Helfer/Geiersbach/Riediger/Hanenberg

Interne Kontrollsysteme in Banken und Sparkassen

- **Vorgaben & Erwartungen der Bankenaufsicht**
- **Schlüsselkontrollen implementieren & optimieren**
- **Kontrollrahmen & Risikoanalysen**
- **Prüfung & Kontrolltests**

3. Auflage

Finanz Colloquium Heidelberg, 2020

Zitiervorschlag:

Autor in: Helfer/Geiersbach/Riediger/Hanenberg (Hrsg.), Interne Kontrollsysteme in Banken und Sparkassen, 3. Auflage, RdNr. XX.

ISBN: 978-3-943170-89-4

Finanz Colloquium Heidelberg GmbH
Im Bosseldorn 30, 69126 Heidelberg
www.FCH-Gruppe.de
info@FCH-Gruppe.de
Satz: MetaLexis, Niedernhausen
Druck: VERLAGSDRUCKEREI SCHMIDT GMBH,
Neustadt an der Aisch

Helfer/Geiersbach/Riediger/Hanenberg

Interne Kontrollsysteme in Banken und Sparkassen

- **Vorgaben & Erwartungen der Bankenaufsicht**
- **Schlüsselkontrollen implementieren & optimieren**
- **Kontrollrahmen & Risikoanalysen**
- **Prüfung & Kontrolltests**

3. Auflage

Ralf Barsch
Geschäftsführer,
Advanced Audit Solutions

Dirk Bolte
WP/StB, stv. Revisionsdirektor, Prüfungsstelle des
Hanseatischen Sparkassen- und Giroverbandes, Hamburg

Jürgen Büschelberger
Leiter des Regionalbereichs Banken und Finanzaufsicht
Hauptverwaltung Bayern, Deutsche Bundesbank

Michael Claaßen
Bereichsleiter Interne Revision,
Volksbank Marl-Recklinghausen eG

Dr. Karsten Geiersbach, CIA (Hrsg.)
CIA, Bereichsleiter Interne Revision,
Kasseler Sparkasse

Ludger Hanenberg (Hrsg.)
Abteilungsleiter Grundsatzabteilung der Versicherungsaufsicht,
Bundesanstalt für Finanzdienstleistungsaufsicht

Michael Helfer (Hrsg.)
Geschäftsführer,
FCH Consult GmbH

Björn Reher
Wirtschaftsprüfer/Steuerberater,
Partner Financial Services/Gesellschafter,
Mazars GmbH & Co. KG

Henning Riediger (Hrsg.)
Prüfungsleiter im Referat Bankgeschäftliche Prüfungen bei
der Hauptverwaltung, Deutsche Bundesbank, Hannover

Pascal Ritz
Geschäftsführer,
Justo Unternehmensberatung GmbH

Dr. Stefan Scheve
Sachgebietsleiter Laufende Aufsicht Sparkassen,
Deutsche Bundesbank Hauptverwaltung
Bremen, Niedersachsen und Sachsen-Anhalt

Marc Stränger
Sparkassenbetriebswirt, Abteilungsleiter Compliance,
Sparkasse Krefeld

Lukas Walla
Mitarbeiter Regulatorik/Compliance in der
Investitionsbank Schleswig-Holstein

Finanz Colloquium Heidelberg, 2020

Inhaltsübersicht

Inhaltsverzeichnis

Vorwort der Herausgeber

Die Entwicklung des Internen Kontrollsystems (IKS) im Bankensektor wurde in den letzten 25 Jahren laufend weiterentwickelt. Insbesondere durch die aufgetretenen Schieflagen und Unregelmäßigkeiten in Kreditinstituten resultierend in oder aus der Finanzmarktkrise 2007, steht das IKS ständig im Mittelpunkt der Gesetzgebung und der aufsichtsrechtlichen Vorschriften. Dies führte im Laufe der Entwicklung zu immer weitergehenden Verschärfungen in den gesetzlichen und bankaufsichtlichen Vorgaben, so dass nunmehr (überfällig) die 3. Auflage dieses Werkes erfolgt.

Während die 1. und 2. Auflage noch durch das Herausgeber-Duo Helfer/ Ullrich begleitet wurden, erfolgte nun eine Veränderung im Herausgeber-Team sowie die Erweiterung des Autorenteams um erfahrene Bankexperten. An dieser Stelle gebührt unser Dank Herrn *Walter Ullrich,* der als Mit-Herausgeber die 1. und 2. Auflage mit viel Engagement und Leidenschaft begleitet hat. Er befindet sich mittlerweile im verdienten Ruhestand und stand somit für eine neue Auflage leider nicht mehr zur Verfügung.

Mit der nun vorliegenden 3. Auflage wird die Grundidee dieses Buches weiter vorangetrieben. Im Kern soll eine Zusammenführung der in den unterschiedlichen Bereichen enthaltenen IKS-Anforderungen und Risikoanalysen zu einem Gesamtsystem im Rahmen eines ganzheitlichen Risikomanagementsystems dargestellt werden. Dabei spannt sich der Bogen von den international beeinflussenden Modellen (insbesondere COSO) über die gesetzlichen und bankaufsichtlichen Vorgaben (zunehmend verschärft durch die europäischen Anforderungen) bis hin zu praxisorientierten Lösungsansätzen. Abgerundet wird das Thema durch interne und externe (Prüfungs-)Tipps. Hilfreich waren dabei die zahlreich vorhandenen literarischen Quellen als Grundlagen für unsere Ausführungen, den jeweiligen Autoren danken wir für ihre fundierten Aussagen und Anregungen.

Im Kern kann man sagen, dass in den letzten Jahren Umfang und auch Qualität der regulatorischen Anforderungen weiter zugenommen haben. Zudem werden die kommenden Jahre das »Zeitalter der Aufsicht« sicher noch ausdehnen. Besonders hervorzuheben sind die SREP-Neuerungen sowie die vergangenen und bereits angekündigten Anpassungen der MaRisk. Hier ist anzumerken, dass die MaRisk wie auch in der Vergangenheit den einschlägigen europäischen und internationalen Vorgaben folgen. Insbesondere der Prozess der Übernahme von Leitlinien der europäischen Aufsichtsgremien

EBA, ESMA und EIOPA ist weiter strukturiert worden. So hat z. B die BaFin im Mai 2019 das Protokoll der Sitzung des Fachgremiums MaRisk vom 05.11.2018 auf die Homepage der BaFin gestellt. Darin wird u. a. ausgeführt, dass »im Regelfall davon ausgegangen werden kann, dass die BaFin die Leitlinien der EBA, der ESMA und der EIOPA in ihre Verwaltungspraxis übernimmt. Soll eine Leitlinie der EU-Behörden ausnahmsweise nicht oder – was in der Praxis eher vorkommt – nicht vollständig (etwa aufgrund von Konflikten mit deutschen gesellschaftsrechtlichen Regelungen) übernommen werden, benennt die BaFin diese Leitlinien auf ihrer Homepage. Im Einzelfall kann für die Übernahme in das deutsche Aufsichtsrecht ein Rechtsakt erforderlich sein (z. B. der Erlass oder die Änderung einer Verordnung). Für den Fall der Umsetzung durch ein Rundschreiben oder die Novellierung eines Rundschreibens müssten die LSIs die hieraus resultierenden Anforderungen aus der Guideline dann in der Tat erst mit der Veröffentlichung des nationalen Rundschreibens anwenden. Auch dann seien die LSIs aber gehalten, sich bereits vorher mit dem Inhalt der betreffenden (und regelmäßig auch in der deutschen Amtssprache vorliegenden) Leitlinien zu befassen und organisatorische Vorkehrungen zu treffen, um die hierin adressierten Anforderungen umzusetzen«. Daher sollten sich die Institute frühzeitig mit neuen europäischen Entwicklungen, primär denen bei der EBA, auseinandersetzen. Dies wird insbesondere die kleineren bis mittleren Institute vor große Herausforderungen stellen. Umso mehr wird es darauf ankommen, die bestehenden Systeme mit den aktuellen und den künftigen Anforderungen in einer sinnvollen, sprich ganzheitlichen, Art und Weise zu verbinden.

Letztlich sollte ein wirksames und hinreichend dokumentiertes IKS nicht nur im Interesse der Bank sein, es steht auch im Fokus der Bankenaufsicht und der Abschluss-/Sonderprüfer. Die nach § 25a KWG geforderte IKS-Wirksamkeits-Überwachung (Regel-Einhaltung) kann bei Organisationsmängeln zudem harte Konsequenzen nach sich ziehen, wie z. B. in der Form von Kapitalzuschlägen. Was also tun? Best Practice ist die Erstellung und Dokumentation einer Prozesslandkarte mit den entsprechenden Teilprozessen. Auf dieser Basis können alle Prozessbeteiligten eine konkrete am Prozessablauf orientierte Risiko- und Kontroll-Zuordnung vornehmen. Das Dilemma der Praxis besteht in vielen Instituten aber immer noch in nicht prozessorientierten Arbeitsanweisungen, die zudem nicht die Abläufe der eigenen IT-Anwendungen mit einbeziehen. Die darin enthaltenen Kontrollen sind oftmals »verstreut« und darüber hinaus nicht MaRisk-konform dargestellt (vgl. MaRisk: »… klare Abgrenzung der Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen

und Kommunikationswege«). Dies führt mitarbeiterseitig dazu, dass Arbeitsanweisungen nicht mehr angemessen gewürdigt und Kontrollen nicht immer verstanden und beachtet werden. Zur Unterstützung der eingangs erwähnten, weiteren Anforderungen der Bankenaufsicht, ist daher eine Identifikation und Dokumentation des gesamten IKS zielführend (inkl. der aufbauorganisatorischen Schlüsselkontrollen, welche zumeist unpräzise in Richtlinien dargelegt sind). Neben der verbesserten Transparenz für die Mitarbeiter (und damit einer höheren Akzeptanz der Regelwerke) gewinnen Vorstand und Aufsichtsrat bzw. Verwaltungsrat ein pragmatisch-effizientes und zuverlässiges Organisationsniveau, welches die Regulatorik eher als Leitplanken für das Geschäftsmodell versteht (und somit die bankaufsichtlichen Anforderungen nicht als Zentrum des Handelns). Auf dieser Basis kann das individuelle IKS-Design, die Dokumentation, ein fortlaufendes Monitoring (inkl. Kontroll-Tests) sowie die Prüfung der Internen Revision aller wesentlichen IKS-Bestandteile erfolgen. Einmal derartig implementiert, können sich Vorstand und Aufsichts-/bzw. Verwaltungsrat regelmäßig durch entsprechende IKS-Reports vom Zustand des IKS überzeugen und gegebenenfalls weitere Maßnahmen veranlassen. Für die Institute gilt daher künftig noch mehr als bisher, die bisherigen Regelwerke und alle diesbezüglichen Verfahren zu überprüfen und zukunftsorientiert auszurichten!

Die Autoren haben in ihren praxisnahen Ausführungen diesbezüglich die verschiedenen Eckpunkte herausgearbeitet. Hilfestellung bieten dabei die Darstellung der maßgeblichen wesentlichen IKS-Bestandteile sowie Praxistipps.

Neben den selbstredend erfolgten Anpassungen auf der Basis der letzten MaRisk-Novelle wurde die inhaltliche Strukturierung des Werkes insbesondere im Abschnitt »IKS-Anforderungen für die Bankprozesse« stark prozessorientiert dargestellt. In diesem Kontext findet auch das sogenanntes Three-Lines-of-Defense-Modell (3 LoD) zunehmend Beachtung in der Praxis und wurde daher ebenfalls neu in das Werk mit integriert. Da im Autorenteam u. a. auch vier Vertreter der Bankenaufsicht mitgewirkt haben, ist es nicht verwunderlich, dass die Sichtweise der Aufsicht in dieser Auflage nochmals erweitert wurde.

Das vorliegende Handbuch wendet sich an alle, die für ein zeitgemäßes Risikomanagementsystem inkl. eines Internen Kontrollsystems in einer Bank oder Sparkasse verantwortlich zeichnen. Das beginnt mit der Geschäftsleitung, den jeweiligen Verantwortlichkeiten in den Stabs-/Steuerungs-, Fach- und Com-

pliancebereichen und endet mit der Internen Revision. Unser Bestreben war und ist es, zu verdeutlichen, dass die institutsinternen IKS-Lösungen eine wichtige Grundlage für das Risikomanagement darstellen und zudem regelmäßig von externer Seite (Abschlussprüfer und Bankenaufsicht) auf den Prüfstand gestellt werden. Ein angemessenes IKS sowie dessen Dokumentation tragen einerseits zur Risikominimierung und zu positiven externen Prüfungsergebnissen und andererseits zu einer optimierten Umsetzung des Geschäftsmodells bei.

Den beteiligten Autoren sagen wir Danke für ihre fundierten Beiträge, in denen sie ihre umfassenden Erfahrungen aus ihrer Berufspraxis sowie ihre theoretischen Fachkenntnisse haben einfließen lassen. Wir hoffen, dass wir Ihnen mit diesem Werk viele praktische Anregungen und Hilfestellungen für die Umsetzung im eigenen Institut geben können. Als Herausgeber-Team würden wir uns zudem auch über Anregungen und Rückfragen sehr freuen.

Okober 2019

Michael Helfer

Dr. Karsten Geiersbach

Henning Riediger

Ludger Hanenberg

A.

Bedeutung des IKS für die Bankenaufsicht

A. Bedeutung des IKS für die Bankenaufsicht

I. Europäische Bankenaufsicht – Umsetzung des SREP

1. Einführung

Mit der Verabschiedung der SREP (Supervisory Review and Evaluation Process-)Leitlinien durch die EBA im Dezember 2014 war die Erwartung verbunden gewesen, dass die europäischen Bank-Aufsichtsbehörden ihre nationalen SREP-Verfahren stärker angleichen. Die deutsche Aufsicht hat sich verpflichtet, diese europäischen Anforderungen in ihren Aufsichtsprozess zu integrieren. Dabei betrat die Aufsicht aber keineswegs völliges Neuland, denn der Prozess der Beurteilung der einzelnen Institute bildete schon seit geraumer Zeit einen wichtigen Teil der aufsichtlichen Praxis. Allerdings bedeutet die mit der Veröffentlichung der Leitlinien verbundene Erwartungshaltung der EBA, dass nunmehr generell für die Institute Kapitalaufschläge wegen bestimmter zusätzlicher institutsspezifischer Risiken festzulegen sind, eine Herausforderung für die Aufsicht. Das dazu entwickelte Verfahren, das eine Kombination aus quantitativen und qualitativen Aspekten umfasst, wird im Rahmen eines stufenweisen Vorgehens seit Mitte 2016 umgesetzt. 1

Dabei kommt u. a. den Governance-Anforderungen eine große Bedeutung zu. Das gilt nicht nur für die nationale Sichtweise, sondern auch für die Erwartungshaltung, wie sie in den SREP-Leitlinien der EBA zum Ausdruck kommt. So beschäftigt sich der Titel 5 der EBA-SREP-Leitlinien (Governance und interne Kontrollen) u. a. mit der Bewertung der internen Unternehmensführung und institutsweiter Kontrollen. Dort wird ein Rahmen abgesteckt, der von den Aufsichtsbehörden auszufüllen ist. 2

So sollen im SREP die interne Unternehmensführung und institutsweiten Kontrollen u. a. in folgenden Aspekten betrachtet werden: 3

- Regelrahmenwerk für generelle interne Unternehmensführung
- Unternehmenskultur und Risikokultur
- Organisation und Funktionsweise des Leitungsorgans
- Vergütungsvorschriften und -praktiken
- Regelwerk zum Risikomanagement einschließlich ICAAP und ILAAP

- **Regelwerk für interne Kontrollen einschließlich der Internen Revision**
- Informationssysteme und Geschäftskontinuität
- Sanierungsplanungen.

4 Im Folgenden soll daher der Schwerpunkt auf einige Erwartungen im Hinblick auf interne Kontrollen einschließlich der Internen Revision gelegt werden.

2. EBA-Leitlinien über interne Unternehmensführung

5 Gemäß den **EBA-Leitlinien über interne Unternehmensführung (Tz. 104)** sollten die verantwortlichen Aufsichtsbehörden einschätzen, ob das Institut über ein angemessenes Regelwerk für interne Kontrollen verfügt. Hierbei sollen **mindestens** die **folgenden Aspekte** abgedeckt sein:

a) Internes Kontrollsystem (IKS), Kontrolleinheiten und Verantwortlichkeiten

6 Das interne Kontrollsystem und seine wesentlichen aufsichtsrechtlichen Anforderungen sind nicht neu. Die aktuelle **MaRisk-Novelle aus 2017** erwartet in AT 4.3 wie bisher auch, dass jedes Institut »entsprechend Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten u. a. Regelungen zur Aufbau- und Ablauforganisation zu treffen hat«. Hierzu gehört insbesondere ein **Regelwerk für das interne Kontrollsystem**. In der Praxis ist zu beobachten, dass t ein solches Rahmenwerk regelmäßig u. a. die folgenden Aspekte umfasst:

- Ausführungen zur IKS-Aufbau- und Ablauforganisation
- Definition von **Aufgabenträgern** (u. a. zentrale sowie dezentrale IKS-Beauftragte, Prozess- und Kontrollverantwortliche sowie die Berichtslinie zur Geschäftsleitung)
- Anwendung des **»3-Lines-of-Defense«**-Modells auf die eigene Organisation
- **IKS-Management** (u. a. Identifizierung und Bewertung von Risiken, Dokumentation, Angemessenheits- und Wirksamkeitsbewertung sowie Maßnahmen zur Stabilisierung/Verbesserung der Kontrollhandlungen und Berichtswesen).

7 So gibt es Modelle, bei der die Verantwortlichkeit für die Implementierung eines solchen Regelwerks in der Hand eines zentralen »IKS-Verantwortlichen«

liegt. Dieser koordiniert nicht nur die Umsetzung, sondern überwacht auch die einheitliche Anwendung der festgelegten Kontrollverfahren.

Aspekte, die zu einem IKS-Rahmenwerk gehören, finden sich u. a. im sog. **3-Lines-of-Defense-Modell** bzw. Modell der 3 Verteidigungs- bzw. Abwehrlinien, auf das sich auch der Baseler Ausschuss in seinem Dokument zur Internen Revision bezieht. 8

In der nachfolgenden Abbildung wird daher die Trennung der unterschiedlichen – jeweils unabhängig voneinander agierenden – Kontrolleinheiten hervorgehoben. 9

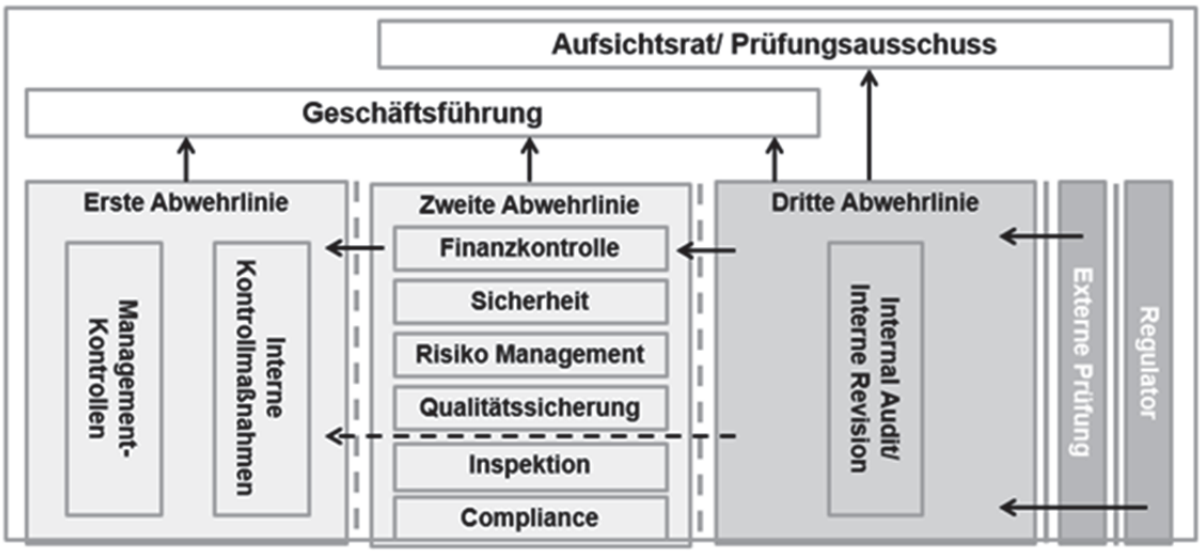

Abbildung A. – 1: 3-Lines-of-Defense-Modell
(European Confederation of Institutes of Internal Auditing (ECIIA))

Die **erste Verteidigungslinie** umfasst das operative Management sowie prozessintegrierte Kontrollen, die verantwortlich sind für die **Bewertung, Kontrolle und Reduzierung von Risiken**. Diese Kontrollhandlungen sind Bestandteil der Aufgaben **im Rahmen des Tagesgeschäfts** der Geschäftsfelder bzw. Fachbereiche. Hierunter fällt auch die **Überwachung der Aktivitäten und Funktionen der zugelassenen Geschäftsleitung**, für die sie direkt verantwortlich ist. In die Verantwortung der Geschäfts- und Unterstützungseinheiten gehören u. a. folgende Aufgaben: 10

- **Kennen der »eigenen« Normen** (schriftlich fixierte Ordnung in Form von Arbeitsanweisungen bzw. Prozessdokumentationen)
- Identifizierung und Kennen der Risiken (**Risikoinventur**)
- Definition von **angemessenen** Kontrollen sowie **Transparenz** der eigenen Schlüsselkontrollen

- Herstellen von **Referenzen zwischen Kontrollen und Risiken** (Eintrittswahrscheinlichkeit und Schadenshöhe)
- Sicherstellen der **Wirksamkeit von Kontrollhandlungen** (Einhaltung der Prozesse und definierten Kontrollen, **Kontroll-Testings**, Kontrollergebnisse, Kontrollreports).

11 Die **zweite Verteidigungslinie** überwacht die Umsetzung wirksamer risikomindernder Maßnahmen, die durch das operative Management durchgeführt werden. Darüber hinaus liegt es in der Verantwortung dieser nachgelagerten Verteidigungslinie die Einhaltung externer Anforderungen zu überwachen. Während die erste Verteidigungslinie die **unmittelbare Verantwortung** für die Identifikation und Steuerung der Risiken hat (Kontrollen, u. a. in Form von 4-Augen-Prinzip, Funktionstrennung und Vorgesetztenkontrolle) nimmt die zweite Verteidigungslinie eine **prozessbegleitende Überwachung** wahr.

12 Im Unterschied zur ersten und zweiten Verteidigungslinie liefert die **dritte Verteidigungslinie** einen wichtigen Beitrag zur Unterstützung der Geschäftsleitung. Das erfolgt vor allem durch einen **risikoorientierten Prüfungsansatz.** Hierbei geht es i. e. L. um die Beurteilung der Effektivität (Funktionsfähigkeit) der Bewertung und Steuerung der Risiken durch die vorgelagerten Verteidigungslinien. Während die zweite Verteidigungslinie prozessbegleitend tätig ist, nimmt die dritte Verteidigungslinie ihre Aufgaben **prozessunabhängig** wahr.

13 In diesem Zusammenhang kann die in den neuen MaRisk AT 4.3.1 geregelte sog. »Cooling-Off-Period« eine besondere Bedeutung erlangen. Gemäß dieser Regelung soll *»beim Wechsel von Mitarbeitern der Vertriebsbereiche in Kontrollbereiche (Risikocontrolling-Funktion, Compliance-Funktion, Marktfolge sowie Abwicklung und Kontrolle) angemessene Übergangsfristen vorzusehen sind, innerhalb derer diese Mitarbeiter keine Tätigkeiten ausüben oder verantworten, die gegen das Verbot der Selbstprüfung und -überprüfung verstoßen«.* Eine ähnliche Vorgabe kennen auch die internationalen Standards für die berufliche Praxis der Internen Revision. Dort beschreibt der Attribut-Standard 1130.A1, dass

> *»Interne Revisoren von der Beurteilung von Geschäftsprozessen absehen müssen, für die sie zuvor verantwortlich waren. Die Objektivität kann als beeinträchtigt angenommen werden, wenn ein Interner Revisor eine Aktivität prüft, für die er im Verlauf des vorangegangenen Jahres verantwortlich war.«*

14 Hiernach kann auch i. S. d. Vorgaben der MaRisk im Allgemeinen Teil 4.3.1 zumindest in vielen Fällen von einer angemessenen »Abkühlungsphase« von 12 Monaten ausgegangen werden.