses definiert. Der Beschaffungsprozess umfasst daneben noch zusätzlich – im Sinne der Erlangung und Bereitstellung der für die Erstellung und Verwertung der Produkte eines Betriebes erforderlichen Güter – u. a. die Aufgaben Bestellvorgang, Termin- und Transportmanagement/-kontrolle, Wareneingang, Rechnungsprüfung und zum Teil auch noch die Kreditorenbuchhaltung.[30)]

Aufgrund der o. a. uneinheitlichen Abgrenzung in der betriebswirtschaftlichen Literatur wie auch in der betrieblichen Praxis werden die Begriffe Beschaffung und Einkauf im Folgenden gleichbedeutend verwendet. Der Begriff Beschaffung/Einkauf wird bezogen auf die nachfolgenden prozessbezogenen IKS-Steuerungs- und Kontrollaktivitäten und deren Überprüfung auf Wirksamkeit im Sinne der sog. „6 R" verwendet, d. h. die Versorgung der Unternehmung mit Waren und Gütern (Materialien, Produkten, Dienstleistungen etc.)

- der benötigten Art (die richtigen Objekte),
- in der richtigen Menge,
- am richtigen Ort,
- zum richtigen Zeitpunkt,

29) Vgl. Kluck, Dieter, Materialwirtschaft und Logistik, 3. überarbeitete Auflage, Stuttgart 2008, S. 1.

30) Vgl. Becker, Jörg, Winkelmann, Axel, Handelscontrolling: Optimale Informationsversorgung mit Kennzahlen, 2. überarbeitete und erweiterte Auflage, Wiesbaden 2008, S. 168; Küpper, Hans-Ulrich, Beschaffung (Kapitel B. 2.), S. 189, in Baetge, Jörg, u. a., Vahlens Kompendium der Betriebswirtschaftslehre, Band 1, Hans-Ulrich Küpper, Kapitel B. 2. Beschaffung, München 1984.

- in der richtigen Qualität und
- zu den richtigen Kosten.[31)]

Ausgenommen hiervon ist die Beschaffung von Immobilien, Finanzmitteln und eigenem Personal.[32)] In diesen Bereichen liegen spezielle Umstände/Besonderheiten und Marktgegebenheiten vor, aufgrund derer eigenständige Bereiche/Abteilungen im Unternehmen, wie z. B. die Bereiche Finanzen/Treasury, Facility-Management und Personal/Human Resources, zuständig sind und dementsprechend hierfür auch separate prozessbezogene IKS-Steuerungs- und Kontrollaktivitäten bestehen.[33)]

Die Bedeutung einer effizienten und effektiven Beschaffung hat für die Zielerreichung der Unternehmung bis in die heutige Zeit aufgrund der kontinuierlich sinkenden Wertschöpfungstiefe stetig zugenommen. Im Jahr 2012 wurden bereits über alle Branchen hinweg durchschnittlich rd. 50 % der Wertschöpfung eines Unternehmens extern eingekauft, verbunden mit entsprechend höheren Einkaufsvolumina.[34)] Aufgrund dessen ist aktuell auch die Existenz und Wirksamkeit eines diesbezüglichen IKS für die Sicherstellung einer ordnungsgemäßen, effizienten Funktionsweise der unternehmensspezifischen Beschaffungs-/Einkaufsaktivitäten von außerordentlich wichtiger Bedeutung für die Unternehmung.

Wie o. a. unterscheidet sich der Beschaffungsprozess in seiner Ausgestaltung individuell von Unternehmen zu Unternehmen, wobei das grundlegende Prozessmodell mit seinen Teilprozessen und deren Inhalten grundsätzlich gleich ist und sich wie folgt darstellt:

31) Vgl. dazu im Einzelnen näher Jünemann, Reinhardt, Materialfluss und Logistik: Systemtechnische Grundlagen mit Praxisbeispielen, Berlin/Heidelberg 1989, S. 18; Kluck, Dieter, Materialwirtschaft und Logistik, 3. überarbeitete Auflage, Stuttgart 2008, S. 7 ff.

32) Die Beschaffung von externen (temporären) Personalkapazitäten im Bereich Projektgeschäft etc. wie z. B. Montage-/Baustellenpersonal ist hiervon ausdrücklich zu trennen und ist dem Bereich Einkauf/Beschaffung zuzuordnen.

33) Zu diesbezüglichen besonderen Punkten/Inhalten betreffend des Themenkomplexes Personal siehe Kapitel 2.5, betreffend des Themenkomplexes Instandhaltung siehe Kapitel 2.6.3 und betreffend des Themenkomplexes Finanzen/Treasury siehe Kapitel 2.11.

34) Vgl. Bungartz, Oliver, Handbuch Interne Kontrollsysteme (IKS), 3., neu bearbeitete Auflage, Berlin 2012, S. 119.

Abbildung 3: Prozessmodell zur Beschaffung

Quelle: Eigene Darstellung

Die möglichen, hinsichtlich ihrer Wirksamkeit zu prüfenden Steuerungs- und Kontrollaktivitäten stellen sich wie folgt dar:

Tabelle 1: Beschaffung/Einkauf

Prozess	**Risiko**	**Prozessbezogene Steuerungs- und Kontrollaktivitäten**	**Prüfung der Wirksamkeit**
Aufbau- und Ablauf-organisation: Regelwerke/ Richtlinien[35]	Aufgrund fehlender, (strukturierter) bzw. nicht hinreichender unternehmensinterner Regelwerke, z.B. in Form von Richtlinien/Arbeitsanweisungen, besteht das grundsätzliche Risiko, dass Prozesse nicht einheitlich, ordnungsgemäß, sicher, effizient und effektiv i.S. einer angemessenen Corporate Governance und ggf. unterer Beachtung/Einhaltung externer Vorschriften (Gesetze etc.) abgewickelt werden, verbunden mit einer unter Umständen fehlerhaften bzw. unvollständigen Rechnungslegung und wirtschaftlichen Schäden.	Die für den Bereich verantwortliche Leitung hat sicherzustellen, dass – für alle wesentlichen Prozessabläufe strukturierte und adäquate Regelwerke in Form von Richtlinien/Arbeitsanweisungen etc. existieren, in den Schnittstellen zu anderen Bereichen/ Abteilungen abgestimmt und den betreffenden Mitarbeitern bekannt sind, – wesentliche Änderungen in den Prozessabläufen bzw. aufgrund von externen Anforderungen (z.B. Gesetzesänderungen) zeitnah zu Änderungen/Anpassungen der Richtlinien/Arbeitsanweisungen etc. führen (Aktualität) und den betreffenden Mitarbeitern bekannt sind, – die Aktualität/Adäquanz des Regelwerks regelmäßig überprüft und ggf. angepasst wird (z.B. mindestens einmal pro Jahr).	Prüfung, ob ordnungsgemäß genehmigte, aktuelle und zweckmäßige Richtlinien/ Arbeitsanweisungen, die inhaltlich alle rechnungslegungsrelevanten Geschäftsprozesse/Angelegenheiten für den Bereich regeln, vorliegen.

35) Zu diesbezüglichen besonderen Punkten/Inhalten betreffend des Themenkomplexes Compliance (inkl. Verhaltenskodex, Kartellrecht, Korruptionsbekämpfung sowie Sonderfällen/-bedingungen in einzelnen Branchen, wie z.B. gesetzlicher Erfordernisse bzgl. der Existenz eines Compliance-Management-Systems im Bankenbereich) siehe Kapitel 2.16.1.

Prozess	Risiko	Prozessbezogene Steuerungs- und Kontrollaktivitäten	Prüfung der Wirksamkeit
Aufbau-organisation	Fehlende Regelungen bzw. Regelungslücken hinsichtlich Kompetenzen, Verantwortlichkeiten, Vollmachten und Vertretung können zu wirtschaftlichen Risiken/ Schäden verbunden mit einer unter Umständen unvollständigen bzw. fehlerhaften Rechnungslegung führen.	Die für den Bereich verantwortliche Leitung hat kontinuierlich sicherzustellen, dass – in den Stellenbeschreibungen die Verantwortlichkeiten inkl. adäquater Funktionstrennungen, – angemessene und sichere Vertretungsregelungen sowie – adäquate Vollmachten-/Unterschriftenregelungen vorhanden, kommuniziert und im entsprechenden Regelwerk dokumentiert sind.	Inhaltliche Prüfung der – Stellenbeschreibungen, – Vertretungsregelungen und – Vollmachten-/Unterschriftenregelungen auf nebenstehende Punkte und auf Aktualität.
Aufbau-organisation	Fachbereiche sind zwar berechtigt, bestimmte Beschaffungsumfänge eigenständig einzukaufen, die notwendige Qualifizierung ist jedoch nicht vorhanden.	Falls der Einkauf bestimmte Beschaffungsvorgänge an Fachbereiche delegiert, ist sicherzustellen, dass es hierzu eindeutige Vorgaben gibt sowie die Fachbereichsmitarbeiter entsprechend geschult/ qualifiziert werden.	Prüfung der Zweckmäßigkeit der Vorgaben bezüglich Wirtschaftlichkeit und Risiken. Prüfung des Schulungs-/Qualifizierungskonzepts auf Vorhandensein und Wirksamkeit. Prüfung einer Stichprobe aus den von den Fachbereichen durchgeführten Einkäufen auf Übereinstimmung mit den Vorgaben (kein sog. Maverick Buying[36]).

36) Maverick Buying bezeichnet die eigenmächtige Beschaffung von Materialien oder Dienstleistungen einzelner Personen oder Abteilungen, ohne den Einkauf einzubeziehen, und somit unter Umgehung festgelegter bzw. standardisierter Beschaffungsprozesse bzw. -wege.

Prozess	Risiko	Prozessbezogene Steuerungs- und Kontrollaktivitäten	Prüfung der Wirksamkeit
Stammdaten	Stammdatenanlagen und -änderungen (Materialwirtschaft, Kreditoren) werden nicht korrekt vorgenommen mit dem Risiko von z.B. Vermögensschäden/-verlusten.	Es existiert ein Verfahren, dass sicherstellt, dass die Erfassung/Änderung von wesentlichen Stammdaten (Firmierungen, Bankverbindungen) gemäß dem vorgegebenen Prozess, z.B. von autorisierten Mitarbeitern im Vier-Augen-Prinzip, vorgenommen wird. Eine Funktionstrennung ist implementiert.	Prüfung, ob – der vorgegebene Prozess (z.B. Nutzung eines Stammdatenanlageformulars, Freigabe der Stammdaten bzw. Kontrolle der eingepflegten Daten durch eine zweite Person, eingeschränkter Personenkreis zur Pflege der Stammdaten) eingehalten wird, – eine Funktionstrennung implementiert ist, d.h. z.B. keine Eingaben von Finanzdaten durch den Einkauf, – bei einer Vertrauensperson des Lieferanten die Richtigkeit der Stammdaten abgefragt werden können.
Stammdaten	Es werden Änderungen an den Stammdaten (Materialwirtschaft, Kreditoren) vorgenommen, die nicht nachvollziehbar/prüfbar sind mit dem Risiko von z.B. Vermögensschäden/-verlusten.	Alle Änderungen der Stammdaten werden systemtechnisch protokolliert, um jederzeit eine Nachvollziehbarkeit zu gewährleisten.	Prüfung, ob z.B. anhand von Stammdatenänderungsprotokollen Änderungen an den Stammdaten nachvollzogen werden können.

Prozess	Risiko	Prozessbezogene Steuerungs- und Kontrollaktivitäten	Prüfung der Wirksamkeit
Bestell-anforderung (BANF) durch den Fachbereich	Die BANFen werden von nicht hierfür berechtigten Mitarbeitern genehmigt. Für den Beschaffungswert steht kein ausreichendes Budget zur Verfügung	In den Fachbereichen besteht ein Genehmigungskonzept unter Beachtung des Vier-Augen-Prinzips und einer wertabhängigen Zuordnung der berechtigten Mitarbeiter. Zusammen mit der BANF-Erstellung muss geprüft werden, ob die benötigten Budgetmittel vorhanden sind. Beachtung der Funktionstrennung: Der BANF-Genehmigter darf nicht bestellberechtigt sein.	Prüfung, ob – hinsichtlich der Genehmigung das Vier-Augen-Prinzip und eine wertabhängige Zuordnung sowie die Funktionstrennung vorgegeben sind und auch eingehalten werden. – bei der BANF-Erstellung (Stichprobe) auch die notwendigen Budgetmittel vorhanden waren.
Lieferanten-auswahl	Finanzielle Schäden aufgrund fehlerhafter Lieferantenauswahl (Nichtkonformität mit technischen und wirtschaftlichen Anforderungen in Bezug auf Zeit, Qualität und Kosten). Die Bewertungskriterien sind nicht geeignet oder bevorzugen einen bestimmten Lieferanten.	Durchführung einer Lieferantenbewertung auf Basis eines existierenden, angemessenen unternehmensintern etablierten Systems zu zwei Zeitpunkten: – Bei Projekten/Projektgeschäft während Angebotsvorbereitungsphase für die wichtigsten Lieferanten, auf deren Angeboten die Angebotskalkulation basiert, – grundsätzlich final vor Abgabe einer Bestellung. Durchführung eines dokumentierten Preisvergleichs entsprechend den unternehmensinternen Einkaufsrichtlinien unter Berücksichtigung der Spezifikationen	Aufnahme des Prozessablaufs inkl. Validierung, ob nebenstehende Steuerungs- und Kontrollaktivitäten i.S. des Minimalprinzips darin verankert sind. Validierung des Prozessablaufs hinsichtlich weiterer Steuerungs- und Kontrollaktivitäten unter Kosten-/Nutzenaspekten.