

2. Grundlagen im Bereich der operationellen Risiken

2.1. Einordnung in das Spektrum der bankbetrieblichen Risikofelder

In der betriebswirtschaftlichen Literatur liegt keine allgemeine und einheitliche Definition des Begriffs „Risiko“ vor.¹⁴ Risiken umschreiben die mögliche Abweichung eines zukünftigen Werts von einem erwarteten oder geplanten Wert.¹⁵ Eine solche Abweichung kann grundsätzlich in zwei Richtungen erfolgen. Eine mögliche positive Abweichung für den Entscheidungsträger wird dabei als „Chance“ bezeichnet, während eine negative Abweichung vom Erwartungswert das „Risiko im engeren Sinne“ beschreibt. Oftmals liegt die Betonung nur auf der negativen Abweichung von einem geplanten Wert.¹⁶ Aufgrund dessen wird mit dem Ausdruck „Risiko“ eine Gefahr möglicher Verluste umschrieben.¹⁷ Auch in der Praxis ist es üblich, nur diese einseitige Betrachtung der ungünstigen Abweichung heranzuziehen,¹⁸ weshalb in der vorliegenden Arbeit der Einfachheit wegen hinsichtlich des Begriffs „Risiko“ auf diese Auffassung abgestellt wird. Es gehört zum alltäglichen Geschäft der Kreditinsti-

¹⁴ Vgl. ROMEIKE, FRANK (Lexikon 2004), S. 102; BARTETZKY, PETER (Risiken 2012), S. 36; STAUSBERG, THOMAS (Fundierung 2012), S. 429. Für eine ausführliche Betrachtung des Risikobegriffs vgl. KRÄMER, GREGOR (Ziele 2000), S. 182–209. Eine umfangreiche Auflistung möglicher Risikoauffassungen erfolgt in KAACK, JÖRN (Performance 2012), S. 12–13 und WEIBENSTEINER, CHRISTIAN (Reputation 2014), S. 10–12.

¹⁵ Vgl. hierzu und zu den nächsten beiden Sätzen BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 865; BRÖSEL, GERRIT (Bankbetrieb 2004), S. 186; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 1; GLEIBNER, WERNER; ROMEIKE, FRANK (Risiko 2015), S. 546.

¹⁶ Vgl. ROMEIKE, FRANK (Lexikon 2004), S. 102; KÖNIGS, HANS-PETER (System 2013), S. 10; KOZLOVA, ELIZAVETA (Datenverarbeitung 2013), S. 107; FISCHER, OLAF (Bankbetriebswirtschaft 2014), S. 218; BERGER, THOMAS (Risikokultur 2015), S. 644.

¹⁷ Vgl. HORN, CHRISTIAN; MÜLLER, CHRISTOPH (Begriff 2001), S. 194; NAGEL, REINHARD (Neuordnung 2010), S. 124; BARTETZKY, PETER (Risiken 2012), S. 36; WOLKE, THOMAS (Risikomanagement 2016), S. 1.

¹⁸ Vgl. BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 865.

tute, Risiken einzugehen.¹⁹ Hierbei versteht man unter Kreditinstituten nach § 1 Abs. 1 Satz 1 KWG „Unternehmen, die Bankgeschäfte²⁰ gewerbsmäßig oder in einem Umfang betreiben, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert.“ Nachfolgend werden die Begriffe „Kreditinstitut“ und „Bank“ dem allgemeinen Sprachgebrauch folgend synonym verwendet.²¹

Die bankbetrieblichen Risiken lassen sich nach ihren Auswirkungen auf die wirtschaftliche Bestandsfestigkeit in zwei Kategorien einteilen: die Erfolgsrisiken und die Liquiditätsrisiken.²² Werden Erfolgsrisiken schlagend, wird das Kreditinstitut mit einem unmittelbar negativen Einfluss auf den Erfolg konfrontiert. Es kommt zu einer Gewinnminderung bzw. einer Verlusterhöhung, die sich in einer negativen Veränderung der Eigenkapitalgröße des Instituts niederschlägt. Dagegen haben Liquiditätsrisiken einen Einfluss auf die Zahlungsfähigkeit des Instituts. Sie gründen als Fristigkeitsrisiken auf zeitlichen Inkongruenzen zwischen Liquiditätszuflüssen und -abflüssen. Zahlungsmittel können dem Institut indessen entweder nicht zu dem erwarteten Zeitpunkt (temporale Liquiditätsrisiken) oder aber nicht in der erwarteten Höhe (quantitative Liquiditätsrisi-

¹⁹ Vgl. MASLEN, MARTIN (Bankensektor 2010), S. 3; DRANSFELD, IGMAR (Messverfahren 2014), S. 1.

²⁰ Die Bankgeschäfte umfassen das Einlagengeschäft, das Pfandbriefgeschäft, das Kreditgeschäft, das Diskontgeschäft, das Finanzkommissionsgeschäft, das Depotgeschäft, die Eingehung der Verpflichtung, zuvor veräußerte Darlehensforderungen vor Fälligkeit zurückzuerwerben, das Garantiegeschäft, das Scheckeinzugsgeschäft, das Wechseleinzugsgeschäft, das Reisescheckgeschäft, das Emissionsgeschäft und die Tätigkeit als zentrale Gegenpartei. Vgl. § 1 Abs. 1 Satz 2 KWG.

²¹ Vgl. WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 15, Fn. 3. Es erfolgt auch eine synonyme Verwendung der Begriffe „Eigenkapital“ und „Eigenmittel“. Vgl. WASCHBUSCH, GERD (Bankenaufsicht 2000), S. 179, Fn. 28.

²² Vgl. hierzu und zu den nächsten vier Sätzen CHRISTIAN, CLAUS-JÖRG (Finanzinnovationen 1992), S. 110; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 2–3; SCHIERENBECK, HENNER; LISTER, MICHAEL; KIRMSE, STEFAN (Rentabilität 2014), S. 373.

ken) zu- oder abfließen.²³ Es besteht die Gefahr, auszahlungswirksame Verpflichtungen nicht mehr erfüllen zu können.²⁴ Das Geldanschlussrisiko umschreibt letzten Endes das Risiko, benötigte Zahlungsmittel durch wirksam gewordene Liquiditätsrisiken aus technischen oder aus Gründen der Bonität nicht beschaffen zu können.²⁵ Somit haben Erfolgsrisiken einen direkten Bezug zum Insolvenztatbestand der Überschuldung, wohingegen Liquiditätsrisiken in einer Zahlungsunfähigkeit münden können.²⁶

Oftmals werden in der betriebswirtschaftlichen Literatur lediglich die Adressenrisiken und die Marktpreisrisiken unter dem Begriff „Erfolgsrisiken“ zusammengefasst.²⁷ Jedoch gliedern sich auch die operationellen Risiken in die Vielfalt der Erfolgsrisiken ein, da mit ihnen ebenfalls eine negative Wirkung auf den finanziellen Erfolg des Kreditinstituts einhergeht.²⁸ Die Gefahr einer Gewinnminderung bzw. Verluststeigerung aufgrund der verschlechterten Bonität eines Geschäftspartners wird dabei als Adressenrisiko bezeichnet.²⁹ Es umschreibt das Risiko der Nichterfüllung

²³ Vgl. BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 52.

²⁴ Vgl. GEIERSBACH, KARSTEN (Revision 2011), S. 349; MENNINGEN, MICHAEL (Problemfelder 2014), S. 56.

²⁵ Vgl. BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 55–56.

²⁶ Vgl. CHRISTIAN, CLAUS-JÖRG (Finanzinnovationen 1992), S. 110; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 3.

²⁷ Vgl. BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 920; SCHÄL, INGO (Risiken 2011), S. 20; SCHIERENBECK, HENNER; LISTER, MICHAEL; KIRMSE, STEFAN (Rentabilität 2014), S. 374.

²⁸ Vgl. KRÄMER, GREGOR (Ziele 2000), S. 227–228; HECHENBLAIKNER, ANJA (IT-Risiken 2006), S. 10.

²⁹ Vgl. BECKER, HANS PAUL (Finanzierung 2010), S. 21; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 27; MECHNIK, CHRISTIAN (Outsourcing 2011), S. 163.

von Zahlungsverpflichtungen durch Vertragspartner.³⁰ Die Negativwirkung ergibt sich durch den Abgleich des vereinbarten respektive erwarteten und des tatsächlich zufließenden Geldbetrags.³¹ Dagegen umschreibt das Marktpreisrisiko die Gefahr einer negativen Auswirkung auf die Erfolgssituation des Instituts aufgrund von Änderungen der Marktpreise.³² Einflussfaktoren sind bspw. Zinssätze, Aktienkurse, Rohstoffpreise oder Währungen.³³ Das operationelle Risiko letztlich bezieht sich auf Verlustpotenziale, die aus personellen, sachlich-technischen, ablaufstrukturellen oder rechtlichen Gründen entstehen.³⁴ Auch höhere Gewalt und Einwirkungen von externen Parteien, wie bspw. kriminelle Handlungen, zählen zu dieser Risikokategorie. Sie hat daher einen Bezug zur Qualität und Effizienz der Organisation, der funktionalen Abläufe, des Personals, der Technik und der Kontrollen.³⁵ Risiken aus externen Einflüssen, wie z. B. Naturkatastrophen oder Terroranschläge, liegen außerhalb der Einflussmöglichkeit der Bank.³⁶ Im Vordergrund steht bei den operationellen

³⁰ Vgl. ROMEIKE, FRANK (Lexikon 2004), S. 70; BCBS (Practices 2009), S. 24; GEIERSBACH, KARSTEN (Revision 2011), S. 349; GISCHER, HORST; HERZ, BERNHARD; MENKHOFF, LUKAS (Kredit 2012), S. 187.

³¹ Vgl. CHRISTIAN, CLAUS-JÖRG (Finanzinnovationen 1992), S. 113.

³² Vgl. BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 998; UTZ, ERICH RUDOLF (Bedeutung 2002), S. 102; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 32; SCHÄL, INGO (Risiko 2011), S. 21; GRELCK, MICHAEL; RICHTER, TIM (Frühwarnindikatoren 2012), S. 510.

³³ Vgl. BECKER, HANS PAUL (Finanzierung 2010), S. 22–23; SCHIERENBECK, HENNER; LISTER, MICHAEL; KIRMBE, STEFAN (Rentabilität 2014), S. 374; HELLENKAMP, DETLEF (Bankwirtschaft 2015), S. 74.

³⁴ Vgl. hierzu und zu dem nächsten Satz BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 869; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 6.

³⁵ Vgl. POSCH, PETER NIKOLAUS; NGUYEN, TRISTAN (Risikoidentifikation 2012), S. 53.

³⁶ Vgl. KAISER, THOMAS; KASPROWICZ, THILO (Reduzierung 2007), S. 331.

Risiken eine ursachenbezogene Definition.³⁷ Sie werden auch als „Betriebsrisiken“ oder „Risiken des internen Leistungsbereichs“ bezeichnet.³⁸

Beachtet werden sollte, dass zwischen den verschiedenen Risikokategorien Interdependenzen bestehen.³⁹ Erfolgsrisiken können Liquiditätsprobleme nach sich ziehen, wenn bspw. durch ein eingetretenes Adressenrisiko in Form eines Kreditausfalls ein nachgelagertes quantitatives Liquiditätsrisiko aufgrund des fehlenden Zuflusses an liquiden Mitteln entsteht. Umgekehrt können Liquiditätsrisiken auch den Erfolg eines Instituts tangieren. So haben ungünstige Refinanzierungskonditionen durch schlagend gewordene qualitative oder quantitative Liquiditätsrisiken einen unmittelbaren Einfluss auf den Erfolg des Instituts. Abhängigkeiten bestehen auch unter den einzelnen Risikokategorien des Erfolgsrisikos, wenn z. B. der Ausfall eines Vertragspartners zum Aufbrechen einer geschlossenen Position führt und sich damit Fremdwährungs- oder Zinsänderungsrisiken ergeben. Abbildung 1 gibt einen Überblick über die bankbetrieblichen Risiken und deren Zusammenhänge.

³⁷ Vgl. KUHN, LUKAS (Gesamtbanksteuerung 2002), S. 156; SCHIERENBECK, HENNER; LISTER, MICHAEL; KIRMBE, STEFAN (Rentabilität 2014), S. 563; WOLKE, THOMAS (Risikomanagement 2016), S. 257.

³⁸ Vgl. BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 869.

³⁹ Vgl. dazu und zu dem restlichen Absatz BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, Gerd (Bankenaufsicht 2011), S. 3–5.

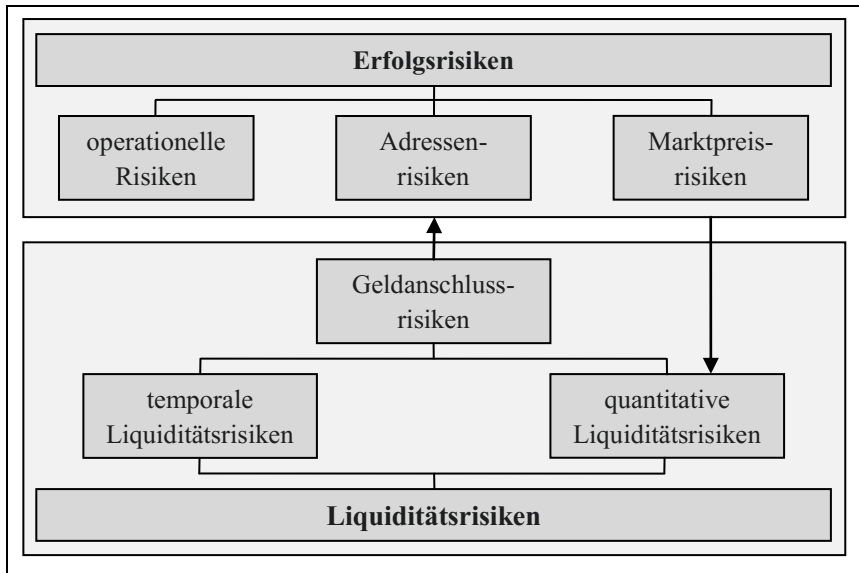


Abbildung 1: Kategorisierung und Interdependenzen der bankbetrieblichen Risiken⁴⁰

2.2. Signifikanz der operationellen Risiken für Kreditinstitute

Operationelle Risiken sind dem Bankgeschäft von jeher inhärent.⁴¹ Sie begleiten ein Institut von seiner Gründung an, weswegen sie als die älteste der Risikokategorien bezeichnet werden.⁴² Operationelle Risiken weisen einige bedeutende Unterschiede zu den anderen Risikokategorien auf,⁴³ die im Folgenden erläutert werden. Das Adressen- und das Marktpreisrisiko gründen auf dem Abschluss von Geschäften und sind daher

⁴⁰ Entnommen aus BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 4.

⁴¹ Vgl. ALLENSPACH, JÖRG (Risikofinanzierungslösungen 2002), S. 286; DEUTSCHE BUNDESBANK; BAFIN (Industrieaktion 2005), S. 10; SCHIERENBECK, HENNER; LISTER, MICHAEL; KIRMBE, STEFAN (Risiko-Controlling 2008), S. 487.

⁴² Vgl. O. V. (Teuer 2001), S. 54; PIAZ, JEAN-MARC (E-Commerce 2001), S. 1231; SCHÖNING, STEPHAN; HOFMANN, MATHIAS (Managementaspekte 2002), S. 882; VIEHMANN, MATTHIAS (Risiko 2006), S. 8; MASLEN, MARTIN (Bankensektor 2010), S. 1.

⁴³ Vgl. KUNZE, BRITTA (Überwachung 2007), S. 43.

geschäftsspezifische Risiken.⁴⁴ Dahingegen sind operationelle Risiken nicht an das Eingehen bestimmter Geschäfte gebunden.⁴⁵ Sie sind mit jeder wirtschaftlichen Aktivität des Instituts untrennbar verknüpft.⁴⁶ Damit sind jene Risiken auch potenziell in allen Unternehmensbereichen vorhanden.⁴⁷ Werden operationelle Risiken schlagend, sind sie zudem geschäftsfeldübergreifend wirksam.⁴⁸ Folglich nehmen sie eine Sonderstellung unter den Risiken ein.⁴⁹ Sie sind nicht nur mit dem Einsatz von Mitarbeitern und Betriebsmitteln verbunden, sondern entstehen auch aus deren Beschaffung und Zusammenwirken im Betriebsablauf.⁵⁰ Operationelle Risiken resultieren hier „aus der Schaffung der Voraussetzungen zum bankbetrieblichen Handeln sowie aus den laufenden Geschäftsprozessen eines Kreditinstituts selbst“⁵¹. Sie müssen eingegangen werden, um das Angebot und den Abschluss von Geschäften erst zu ermöglichen.⁵² Operationelle Risiken sind stets latent vorhanden. Im Extremfall entstehen Verluste bereits bevor das Institut einen einzigen Kunden besitzt oder ein einziges Geschäft abgeschlossen hat.⁵³ Sie beruhen vor-

⁴⁴ Vgl. GLASER, CHRISTIAN (Leasing 2015), S. 102.

⁴⁵ Vgl. WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 47; VIEHMANN, MATTHIAS (Risiko 2006), S. 8.

⁴⁶ Vgl. o. V. (Teuer 2001), S. 54; BECKER, AXEL (Auswirkungen 2005), S. 541; MOHR, BETTINA (Bausteine 2007), S. 66; SCHILLINGS, ROBERT (Gefahr 2008), S. 26; BCBS (Practices 2009), S. 25; HAACKERT, MICHAEL (Aufbau 2009).

⁴⁷ Vgl. WIEDEMANN, ARND; MINZ, KRISTEN-ANNETTE; NIEMEYER, FRITZ (Handlungsfelder 2003), S. 15; KAISER, THOMAS; KASPROWICZ, THILO (Reduzierung 2007), S. 331; WITZANI, ANDREAS (Kapitalanlagegesellschaft 2007), S. 94; LENZMANN, BJÖRN (Bestandteil 2008), S. 280; POSCH, PETER NIKOLAUS; NGUYEN, TRISTAN (Risikoidentifikation 2012), S. 54.

⁴⁸ Vgl. ZIEGER, THOMAS (Überblick 2010), S. 17.

⁴⁹ Vgl. EINHAUS, CHRISTIAN (Diskussion 2002), S. 488.

⁵⁰ Vgl. BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 885.

⁵¹ WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 47.

⁵² Vgl. BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 6; SCHÄL, INGO (Risiken 2011), S. 14.

⁵³ Vgl. zu den letzten beiden Sätzen MINZ, KRISTEN-ANNETTE (Risiken 2004), S. 1; HAUBWALD, FALK (Führungsaufgabe 2008), S. 66.

nehmlich auf endogenen Faktoren.⁵⁴ Aus diesem Grund sind sie stark unternehmensspezifisch.⁵⁵ Im Gegensatz zu Adressen- und Marktpreisrisiken weisen die operationellen Risiken ein asymmetrisches Profil auf, d. h. den eingegangenen Risiken steht keine Ertragschance gegenüber.⁵⁶ Sie weisen nur eine Verlustseite aus,⁵⁷ weswegen sie nicht bewusst eingegangen werden, um einen Ertrag zu erzielen.⁵⁸ Operationelle Risiken sind komplex, vielseitig, miteinander gekoppelt, dynamisch, unbeständig und sie treten diskontinuierlich auf.⁵⁹ Auch handelt es sich um eine sehr heterogene Risikoart.⁶⁰ Ihre Bandbreite ist sehr groß,⁶¹ denn sie erstreckt sich von kleinen, für das Institut unbedeutenden Fällen bis hin zu existenzgefährdenden Ereignissen.⁶² Dies wurde vor allem durch spektakuläre Schadensfälle in der Vergangenheit deutlich.⁶³ Es kann festgehalten wer-

⁵⁴ Vgl. KUNZE, BRITTA (Überwachung 2007), S. 43–44; STORKEY, IAN (Treasuries 2011), S. 2; KAISER, THOMAS (Berücksichtigung 2015), S. 339.

⁵⁵ Vgl. SCHILLINGS, ROBERT (Gefahr 2008), S. 26; MASLEN, MARTIN (Bankensektor 2010), S. 14; ZIEGER, THOMAS (Überblick 2010), S. 17; WOLKE, THOMAS (Risikomanagement 2016), S. 258.

⁵⁶ Vgl. JUDT, EWALD; AIGNER, BARBARA (Glossar 2006), S. 46; PIAZ, JEAN-MARC (Mehrwert 2007), S. 61; MASLEN, MARTIN (Bankensektor 2010), S. 14; ZIEGER, THOMAS (Überblick 2010), S. 17; KÖNIGS, HANS-PETER (System 2013), S. 10; GLASER, CHRISTIAN (Leasing 2015), S. 32.

⁵⁷ Vgl. VIEHMANN, MATTHIAS (Risiko 2006), S. 7–8; VAN DEN BRINK, GERRIT JAN (Messung 2011), S. 114.

⁵⁸ Vgl. GLASER, CHRISTIAN (Aufbau 2011), S. 167; BARTETZKY, PETER (Risiken 2012), S. 71; BUCHMÜLLER, PATRIK; STURM, PHILIPP (Überwachung 2013), S. 449.

⁵⁹ Vgl. SCHILLINGS, ROBERT (Gefahr 2008), S. 26.

⁶⁰ Vgl. WEGMANN, PATRICK (Basel 2005), S. 504; WOLKE, THOMAS (Risikomanagement 2016), S. 259.

⁶¹ Vgl. FRICKE, JENS (Marktrisiken 2006), S. 10.

⁶² Vgl. WEGMANN, PATRICK (Basel 2005), S. 504; FREY, WERNER; WITT, THOMAS (Prüfung 2013), S. 271.

⁶³ Vgl. BÖCKER, ULRICH; GRÖHN, PATRIK (Einführung 2002), S. 376; ANGERMÜLLER, NIELS OLAF (Prüfungspraxis 2004), S. 196; MÜLLER, ALOIS; DEMMEL, ANDRE; KIPP, DANIEL (Bankenaufsicht 2011), S. 53; BAYER, VERENA (Modellierung 2012), S. 1; SLADEK, MARIO HENRY (Risikokategorie 2015), S. 1.

den, dass operationelle Risiken für Kreditinstitute eine zunehmend bedeutendere Rolle spielen.⁶⁴

Gründe hierfür sind u. a. die stetig voranschreitende Globalisierung, der technische Fortschritt und die damit verbundene Automatisierung und Änderung von Prozessen und neue innovative Finanzprodukte, die die Komplexität der Geschäftstätigkeit erhöhen.⁶⁵ Daneben fördern auch die durch die wachsende Rolle der Informationstechnologie entstehenden alternativen Vertriebswege diese Entwicklung.⁶⁶ Mit der Komplexität der Transaktionen gehen auch erhöhte Anforderungen an die Datenqualität einher.⁶⁷ Darüber hinaus steigert das wachsende Geschäftsvolumen bzw. die zunehmende Größe der Institute das operationelle Verlustpotenzial.⁶⁸ Ebenso verhält es sich mit der Tendenz zum Outsourcing aufgrund der starken Abhängigkeit von modernen Informationstechnologien und der damit einhergehenden Dependenz von Dritten.⁶⁹ Des Weiteren ist eine Zunahme von externen Bedrohungen zu beobachten.⁷⁰ Die genannten Gründe sind nach wie vor aktuell.⁷¹ In Kreditinstituten sind deshalb das Interesse und das Bewusstsein für die operationellen Risiken gestiegen.⁷²

⁶⁴ Vgl. DEUTSCHE BUNDESBANK (Risikolage 2004), S. 48; o. V. (Handlung 2016).

⁶⁵ Vgl. JUDT, EWALD; AIGNER, BARBARA (Glossar 2006), S. 46; AUER, MICHAEL (Risikomanagement 2008), S. 13; HAACKERT, MICHAEL (Aufbau 2009); BAYER, VERENA (Modellierung 2012), S. 1.

⁶⁶ Vgl. DAFERNER, MARC; QUICK, MARKUS; VOIT, JOHANNES (Datenpool 2006), S. 197.

⁶⁷ Vgl. o. V. (Herausforderung 2000), S. 88.

⁶⁸ Vgl. JUDT, EWALD; AIGNER, BARBARA (Glossar 2006), S. 46; MÜLLER, ALOIS; DEMMEL, ANDRE; KIPP, DANIEL (Bankenaufsicht 2011), S. 54.

⁶⁹ Vgl. DEUTSCHE BUNDESBANK (Eigenkapitalvereinbarung 2001), S. 28; GRAMLICH, DANIELA; GRAMLICH, STEFAN (Würdigung 2002), S. 66; JUDT, EWALD; AIGNER, BARBARA (Glossar 2006), S. 46; MÜLLER, ALOIS; DEMMEL, ANDRE; KIPP, DANIEL (Bankenaufsicht 2011), S. 54.

⁷⁰ Vgl. FAISST, ULRICH (Steuerung 2003), S. 2.

⁷¹ Vgl. SCHULTE-MATTLER, HERMANN; MATTAL, BENJAMIN (CRR-Risikobereiche 2015).

⁷² Vgl. DRESEL, TANJA; DULDINGER, ANDREAS; ZANTHIER, ULRICH VON (Praxis 2003), S. 468; MEYER, CLAUDIA; HAACKERT, MICHAEL (Management 2008), S. 473; MECHNIK, CHRISTIAN (Outsourcing 2011), S. 164; HORBENKO, NATALIYA (Banken 2012), S. 1.

Einige Autoren bezeichnen sie als die zweitwichtigste Risikoklasse für Kreditinstitute nach den Adressenrisiken.⁷³ Andere sehen die operationellen Risiken einschließlich der Rechtsrisiken als die größte Gefahr innerhalb des Spektrums der bankbetrieblichen Risiken an.⁷⁴ 60 % der Risiken sind direkt oder indirekt auf operationelle Risiken zurückzuführen.⁷⁵ Viele Verluste stammen aus oder werden in erheblichem Maße durch operationelle Risiken verursacht.⁷⁶ KAISER schlussfolgert, dass Non-Financial Risks⁷⁷, die die operationellen Risiken beinhalten, zu größeren Verlusten führen können als Adressen- und Marktpreisrisiken und dass ihre Bedeutung auch in Zukunft einen Anstieg verzeichnen wird.⁷⁸ Dies bestätigt das von der EBA durchgeführte Risk Assessment im Jahre 2015, welches bei 35 % der Teilnehmer erhöhte operationelle Risiken ausweist.⁷⁹ Ergo ist es für Kreditinstitute unabdingbar, sich gezielt mit der Handhabung dieser Risikokategorie zu befassen. Aus diesem Grund werden nachfolgend zunächst die Teilkategorien des operationellen Risikos analysiert und mit Beispielen veranschaulicht.

⁷³ Vgl. DEUTSCHE BUNDESBANK (Eigenkapitalvereinbarung 2001), S. 28; SCHULTE-MATTLER, HERMANN; MANNS, THORSTEN (Meilenstein 2005), S. 544; WOLF, MARTIN (Basel II 2005), S. 7.

⁷⁴ Vgl. BÖHMERT, KARIN (Stresstest 2014), S. 2.

⁷⁵ Vgl. O. V. (Banken 2006).

⁷⁶ Vgl. KAISER, THOMAS; KÖHNE, MARC FELIX (Risiken 2007), S. 37; MASLEN, MARTIN (Bankensektor 2010), S. 14.

⁷⁷ Non-Financial Risks stören den normalen Geschäftsablauf oder entstehen aus einer Veränderung des Geschäftsablaufs heraus. Vgl. KAISER, THOMAS (Management 2015), S. 20.

⁷⁸ Vgl. KAISER, THOMAS (Management 2015), S. 25.

⁷⁹ Vgl. EBA (Risk Assessment 2015), S. 66.

2.3. Definition der verschiedenen Kategorien des operationellen Risikos

2.3.1. Personelle Risiken

Unter personellen Risiken werden alle Risiken verstanden, die aus dem Einsatz oder der Neueinstellung von Mitarbeitern resultieren können.⁸⁰ Diese sind unterteilt in quantitative und qualitative personelle Risiken.⁸¹ Quantitative personelle Risiken umschreiben die Gefahr, die mit der mengenmäßigen Beschaffung oder dem mengenmäßigen Einsatz von Mitarbeitern verbunden ist.⁸² Durch den Ausfall von Mitarbeitern kann bspw. der reibungslose Betrieb einer Filiale gefährdet sein.⁸³ Die Beschaffung von hinreichend qualifiziertem Personal für neuartige Finanzdienstleistungen stellt eine weitere Problematik dar. Es besteht also die Gefahr, nicht in ausreichendem Maße qualifizierte Mitarbeiter zur Verfügung zu haben.⁸⁴ Ein zusätzliches Problem ist der Wissensverlust durch Personalabwanderungen, wenn neu eingestellte Mitarbeiter aufgrund nicht erfüllter Erwartungen oder bereits beschäftigte Mitarbeiter wegen Unzufriedenheit oder Veränderungen privater Natur das Institut verlassen.⁸⁵ Das Wissen ist meist heterogen auf Mitarbeiter verteilt und nicht ausreichend dokumentiert.⁸⁶ Bei unerwünschten Personalfluktuationen scheiden meist besonders gut qualifizierte Mitarbeiter aus, was mit einem Verlust an Spezialwissen einhergeht.⁸⁷

⁸⁰ Vgl. BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 886; BÜSCHGEN, HANS EGON (Bank-Lexikon 2006), S. 729; WINGENDORF, CHRISTIAN (Fremdfinanzierung 2010), S. 138.

⁸¹ Vgl. BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 886; BÜSCHGEN, HANS EGON (Bank-Lexikon 2006), S. 729.

⁸² Vgl. KRÄMER, GREGOR (Ziele 2000), S. 229; BÜSCHGEN, HANS EGON (Bank-Lexikon 2006), S. 729.

⁸³ Vgl. hierzu und zu dem folgenden Satz KRÄMER, GREGOR (Ziele 2000), S. 229–230.

⁸⁴ Vgl. THIES, KARLHEINZ (Prozess-Risiken 2008), S. 17.

⁸⁵ Vgl. WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 41.

⁸⁶ Vgl. HERZMANN, FRANK (Finanzmarktkommunikation 2009), S. 141.

⁸⁷ Vgl. GLASER, CHRISTIAN (Leasing 2015), S. 199.

Qualitative personelle Risiken beziehen sich auf fachliche und charakterliche Eigenschaften der Mitarbeiter.⁸⁸ Fehlende oder unzureichende Qualifikationen, Nachlässigkeit, Pflichtvergessenheit, Arbeitsüberlastung, ungenügende Arbeitsauslastung und private sowie berufliche Probleme können solche Risiken begründen.⁸⁹ Etwa 50 % der Mitarbeiter im Banken- und Versicherungssektor leiden an einem Burnout oder sind akut gefährdet.⁹⁰ Andererseits können auch vorsätzliche Handlungen den Betriebsablauf beeinträchtigen oder auf kriminelle Tätigkeiten abzielen.⁹¹ Qualitative personelle Risiken sind die Folge von unbeabsichtigten, fahrlässigen oder vorsätzlichen Handlungen der Mitarbeiter und lassen sich demnach in die Unterkategorien Fahrlässigkeitsrisiko, Betrugs- und Diebstahlsrisiko sowie Irrtumsrisiko einteilen. Ein bewusstes oder unbewusstes Missachten der Vorschriften und Regeln wird als Fahrlässigkeitsrisiko verstanden, wobei der jeweilige Mitarbeiter bei einem bewussten fahrlässigen Handeln die Schädigung der Bank willentlich in Kauf nimmt.⁹² Solcherlei Verhalten kann eine Vorstufe zum Betrug darstellen. Die Betrugs- und Diebstahlsrisiken, die die Gefahr umschreiben, dass ein Mitarbeiter monetäre oder nicht monetäre Vermögensgegenstände unterschlägt, sind zu jeder Zeit latent vorhanden. Ein Betrug oder Diebstahl wird mit Vorsatz ausgeübt. Der Betrug ist durch den Missbrauch der beruflichen Position zur persönlichen Bereicherung des Betrügers gekenn-

⁸⁸ Vgl. BÜSCHGEN, HANS EGON (Bank-Lexikon 2006), S. 729; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 9.

⁸⁹ Vgl. BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 9–10. Bei Konfrontation mit einer bestimmten Informationsmenge ist es möglich, dass Umwelteinflüsse nur noch eingeschränkt wahrgenommen werden, was zu einem Verlust der Übersicht, der Verdrängung von Ereignissen oder Stress führen kann. Vgl. MINZ, KRISTEN-ANNETTE (Risiken 2004), S. 22.

⁹⁰ Vgl. O. V. (Burnout 2015), S. 77.

⁹¹ Vgl. hierzu und zu dem folgenden Satz BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 9–10.

⁹² Vgl. dazu und zu den nächsten drei Sätzen WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 38–41; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 10–11.

zeichnet,⁹³ was bei Fahrlässigkeits- und Irrtumsrisiken nicht zum Tragen kommt.⁹⁴ Er erfolgt aufgrund eines empfundenen Unrechts, aus einer sich bietenden Gelegenheit oder aus Vorsatz.⁹⁵ Besonders in Umbruchphasen verstärkt sich die Unzufriedenheit der Mitarbeiter, was Betrugsfälle fördern kann.⁹⁶ Letztlich erfolgt das Irrtumsrisiko aus insuffizienter Aufgabenerfüllung nicht willentlich.⁹⁷ Gründe hierfür sind z. B. eine nicht ausreichende Qualifizierung, ein gutgläubiges Handeln der betreffenden Person oder eine arbeitsmäßige Überlastung. Stressbedingt kann die Konzentration der Mitarbeiter nachlassen, was unbeabsichtigte Schäden oder Unfälle fördern kann.⁹⁸ Im Gegensatz zum Fahrlässigkeitsrisiko werden beim Irrtumsrisiko keine internen Richtlinien oder externe Gesetze gebrochen.⁹⁹ Irrtümer beinhalten Eingabefehler, Schreibfehler oder Verwechslungen.¹⁰⁰ Personelle Risiken umfassen auch Schäden, die aus einem schlechten Betriebsklima, aus einem falschen Führungsverständnis und aus fehlender Kommunikation heraus entstehen.¹⁰¹ Speziell in der Finanzbranche sind Betrugsfälle besonders virulent.¹⁰² Dabei ist auffal-

⁹³ Vgl. GLASER, CHRISTIAN (Erfahrungsbericht 2011); HÄNEL, CORINNA (Fraud-Prävention 2016), S. 31.

⁹⁴ Vgl. O. V. (Risiken 1998); WIEDEMANN, ARND; MINZ, KRISTEN-ANNETTE; NIEMEYER, FRITZ (Handlungsfelder 2003), S. 23.

⁹⁵ Vgl. GRIEGER-LANGER, SUZANNE (Prävention 2012), S. 471.

⁹⁶ Vgl. O. V. (Fraud 2010).

⁹⁷ Vgl. hierzu und zu dem nächsten Satz WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 39; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 12.

⁹⁸ Vgl. WENGERT, HOLGER; SCHNITTENHELM, FRANK ANDREAS (Corporate 2013), S. 33.

⁹⁹ Vgl. O. V. (Risiken 1998); WIEDEMANN, ARND; MINZ, KRISTEN-ANNETTE; NIEMEYER, FRITZ (Handlungsfelder 2003), S. 23.

¹⁰⁰ Vgl. SIMON, WERNER (Herausforderung 2002), S. 130.

¹⁰¹ Vgl. WOLKE, THOMAS (Risikomanagement 2016), S. 267.

¹⁰² Vgl. MÜLLER, GIORGIO (Datenkonsortium 2012), S. 56.

lend, dass Unternehmen zum größten Teil von eigenen Mitarbeitern oder Managern geschädigt werden.¹⁰³

Ein Beispiel für den existenzbedrohenden Charakter der operationellen Risiken ist der Fall der Barings Bank.¹⁰⁴ Er stellt einen der bedeutendsten Fälle in der Bankgeschichte dar.¹⁰⁵ Die kriminellen Aktivitäten eines einzigen Mitarbeiters zwangen die Barings Bank 1995 zur Geschäftsaufgabe.¹⁰⁶ Nick Leeson war Händler in Singapur, wo er Arbitragemöglichkeiten zwischen Kursen des Aktienindex Nikkei 225 an den Börsen von Singapur und Osaka ausnutzen sollte.¹⁰⁷ Stattdessen verwendete er die Derivate zu unautorisierten Spekulationen. Durch extrem riskante Geschäfte versuchte er den Gewinn der Bank zu steigern, um dadurch sein Renommee und sein gewinnabhängiges Gehalt zu erhöhen.¹⁰⁸ Daraus entstanden der Bank hohe Gewinne, die nicht das Resultat von risikoarmen Arbitragegeschäften hätten sein können, jedoch erschienen die Abrechnungen und Papiere stets stimmig.¹⁰⁹ So erstellte Leeson fiktive Kunden, in deren Auftrag er vermeintlich die Spekulationen durchführte. Möglich wurde dies durch eine fehlende Trennung der Verantwortungsbereiche, die zur Folge hatte, dass Leeson seine eigenen Abrechnungen anfertigen konnte.¹¹⁰ Lediglich die Gewinne wurden gemeldet, während die Verluste der unautorisierten Geschäfte verschleiert wurden.¹¹¹ LEE-

¹⁰³ Vgl. BUSSMANN, KAI; NESTLER, CLAUDIA; SALVENMOSER, STEFFEN (Wirtschaftskriminalität 2011), S. 62.

¹⁰⁴ Vgl. PEEMÖLLER, FRED; FRIEDRICH, RENATE (Herausforderung 2002), S. 44.

¹⁰⁵ Vgl. UTZ, ERICH RUDOLF (Bedeutung 2002), S. 104.

¹⁰⁶ Vgl. HASELRIEDER, MICHAEL (Alleingang 2005); KETTE, SVEN (Bankenregulierung 2008), S. 23–24; HOSTETTLER, STEPHAN; BENECKE, FELIX (Risikofaktor 2009).

¹⁰⁷ Vgl. dazu und zu dem nächsten Satz HILLENBRAND, TOM (Arbeiterjunge 2005); WETZEL, KATHARINA (Zeit 2013).

¹⁰⁸ Vgl. WENGERT, HOLGER; SCHNITTENHELM, FRANK ANDREAS (Corporate 2013), S. 33.

¹⁰⁹ Vgl. hierzu und zu dem folgenden Satz HILLENBRAND, TOM (Arbeiterjunge 2005).

¹¹⁰ Vgl. KÖRNERT, JAN (Ketteneffekte 1996), S. 613; HILLENBRAND, TOM (Arbeiterjunge 2005); ZIEGER, THOMAS (Bankunternehmen 2010), S. 319.

¹¹¹ Vgl. KÖRNERT, JAN (Bankenkrise 1996), S. 518–519; HILLENBRAND, TOM (Arbeiterjunge 2005).

SON selbst berichtet über seine Vorgesetzten, dass diese seine Geschäfte nicht verstanden und er sich letztlich selbst kontrollierte.¹¹² Hinweise der Revision auf Unstimmigkeiten wurden von der Geschäftsleitung nicht beachtet.¹¹³ 1995 schloss Leeson Spekulationen darüber ab, dass der Nikkei sich in den nächsten Monaten nicht weitgehend verändern würde.¹¹⁴ Ein Erdbeben in der westjapanischen Industriestadt Kobe führte jedoch dazu, dass der Nikkei zusammenbrach. Letztendlich belief sich das Nominalvolumen der Wetten auf Kursbewegungen auf rund 60 Mrd. USD. Der verbleibende Verlust von 1,4 Mrd. USD führte wegen Zahlungsunfähigkeit zur Schließung des Instituts.¹¹⁵ Dieses Beispiel verdeutlicht, dass Betrugs- und Diebstahlrisiken durch das Fehlen oder das Versagen von Kontrollmaßnahmen gefördert werden.¹¹⁶ Eine unangemessene Ablauforganisation, in Form der fehlenden Funktionstrennung, und das Versagen interner Kontrollverfahren ermöglichten erst den Zusammenbruch der Bank.¹¹⁷ Oftmals gibt es bei operationellen Risiken nicht eine einzige eindeutige Ursache, auf die der Verlust zurückzuführen ist, sondern es ist eine Kombination mehrerer Ursachen zu beobachten.¹¹⁸ Insofern existiert

¹¹² Vgl. NICK LEESON, zitiert in EULER, CHRISTIAN (Kultur 2013).

¹¹³ Vgl. ZIEGER, THOMAS (Bankunternehmen 2010), S. 319.

¹¹⁴ Vgl. hierzu und zu den nächsten drei Sätzen o. V. (Wirtschaftskrimi 2002); HEUSINGER, ROBERT VON (Gier 2003); HILLENBRAND, TOM (Arbeiterjunge 2005).

¹¹⁵ Andere Autoren sprechen von Verlusten zwischen 1,3 und 1,6 Mrd. USD. Vgl. VAN DEN BRINK, GERRIT JAN (Risikoaggregation 2008), S. 202; ENRICH, DAVID; COLCHESTER, MAX (Skandalbanker 2013).

¹¹⁶ Vgl. WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 38; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 11. Anpassungen der Kontrollumgebung können die Möglichkeit von Betrugsfällen minimieren. Vgl. VIEHMANN, MATTHIAS (Risiko 2006), S. 9.

¹¹⁷ Vgl. KÖRNERT, JAN (Konsequenzen 1997), S. 442; BEECK, HELMUT; KAISER, THOMAS (Quantifizierung 2000), S. 634; SCHÖNING, STEPHAN; HOFMANN, MATHIAS (Managementaspekte 2002), S. 883–884; FREY, WERNER; WITT, THOMAS (Prüfung 2013), S. 272. Eine genaue Darstellung des Versagens der internen und externen Kontrollen beinhaltet KÖRNERT, JAN (Ketteneffekte 1996), S. 612–616.

¹¹⁸ Vgl. KUNZE, BRITTA (Überwachung 2007), S. 29; GLASER, CHRISTIAN (Leasing 2015), S. 33.

beim operationellen Risiko eine Abgrenzungsproblematik.¹¹⁹ So kann ebenfalls argumentiert werden, dass der Zusammenbruch des Instituts ohne das Erdbeben in Kobe, das den Kurssturz an der Börse in Tokio auslöste, nicht eingetreten wäre.¹²⁰ Das Beispiel Barings trug maßgeblich dazu bei, das Bewusstsein für die operationellen Risiken in der Bankenwelt zu wecken.¹²¹ Ein ähnliches Beispiel ist das des Jérôme Kerviel, der 2008 bei der französischen Großbank Société Générale einen Verlust von 4,9 Mrd. EUR durch Spekulationen herbeiführte.¹²²

Neben den finanziellen Folgen sollte auch ein Augenmerk auf immaterielle Schäden wie mögliche Reputationsverluste gelegt werden.¹²³ In jedem siebten deutschen Unternehmen gab es im Jahr 2015 einen bedeutsamen Betrugs- oder Korruptionsfall.¹²⁴ Personelle Risiken spielen gerade bei Dienstleistungsunternehmen wie Kreditinstituten, bei denen das Personal im Mittelpunkt steht, eine besondere Rolle, da letztlich immer der Mensch die Entscheidungen trifft.¹²⁵ Viele Risiken sind auf ein mögliches Fehlverhalten der Mitarbeiter zurückzuführen.¹²⁶ Auslöser fast jedes Erfolgs oder Misserfolgs ist eine menschliche Leistung oder Fehlleistung.¹²⁷ Der Risikofaktor Mensch steht damit im Zentrum der operationellen Ri-

¹¹⁹ Vgl. WOLKE, THOMAS (Risikomanagement 2016), S. 267.

¹²⁰ Vgl. PEACHEY, ALAN (Finanzdesaster 2002), S. 331.

¹²¹ Vgl. O. V. (Risiken 1998).

¹²² Vgl. BUCHMÜLLER, PATRIK; HAAS, MARCUS (Bankpraxis 2009), S. 38; MÜLLER, GIORGIO (Datenkonsortium 2012), S. 56. Eine ausführliche Darstellung findet sich in JUNGBLUTH, RÜDIGER (Aktienhändler 2008). Eine Schilderung der Ereignisse aus der Sicht von Jérôme Kerviel selbst erfolgt in PAULY, CHRISTOPH (Rad 2010).

¹²³ Vgl. GLASER, CHRISTIAN (Erfahrungsbericht 2011); JACKMUTH, HANS-WILLI; DE LAMBOY, CHRISTIAN; ZAWILLA, PETER (Schlüsselfaktor 2012), S. 4; BUNDESKRIMINALAMT (Wirtschaftskriminalität 2014), S. 5.

¹²⁴ Vgl. O. V. (Bestechungsleistungen 2016), S. 34.

¹²⁵ Vgl. WIEDEMANN, ARND; MINZ, KRISTEN-ANNETTE; NIEMEYER, FRITZ (Handlungsfelder 2003), S. 23; MINZ, KRISTEN-ANNETTE (Risiken 2004), S. 21. Die Ursprungsquelle von PWC ist nicht länger verfügbar.

¹²⁶ Vgl. ROMEIKE, FRANK (Fraud-Kontext 2012), S. 244.

¹²⁷ Vgl. KOBİ, JEAN-MARCEL (Personalrisiken 2015), S. 416.

siken.¹²⁸ Die meisten Unternehmen besitzen kein Bewusstsein für die durch die Nichtbeachtung des personellen Risikos entstehenden Kosten.¹²⁹ Die Gefährdung durch die eigenen Mitarbeiter ist somit ein zentraler Bezugspunkt des operationellen Risikos.¹³⁰ Ein weiterer Punkt sind die Risiken, die aus der Informations- und Kommunikationstechnologie erwachsen können.

2.3.2. *Sachlich-technische Risiken*

Unter den sachlich-technischen Risiken sind alle Gefahren zu verstehen, die aus der Beschaffung und dem Einsatz von Betriebsmitteln wie Grundstücken, Gebäuden, Maschinen und Datenverarbeitungsanlagen entstehen.¹³¹ Es erfolgt auch hier eine Einteilung in quantitative und qualitative sachlich-technische Risiken. Nachteilige Auswirkungen durch eine falsche Dimensionierung der Betriebsmittel werden als quantitative sachlich-technische Risiken bezeichnet. Ein solches Risiko liegt bspw. dann vor, wenn die Datenverarbeitungsanlage nicht die adäquate Größe besitzt und dadurch entweder hohe Fehlfunktionen, ein verfrühter Verschleiß wegen einer Überbeanspruchung des Systems oder eine zu geringe Kapazitätsauslastung eintreten, die hohe Leerkosten mit sich bringt. Eignen sich die eingesetzten Betriebsmittel hingegen nicht für den vorgesehenen Zweck, spricht man von qualitativen sachlich-technischen Risiken. So kann für die zu verrichtende Aufgabe nicht das am besten geeignete System beschafft worden sein. Dahingegen können die eingesetzten Betriebsmittel selbst bei einer bestmöglichen Auslegung auf die zu verrichtende Tätigkeit ausfallen oder fehlerhaft arbeiten.

¹²⁸ Vgl. MINZ, KRISTEN-ANNETTE (Risiken 2004), S. 10–11; FÜHRING, MEIK (Risikomanagement 2006), S. 141; FREY, WERNER; WITT, THOMAS (Prüfung 2013), S. 298.

¹²⁹ Vgl. WOIDE, WOLFGANG (Personalarbeit 2007), S. 74.

¹³⁰ Vgl. dazu und zu dem nächsten Satz KETTE, SVEN (Bankenregulierung 2008), S. 162.

¹³¹ Vgl. hierzu und zu dem restlichen Absatz BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 888–889; KRÄMER, GREGOR (Ziele 2000), S. 230–232; BÜSCHGEN, HANS EGON (Bank-Lexikon 2006), S. 810; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 15.

Der Bankbetrieb ist ohne eine verlässliche und integrierte IT nicht mehr möglich.¹³² Der Geschäftserfolg ist in außerordentlichem Maße an eine sichere IT gebunden.¹³³ Die Informations- und Kommunikationstechnologie durchdringt nicht nur jeden Geschäftsbereich des Instituts, sondern beeinflusst auch deren Geschäftsmodell wesentlich, weswegen sie einen entscheidenden Wettbewerbsfaktor verkörpert.¹³⁴ Mit veralteten Systemen ist keine effektive und fehlerfreie Umsetzung neuer Prozesse möglich.¹³⁵ Operationelle Risiken spielen in Zeiten der erhöhten IT-Abhängigkeit eine entscheidende Rolle.¹³⁶ Daraus resultieren eine wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden.¹³⁷ Kaum eine andere Branche weist eine so große Dependenz von der Sicherheit und Verfügbarkeit der Informationssysteme auf wie der Finanzsektor.¹³⁸ Das Online-Banking, Geldautomaten und Handelsplattformen sind von einer funktionsfähigen IT abhängig.¹³⁹ Institute sind sowohl bei der Kommunikation als auch bei der Bewerksstellung interner Abläufe auf die Technologie angewiesen.¹⁴⁰ Fehler oder Störungen in den Informations-, Abwicklungs- oder Handelssystemen sind oftmals mit schwerwiegenden materiellen und immateriellen Folgen für das Institut verbunden.¹⁴¹ Es liegt ein enormes Risikopotenzial vor.¹⁴² Der größte Teil

¹³² Vgl. O. V. (IT-Sicherheitsgesetz 2014); BRODNIK, BRANIMIR; WENDT, STEFAN (IT-Auslagerung 2015), S. 60.

¹³³ Vgl. GRUDZIEN, WALDEMAR (Regulierungsarbitrage 2016), S. 46.

¹³⁴ Vgl. HIRSCHMANN, STEFAN (Zukunft 2015), S. 26.

¹³⁵ Vgl. KRAUS, ANJA (Terror 2016), S. 42.

¹³⁶ Vgl. DEUTSCHE BUNDESBANK (Risikolage 2004), S. 48; KÜHLWEIN, ANNA-JOY; BURKERT, UWE (Bankanalyse 2015), S. 175.

¹³⁷ Vgl. BSI (Informationssicherheit 2012), S. 10.

¹³⁸ Vgl. LORY, ROLF (IT-Sicherheit 2006).

¹³⁹ Vgl. KÜHLWEIN, ANNA-JOY; BURKERT, UWE (Bankanalyse 2015), S. 175.

¹⁴⁰ Vgl. KUSSIN, MATTHIAS (Regulierung 2009), S. 206.

¹⁴¹ Vgl. MINZ, KRISTEN-ANNETTE (Risiken 2004), S. 19; AMIKA, STEFANIE (IT-Sicherheit 2005), S. 30; WEBER, FELIX (Pflicht 2007).

¹⁴² Vgl. NIEDERMEIER, ROBERT (Datenverarbeitung 2005), S. 19; KAISER, THOMAS (Management 2015), S. 20.

aller Pannen und Ausfälle hinsichtlich der IT eines Instituts geht jedoch auf menschliches Versagen und Unwissenheit zurück.¹⁴³ Bei Datendiebstählen oder Manipulationen befindet sich der Täter meist hinter der Firewall.¹⁴⁴ Hier lässt sich ein Bezug zu den Risiken der IT-Sicherheit herstellen, die eine fehlende oder mangelnde interne und externe Zugangssicherheit der eingesetzten Systeme bezeichnen.¹⁴⁵ In diesem Zusammenhang taucht der Mensch als besonderer Risikofaktor auf.¹⁴⁶ Sicherheitslücken sind in 90 % der Fälle durch menschliches Fehlverhalten verursacht. Es handelt sich um ungewollte Datenverluste oder -preisgaben durch eigene Mitarbeiter, Softwarefehler oder den Verlust bzw. Diebstahl von mobilen Endgeräten.¹⁴⁷ Die Nutzung eigener mobiler Endgeräte stellt eine interne Schwachstelle dar.¹⁴⁸ Die installierten Anwendungen erhöhen die Sicherheitsrisiken für die Unternehmensnetzwerke.¹⁴⁹ Die Hauptbedrohung bezüglich solcher Risiken stammt daher aus dem Inneren des Instituts.¹⁵⁰ Es sollte zudem an Reputationsrisiken gedacht werden, die durch den Ausfall der IT entstehen können.¹⁵¹

Zur Veranschaulichung sollen einige Beispiele genannt werden. Im August 2015 verhinderte ein Softwarefehler bei der Bank of New York Mel-

¹⁴³ Vgl. CRAMER, JÖRG-ENGELBRECHT (Grenzen 1999), S. 1310.

¹⁴⁴ Vgl. RAINER VON ZUR MÜHLEN, zitiert in HARDT, CHRISTOPH (Feind 2002), S. 10.

¹⁴⁵ Vgl. KAMIN, MICHAEL (Implementierung 2007), S. 51.

¹⁴⁶ Vgl. FALK, MICHAEL; HOFMANN, MARC (Kontext 2006), S. 75; KLIPPER, SEBASTIAN (Security 2015), S. 45.

¹⁴⁷ Vgl. zu den letzten beiden Sätzen KREITERLING, CHRISTOPH (Mensch 2015), S. 20–21.

¹⁴⁸ Vgl. LOCHMAIER, LOTHAR (Fleck 2008), S. 72; O. V. (Schatten-IT 2016), S. 45; O. V. (Smartphone 2016), S. 45; WENDT, CARSTEN; HOFFRITZ, FRANK (Bedrohung 2016), S. 72.

¹⁴⁹ Vgl. HIRSCHMANN, STEFAN (Risikosilos 2015). Innerhalb der ersten sechs Monate des Jahres 2016 sind 3 Mio. Geräte über App Stores mit Schadprogrammen wie Spionage-Softwares und SMS-Phishing in Berührung gekommen. Vgl. O. V. (Smartphone 2016), S. 45.

¹⁵⁰ Vgl. LORY, ROLF (Pflichtübung 2006); KOB, TIMO (Informationssicherheit 2012), S. 325.

¹⁵¹ Vgl. ABEL, ANDREAS (Rechenzentren 2013), S. 782.

lon, dass die richtigen Kurse für mehr als 1.000 Fonds eingestellt werden konnten.¹⁵² Bei den Sparkassen wurden im März 2016 alle Zahlungen, die Kunden mit der EC-Karte tätigten, aufgrund eines Fehlers beim Bankendienstleister TeleCash zweimal verarbeitet, weswegen eine doppelte Abbuchung des Betrags erfolgte.¹⁵³ Bei der Deutschen Bank kam es im Juni 2016 zu einem ähnlichen Softwarefehler.¹⁵⁴ Im Online-Banking wurden am Vortag, dem 01.06.2016, von Kunden getätigte Zahlungen erneut abgebucht. Während die Deutsche Bank beteuerte, dass keine tatsächliche Buchung erfolgte und es sich nur um ein Darstellungsproblem handelte, wirkten sich die Transaktionen trotzdem auf den tatsächlichen Kontostand der Kunden aus. Während manche Konten einen höheren Saldo auswiesen, rutschten andere Kunden wegen doppelt abgebuchter Mieten, Versicherungen oder Strom am Monatsanfang in die roten Zahlen. Dadurch waren bargeldlose Zahlungen und eine Bargeldbeschaffung an Terminals in einigen Fällen nicht mehr möglich. Selbst am 06.06.2016, nachdem der Schaden laut der Deutschen Bank behoben worden war, kam es noch zu Schwierigkeiten im Online-Banking.¹⁵⁵ So konnten Lastschriften nur telefonisch zurückgebucht werden. Andere Kunden beschwerten sich unter Nutzung sozialer Medien über konkret entstandene Schäden. Selbst Konzernchef JOHN CYRAN teilte bei seinem Amtsantritt im Juli 2015 mit, dass die Systeme der Bank ineffektiv, veraltet und ineffizient seien.¹⁵⁶ Im Juli 2016 kam es zu einer schwerwiegenden Panne im Online-Banking bei der Commerzbank-Tochter Comdi-

¹⁵² Vgl. STRASBURG, JENNY (Schäden 2015).

¹⁵³ Vgl. o. V. (Abbuchungen 2016); o. V. (Kartenzahlungen 2016); o. V. (Sparkassenkunden 2016).

¹⁵⁴ Vgl. hierzu und zu den nächsten vier Sätzen DOWIDEIT, MARTIN (Buchungspanne 2016); KRAMER, SARAH (Geld 2016); o. V. (Kunden 2016); o. V. (Probleme 2016); o. V. (Software-Panne 2016).

¹⁵⁵ Vgl. dazu und zu den beiden folgenden Sätzen o. V. (IT-Panne 2016).

¹⁵⁶ Vgl. JOHN CYRAN, zitiert in KRAMER, SARAH (Geld 2016); o. V. (Kunden 2016).

rect.¹⁵⁷ Dort hatten Kunden aufgrund eines Systemfehlers nach einem Software-Update nicht Zugriff auf ihre eigenen Daten, sondern auf die Daten und Konten anderer Kunden. Zeitweise war die Homepage der Bank nicht mehr erreichbar.

2.3.3. *Ablaufstrukturelle Risiken*

Die ablaufstrukturellen Risiken lassen sich in interne und externe ablaufstrukturelle Risiken gliedern.¹⁵⁸ Die internen ablaufstrukturellen Risiken resultieren aus der Ablauforganisation eines Instituts und äußern sich in einer mangelnden Geschäftsprozessordnung.¹⁵⁹ Gefahrenpotenzial liegt in einer zu akribischen Definition, jedoch auch in einer fehlerhaften Abstimmung der einzelnen Prozesse. So wohnen einer nicht sachgerechten und ineffizienten Führungsstruktur und Kompetenzzuordnung Risiken inne.¹⁶⁰ Sowohl unklare als auch unzweckmäßig delegierte Anordnungen und Weisungen können in Behinderungen der Arbeitsausführung münden. Arbeitsabläufe können unflexibel sein oder Lücken aufweisen und dadurch Fehlerpotenziale bieten. Das Risiko besteht demnach darin, dass Prozesse nicht in optimaler Weise ablaufen und betrifft ebenso eine mangelnde Information bzw. Kommunikation.¹⁶¹ Weitere Ursachen können in einer unzureichenden Definition der Schnittstellen, unklaren Qualitätsmerkmalen sowie Verfahren oder gravierenden Ablauf- oder Medienbrüchen liegen.¹⁶² Fehlende Kontrollen und mangelnde Sicherheit bzw. Routine in neuen Prozessen treten hinzu.¹⁶³

¹⁵⁷ Vgl. hierzu und zu den nächsten beiden Sätzen KAISER, STEFAN (Panne 2016); RÖDER, JÜRGEN; DOWIDEIT, MARTIN (Kontostände 2016).

¹⁵⁸ Vgl. KRÄMER, GREGOR (Ziele 2000), S. 228.

¹⁵⁹ Vgl. dazu und zu dem folgenden Satz BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 20.

¹⁶⁰ Vgl. hierzu und zu den nächsten beiden Sätzen BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 889.

¹⁶¹ Vgl. KAMIN, MICHAEL (Implementierung 2007), S. 42.

¹⁶² Vgl. THIES, KARLHEINZ (Prozess-Risiken 2008), S. 17.

¹⁶³ Vgl. MINZ, KRISTEN-ANNETTE (Risiken 2004), S. 23.

Gerade Schwächen in der Unternehmensführung und -organisation, in den internen Kontrollen und in der internen sowie externen Überwachung sind in den vergangenen Jahren Auslöser für das Eintreten bedeutender operationeller Verluste gewesen.¹⁶⁴ Bereits behandelt wurden die Beispiele der Barings Bank und der Société Générale, die durch mangelnde Kontrollmechanismen erst ermöglicht wurden.¹⁶⁵ In diese Liste reiht sich der Vorfall der UBS im Jahr 2011 ein, bei der Kweku Adoboli einen Verlust von 2,3 Mrd. USD verursachte.¹⁶⁶ Hierbei ging die Finanzbranche fälschlicherweise davon aus, dass dies nach dem Vorfall der Société Générale Anfang 2008 nicht mehr möglich wäre. Schwache interne Kontrollsysteme waren auch in diesem Fall eine wesentliche Ursache.¹⁶⁷ Hinweise zu gefährlichen Transaktionen wurden nicht weitergegeben und Überschreitungen der Handelslimits blieben ohne Konsequenzen. LEESON sprach von einer Bankrotterklärung des Finanzsystems und davon, dass die Banken aus ihren Fehlern nichts gelernt haben.¹⁶⁸ Auch Adoboli trifft diese Einschätzung über die Bankenwelt.¹⁶⁹ Bei der amerikanischen Bank Citigroup sorgten im Jahr 2015 derweil unentdeckte Transaktionen beinahe zu einem Verlust von 400 Mio. USD.¹⁷⁰ Auch bei der Deutschen Bank wurden im letzten Jahr die Kontrollsysteme bemängelt, was dazu führte, dass sie durch den Stresstest der Fed fiel.¹⁷¹ Bereits zuvor warf die Notenbank dem Institut Nachlässigkeit in der Rechnungslegung und der

¹⁶⁴ Vgl. KUNZE, BRITTA (Überwachung 2007), S. 42.

¹⁶⁵ Vgl. Kapitel 2.3.1.

¹⁶⁶ Vgl. dazu und zu dem folgenden Satz WELP, CORNELIUS; ESTERHÁZY, YVONNE (Versagen 2011). Für genauere Angaben und den weiteren Verlauf dieses Falls vgl. KAISER, TINA (Haftstrafe 2012).

¹⁶⁷ Vgl. hierzu und zu dem nächsten Satz ZULAUF, DANIEL (Leine 2012), S. 3.

¹⁶⁸ Vgl. NICK LEESON, zitiert in BAUMANN, CLAUDE (Banken 2011).

¹⁶⁹ Vgl. O. V. (Finanzindustrie 2015).

¹⁷⁰ Vgl. STRASBURG, JENNY (Citi 2015); STRASBURG, JENNY (Schäden 2015).

¹⁷¹ Vgl. O. V. (Mängel 2015); O. V. (Stresstest 2015). So waren die Bücher der Deutschen Bank zwischen dem 01.10.2008 und dem 31.03.2009 fehlerhaft. Vorwürfe wurden laut, dass während der Finanzkrise Papierverluste in Milliardenhöhe versteckt wurden. Vgl. HENNING, EYK; NISSEN, MADELEINE (Millionenstrafe 2015).

Internen Revision vor.¹⁷² Genauso verhielt es sich beim diesjährigen Stresstest, bei dem die unzureichenden Fortschritte beanstandet wurden.¹⁷³

Die externen ablaufstrukturellen Risiken werden auch als „Reputationsrisiken“ oder „Imagerisiken“ bezeichnet.¹⁷⁴ Die Reputation beschreibt die Wahrnehmung der Interessensgruppen eines Instituts bezüglich dessen Leistungsfähigkeit, Kompetenz, Integrität und Vertrauenswürdigkeit unter Einbeziehung vergangener und zukünftiger Aspekte.¹⁷⁵ Es besteht demnach die Gefahr, dass negative Publizität über das Geschäftsgebaren und die Geschäftsverbindungen einer Bank, ob zutreffend oder nicht, das Vertrauen in die Integrität des Instituts beeinträchtigen.¹⁷⁶ Die Reputation ist im Hinblick auf die vertrauensbasierten Bankgeschäfte von essenzieller Bedeutung.¹⁷⁷ Sie ist deshalb in der Finanzbranche ein zentraler Wettbewerbsfaktor.¹⁷⁸ Dort wird das Reputationsrisiko pauschal als das größte Risiko nach dem wachsenden regulatorischen Druck wahrgenommen, womit ihm eine größere Bedeutung als dem Marktpreis- und Adressenrisiko zuteilwird.¹⁷⁹ Es ist das einflussreichste Risiko im Hinblick auf die

¹⁷² Vgl. o. V. (Mängel 2015).

¹⁷³ Vgl. o. V. (US-Stresstest 2016). Ein Mangel des Kontrollsystems stellt bspw. die Verbreitung von sensiblen Daten per Lautsprecher an Analysten und Händler dar. Zwischen 2008 und 2014 waren jene Daten ebenfalls Unbefugten wie Mitarbeitern aus der Vermögensverwaltung zugänglich. Aufgrund der Verletzung der Vertraulichkeitsbestimmung wurde eine Geldstrafe von 12,5 Mio. USD auferlegt. Vgl. o. V. (USA 2016).

¹⁷⁴ Vgl. BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 20.

¹⁷⁵ Vgl. BARTETZKY, PETER (Risiken 2012), S. 74; HOFMANN, JONATHAN; SCHMOLZ, SANDRA (Controlling 2014), S. 90; SPRENGEL, RAINER (Reputation 2015), S. 41.

¹⁷⁶ Vgl. BCBS (Sorgfaltspflicht 2001), S. 3.

¹⁷⁷ Vgl. BCBS (Bankenaufsicht 1997), S. 22; BCBS (Sorgfaltspflicht 2001), S. 3; EILENBERGER, GUIDO (Bankbetriebswirtschaftslehre 2012), S. 73.

¹⁷⁸ Vgl. GRAMLICH, STEFAN (Risikomanagement 2009), S. 371; GLASER, CHRISTIAN (Leasing 2015), S. 37.

¹⁷⁹ Vgl. ASHER, JESAL u. a. (Expectations 2013), S. 43.

Geschäftsstrategie.¹⁸⁰ Die positive Reputation, die über Jahre aufgebaut wurde, kann innerhalb von wenigen Sekunden durch eine emotionale Reaktion aufgrund eines Vertrauensbruchs zunichte gemacht werden.¹⁸¹ Bereits BENJAMIN FRANKLIN, Gründervater der USA, sagte: „It takes many good deeds to build a good reputation and only one bad one to lose it“.¹⁸² Deswegen muss beachtet werden, dass in dieser Risikokategorie jeder einzelne Mitarbeiter einen Reputationsträger darstellt und dahingehend sensibilisiert werden muss.¹⁸³ Sie sind die Repräsentanten des Instituts nach außen und beeinflussen so die Meinungsbildung der Stakeholder.¹⁸⁴ Reputationsschäden weisen das höchste unkalkulierbare Schadenspotenzial auf.¹⁸⁵ Verlautbarungen von ehemaligen oder aktuellen Mitarbeitern und Wettbewerbern, Gerüchte über eine Pleite oder strafrechtliche Ermittlungen, über aufsichtsbehördliche Maßnahmen oder ein auslaufendes Patent können alle für sich genommen ein Auslöser für ein Reputationsrisiko darstellen, das auch auf andere Unternehmen übergreifen und einen Dominoeffekt auslösen kann. Sie führen zu einer zurückgehenden Kundenbindung und -zufriedenheit, schwieriger Neukundengewinnung, sinkendem Umsatz und höheren Refinanzierungskosten. Eine Beschaffung neuer liquider Mittel kann überdies letztlich nicht mehr möglich sein. Zudem können sie sich auf den Aktienkurs von börsennotierten Instituten auswirken, aber auch intern zu einer niedrigeren Mitarbeiterzufriedenheit, höheren Fluktuation, geringeren Identifikation mit dem Unternehmen und sinkenden Attraktivität für neue potenzielle Mitarbeiter führen.¹⁸⁶ Im Schadensfall können die Reputationsrisiken die

¹⁸⁰ Vgl. DELOITTE (Strategic Risk 2013), S. 9.

¹⁸¹ Vgl. DUTSCHKE, WALTER u. a. (Risikokultur 2012); HIRSCHMANN, STEFAN (Risikokultur 2012).

¹⁸² BENJAMIN FRANKLIN, zitiert in WEIßENSTEINER, CHRISTIAN (Reputation 2014), S. 33.

¹⁸³ Vgl. DUTSCHKE, WALTER u. a. (Risikokultur 2012).

¹⁸⁴ Vgl. BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 20.

¹⁸⁵ Vgl. dazu und zu dem folgenden Satz BUNNENBERG, STEFFEN (Recht 2015), S. 44.

¹⁸⁶ Vgl. zu den letzten drei Sätzen KAISER, THOMAS (Banken 2010), S. 127.

restlichen operationellen Risikobereiche bei weitem übersteigen.¹⁸⁷ Sie schädigen das Vertrauen in das jeweilige Institut.¹⁸⁸ Deswegen sind Reputationsrisiken nicht zu unterschätzen.¹⁸⁹ Der Eintritt von indirekten Schäden wird in zunehmendem Maße unkalkulierbar und schwer beherrschbar.¹⁹⁰ Operationelle Risiken im Allgemeinen ziehen häufig ein großes Medienecho nach sich und führen so zu Reputationsverlusten.¹⁹¹ Hierbei stellen soziale Netzwerke eine Bedrohung aufgrund der beschleunigten Kommunikation und der Verbreitung über mehrere Kanäle dar.¹⁹² Unternehmen erfahren ein größeres Risiko, die Kontrolle darüber zu verlieren, wie sie in der Öffentlichkeit wahrgenommen werden.¹⁹³ Ein unzufriedener Kunde kann in kurzer Zeit tausende Empfänger erreichen, die wiederum durch bestätigende Antworten einen Schneeballeffekt auslösen können.¹⁹⁴ Trotz der schweren Quantifizierbarkeit des Risikopotenzials der Reputationsrisiken kann festgestellt werden, dass es erheblich zugenommen hat.¹⁹⁵

¹⁸⁷ Vgl. UTTINGER, URS; SCHMID, SANDRO; SCHAFFNER, ROLF (Chance 2005), S. 82.

¹⁸⁸ Vgl. SCHMIDT, BODO (Controlling 2009), S. 83; LEUKER, ULRICH (Reputationsrisiken 2013), S. 545.

¹⁸⁹ Vgl. DEUTSCHE BUNDESBANK (Schattenbanksystem 2012), S. 71.

¹⁹⁰ Vgl. BUSSMANN, KAI; NESTLER, CLAUDIA; SALVENMOSER, STEFFEN (Wirtschaftskriminalität 2011), S. 22.

¹⁹¹ Vgl. ZIEGER, THOMAS (Bankunternehmen 2010), S. 323.

¹⁹² Vgl. BUNNENBERG, STEFFEN (Recht 2015), S. 44; KAISER, THOMAS (Management 2015), S. 25.

¹⁹³ Vgl. DELOITTE (Strategic Risk 2013), S. 9.

¹⁹⁴ Vgl. RIEKEBERG, MARCUS (Medien 2011), S. 304. Im Besonderen ist an sogenannte „Shit Storms“ zu denken, bei denen sich durch bestimmte negative Nachrichten erhebliche Anfeindungen und negative Meinungsäußerungen gegenüber dem Unternehmen entwickeln. Vgl. GLASER, CHRISTIAN (Leasing 2015), S. 37.

¹⁹⁵ Vgl. DEUTSCHE BUNDESBANK (Stabilitätslage 2006), S. 58–59.

2.3.4. *Rechtliche Risiken*

Kreditinstitute sind verschiedenen Arten von Rechtsrisiken ausgesetzt.¹⁹⁶ Rechtliche Risiken stellen allgemein Risiken dar, die sich aus einer fehlerhaften rechtlichen Gestaltung von Verträgen, Geschäften oder Transaktionen ergeben.¹⁹⁷ Damit besteht die Gefahr einer negativen Auswirkung auf den Erfolg eines Instituts aufgrund der Veränderung oder Nichtbeachtung rechtlicher Rahmenbedingungen.¹⁹⁸ Hierunter fällt auch die Fehlinterpretation oder Missachtung von rechtlichen Vorschriften durch einzelne Mitarbeiter, Organisationseinheiten oder auch des gesamten Unternehmens.¹⁹⁹ Rechtsrisiken können demnach daraus entstehen, dass sich für Verträge, die dem aktuellen Rechtsrahmen entsprechend abgefasst sind, jener Rechtsrahmen verändert.²⁰⁰ Gründe hierfür liegen in der Neufassung gesetzlicher Vorschriften oder Änderung der Rechtsprechung. Falsche Annahmen, schlecht gewählte Formulierungen oder das Übersehen kritischer Stellen in Verträgen können sich als weitere Ausgangspunkte von Rechtsrisiken erweisen.²⁰¹ So kann auch bei einem unveränderten Rechtsrahmen eine fehlerhafte Formulierung der vertraglichen Vereinbarung eine weitere Quelle von rechtlichen Risiken darstellen.²⁰² Ferner können wesentliche Vertragsbestandteile fehlen oder missverständlich formuliert sein, wodurch eine Durchsetzbarkeit der Verträge

¹⁹⁶ Vgl. BCBS (Bankenaufsicht 1997), S. 21. Die Begriffe „Rechtsrisiken“ und „rechtliche Risiken“ werden synonym verwendet.

¹⁹⁷ Vgl. BÜSCHGEN, HANS EGON (Bank-Lexikon 2006), S. 774.

¹⁹⁸ Vgl. BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 22.

¹⁹⁹ Vgl. BARTETZKY, PETER (Risiken 2012), S. 71; GLASER, CHRISTIAN (Leasing 2015), S. 34.

²⁰⁰ Vgl. dazu und zu dem nächsten Satz BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 890; VAN DEN BRINK, GERRIT JAN (Anforderungen 2007), S. 132; AUER, MICHAEL (Risikomanagement 2008), S. 24.

²⁰¹ Vgl. SIMON, WERNER (Herausforderung 2002), S. 132; ROMEIKE, FRANK (Lexikon 2004), S. 99.

²⁰² Vgl. dazu und zu den beiden folgenden Sätzen BÜSCHGEN, HANS EGON (Bankmanagement 1998), S. 891.

unmöglich werden kann. Eine zusätzliche Folge können Schadensersatzzahlungen und Kosten aus Rechtsstreitigkeiten darstellen. Darunter fallen auch Strafzahlungen aus aufsichtsrechtlichen Maßnahmen.²⁰³ Die Rechtsrisiken werden von der EBA als Bedrohungen mit einem hohen Risikolevel gesehen.²⁰⁴ Seit jeher sind rechtliche Risiken aus gerichtlichen oder außergerichtlichen Auseinandersetzungen ein inhärentes Risiko im bankgeschäftlichen Handeln.²⁰⁵ Zum Teil werden diese ganz bewusst im Zuge von kompetitiven Strategien zur Gewinnung neuer Kunden oder Geschäftsfelder eingeplant. Es ist ein erheblicher Anstieg an gerichtlichen und außergerichtlichen Auseinandersetzungen zu beobachten, die auf den gleichen Phänomenen beruhen, die auch für den generellen Anstieg der operationellen Risiken im Ganzen verantwortlich sind. Die Internationalisierung lässt die Frage des anwendbaren Rechts bei grenzüberschreitenden Tätigkeiten aufkommen. Banken, die im angelsächsischen Raum tätig sind, werden wegen des Rechtsinstituts des Strafschadens²⁰⁶ hohen Schadensersatzforderungen ausgesetzt. Auch die Komplexität der Produkte fördert die Gefahren aus rechtlichen Konflikten. Dazu treten die Stärkung des Verbraucher- und Anlegerschutzes in der Gesetzgebung und die zunehmende Digitalisierung, die neue potenzielle Rechtsrisiken, bspw. verursacht durch Hackerangriffe auf Kundenendgeräte, mit sich bringen.

Rechtsstreitigkeiten stellen in zunehmendem Maße eine dauerhafte Belastung für Kreditinstitute dar, was vor allem durch das Aufarbeiten von

²⁰³ Vgl. BITZ, MICHAEL; MATZKE, DIRK (Entwicklungslinien 2011), S. 351.

²⁰⁴ Vgl. EBA (Annual Report 2016), S. 51; EBA (Dashboard 2016), S. 4.

²⁰⁵ Vgl. hierzu und zu dem restlichen Abschnitt DEUTSCHE BUNDESBANK (Stabilitätslage 2006), S. 58.

²⁰⁶ Der Strafschadensersatz dient primär der Abschreckung und der Bestrafung. Es erfolgt eine Erhöhung des tatsächlich entstandenen Schadens um ein Mehrfaches. Vgl. DREIER, THOMAS (Kompensation 2002), S. 185.

Verfehlungen vor der Finanzkrise verstärkt wird.²⁰⁷ Die Strafzahlungen seit der Finanzkrise belaufen sich in Amerika und Westeuropa auf etwa 260 Mrd. USD.²⁰⁸ In den vergangenen Jahren sind sowohl die Anzahl und das Ausmaß der Risiken in Zusammenhang mit Fehlverhalten als auch die Anzahl und der Umfang der verhängten Sanktionen angestiegen.²⁰⁹ Derzeit sind insgesamt lediglich etwa zwei Drittel der offenen Rechtsstreitigkeiten beigelegt worden, weswegen gegenwärtig noch ein signifikantes Risiko- und Kostenpotenzial besteht. Auch für das Jahr 2016 rechnen die Institute mit ansteigenden Belastungen durch Strafzahlungen.²¹⁰ In einigen Fällen übersteigen die Verluste und Rückstellungen für rechtliche Risiken bereits die Abschreibungsbeträge für die Adressenrisiken.²¹¹ Ein Rekordverlust erfuhr die Bank of America, die 2014 16,65 Mrd. USD zahlen musste.²¹² Bei der Deutschen Bank lagen im Jahr 2015 etwa 7.000 Rechtsstreitigkeiten vor.²¹³ Sie hat in den vergangenen Jahren bei fast jedem größeren Finanzskandal zum Kreis der Verdächtigen gezählt.²¹⁴ Damit ergaben sich in den letzten Jahren für das Institut Rechtskosten von mehr als 12 Mrd. EUR, die die Gewinne in diesen Jahren aufgezehrt haben.²¹⁵ Anlage 1 gibt diesbezüglich einen Überblick über einige der zahlreichen Rechtsstreitigkeiten. Nachdem zuvor eine Sonderprüfung von der Bank verweigert wurde, erfolgte außergerichtlich nun doch eine Zu-

²⁰⁷ Vgl. HIRSCHMANN, STEFAN (Rechtsfalle 2015), S. 11; KASPROWICZ, THILO; KAISER, THOMAS (Fokus 2015), S. 5; O. V. (Systemrisiko 2015), S. 42; KÄFER, DOMINIK (Finanzkriminalität 2016), S. 44.

²⁰⁸ Vgl. FISCHER, BENJAMIN (Finanzkrise 2016).

²⁰⁹ Vgl. dazu und zu dem folgenden Satz KÄFER, DOMINIK (Finanzkriminalität 2016), S. 45.

²¹⁰ Vgl. O. V. (Systemrisiko 2015), S. 42.

²¹¹ Vgl. KAISER, THOMAS (Management 2015), S. 20.

²¹² Vgl. O. V. (Handlung 2016). HIRSCHMANN spricht hierbei von insgesamt etwa 22,4 Mrd. EUR. Vgl. HIRSCHMANN, STEFAN (Rechtsfalle 2015), S. 11.

²¹³ Vgl. HIRSCHMANN, STEFAN (Rechtsfalle 2015), S. 11.

²¹⁴ Vgl. KUNZ, ANNE; SEIBEL, KARSTEN (Deutsche Bank 2016).

²¹⁵ Vgl. COMFORT, NICHOLAS; CHOUDHURY, AMBEREEN (Rechtskosten 2016); O. V. (Sonderprüfung 2016).

stimmung, nachdem die DSW vor Gericht zog.²¹⁶ Im Zuge dessen soll überprüft werden, ob die Risikokontrollsysteme der Bank ausreichend und streng genug sind. Zudem wird geprüft, ob die Rückstellungen des Instituts für die laufenden Rechtsverfahren und drohenden Vergleichszahlungen ausreichen. Am Beispiel der Deutschen Bank zeigen sich ebenfalls die hohen Reputationsrisiken, die als Folge solcher Rechtsrisiken entstehen können.²¹⁷

2.3.5. Externe Ereignisrisiken

Die externen Ereignisrisiken beinhalten die natürlichen und die künstlichen Katastrophenrisiken. Während die natürlichen Katastrophenrisiken auf Naturkatastrophen wie Bränden, Blitzeinschlägen, Erdbeben, Stürmen, Sturzfluten oder Überschwemmungen beruhen, bezeichnen künstliche Katastrophenrisiken insb. Banküberfälle, Geiselnahmen, Brandstiftungen oder Terroranschläge, die von Dritten bewusst herbeigeführt werden. Meist muss davon ausgegangen werden, dass der Eintritt einer Naturkatastrophe dazu führt, dass der Geschäftsbetrieb eingestellt werden muss oder zumindest stark beeinträchtigt wird. Es zeigen sich erneut die Interdependenzen der einzelnen Risikokategorien, da ein künstliches Katastrophenrisiko ein quantitatives personelles Risiko mit sich bringen kann, wenn Mitarbeiter aufgrund der psychischen Belastung von Banküberfällen oder Geiselnahmen ausfallen respektive im Zuge einer Brandstiftung oder eines Terroranschlags den Tod finden oder physisch und psychisch beeinträchtigt werden. Diese Risikoklasse ist von der Bank nicht direkt beeinflussbar. Mögliche Vorsorgemaßnahmen sind die Wahl des Standortes, die Installation von Alarmanlagen, der Einsatz von

²¹⁶ Vgl. dazu und zu den beiden folgenden Sätzen O. V. (Sonderprüfung 2015); BARTZ, TIM (Sonderprüfung 2016); KUNZ, ANNE; SEIBEL, KARSTEN (Deutsche Bank 2016); O. V. (Aktionärsvereinigung 2016); O. V. (Rückstellungen 2016).

²¹⁷ Vgl. HOFMANN, JONATHAN; SCHMOLZ, SANDRA (Controlling 2014), S. 93–94.

Wachpersonal und die Einrichtung von Sicherheitsschleusen.²¹⁸ Katastrophenrisiken sind nicht vorhersehbar, weswegen die Ausarbeitung eines Notfallplans keine Garantie für die Funktionsfähigkeit des Instituts darstellt, jedoch die notwendige Handlungsfähigkeit in solchen Extremsituationen gewährleisten kann.²¹⁹ Die Anzahl und Stärke von Naturkatastrophen sind laut Rückversicherungsunternehmen in den letzten Jahren angestiegen.²²⁰

Ein Beispiel für ein natürliches Katastrophenrisiko ist das der Sparkasse Passau, bei der aufgrund eines Elbe-Hochwassers im Jahr 2016 das EDV-System beschädigt wurde, weswegen Selbstbedienungsautomaten jener Sparkasse kein Geld mehr auszahlen konnten.²²¹ Demgegenüber stellt der 11. September 2001 ein dramatisches Beispiel für ein künstliches Katastrophenrisiko dar, das die Bedeutung der operationellen Risiken eindrücklich verdeutlicht.²²² Zwei Flugzeuge trafen die Twin Tower des World Trade Centers in New York City, während gleichzeitig ein weiteres das Pentagon traf und ein viertes in Pennsylvania abstürzte.²²³ Mit diesem Angriff wurde das gesamte Finanzsystem der Welt getroffen.²²⁴ Dabei hatten die Institute sich gegenseitig mit Liquidität ausgeholfen. Zahlreiche New Yorker Institute waren nach dem 11. September zunächst handlungsunfähig.²²⁵ Die Abrechnungskapazitäten der Bank of New York

²¹⁸ Vgl. zu dem bisherigen Absatz WASCHBUSCH, GERD; LESCH, STEFANIE (Schlüssel 2004), S. 46–47; BIEG, HARTMUT; KRÄMER, GREGOR; WASCHBUSCH, GERD (Bankenaufsicht 2011), S. 26.

²¹⁹ Vgl. WITZANI, ANDREAS (Kapitalanlagegesellschaft 2007), S. 93.

²²⁰ Vgl. WENGERT, HOLGER; SCHNITTENHELM, FRANK ANDREAS (Corporate 2013), S. 34.

²²¹ Vgl. o. V. (Hochwasser 2016).

²²² Vgl. OECD (Government 2005), S. 76.

²²³ Vgl. OECD (Terrorism 2005), S. 9. Für eine ausführliche Betrachtung der Ereignisse im Laufe des 11. Septembers 2001 vgl. ABKOWITZ, MARK (Response 2008), S. 126–147.

²²⁴ Vgl. dazu und zu dem nächsten Satz o. V. (Finanzsystem 2001); WITTKOWSKI, BERND (Schurken 2001), S. 17.

²²⁵ Vgl. hierzu und zu den nächsten drei Sätzen MAISCH, MICHAEL u. a. (Terror 2003), S. 25; o. V. (Terroranschläge 2003).

waren ausgefallen, weswegen bspw. die Deutsche Bank mit ihren Ersatzsystemen in New Jersey einen großen Teil des Clearingverkehrs übernommen hatte. Über Tage hinweg standen Kreditlinien offen, die aufgrund der Systemausfälle nur auf mündlichen Zusagen beruhten. Damit sich ein solcher Vorfall nicht wiederholen kann, muss seither jedes Institut über einen Ausweichstandort verfügen, der mindestens 300 Meilen entfernt liegt. Während des Anschlags wurden zudem wichtige Akten zerstört.²²⁶ Mehr als 50 % der Unternehmen, die im World Trade Center eingemietet waren, haben in der Folgezeit Insolvenz angemeldet.²²⁷

Betrugsfälle werden nicht nur von eigenen Mitarbeitern verübt, sondern auch von Dritten, die bspw. durch Hackerangriffe unbefugt einen Zugriff auf das System des Instituts erlangen.²²⁸ Die Computer- und Internetkriminalität gewinnen durch die zunehmende Digitalisierung und Vernetzung an Bedeutung.²²⁹ Cyberrisiken werden als die bedeutendsten Zukunftsrisiken angesehen.²³⁰ Ihre Anzahl und Komplexität nehmen weltweit zu, da der Professionalitätsgrad der Angreifer steigt.²³¹ Des Weiteren sind Cyberangriffe kaum mehr zu erkennen und schwer abzuwehren.²³² Die Angreifer nutzen neue Schwachstellen immer schneller und mit im-

²²⁶ Vgl. KULS, NORBERT (Terroranschlag 2001), S. 18.

²²⁷ Vgl. ROSENKRANZ, FRIEDRICH; MISSLER-BEHR, MAGDALENA (Unternehmensrisiken 2005), S. 3.

²²⁸ Vgl. GLASER, CHRISTIAN (Erfahrungsbericht 2011).

²²⁹ Vgl. MASLEN, MARTIN (Bankensektor 2010), S. 47; HIRSCHMANN, STEFAN (IT-Risikomanagement 2015).

²³⁰ Vgl. HIRSCHMANN, STEFAN (OpRisk-Forum 2016). Es erfolgt eine Einteilung der Cyberrisiken wie Hackerangriffe in das externe Ereignisrisiko, da das Täterprofil eines externen Dritten vorliegt und das Institut zumeist keinen Einfluss auf den Eintritt oder Umfang eines Hackerangriffs hat. Jedoch wurde bereits mehrfach festgestellt, dass die Teilkategorien des operationellen Risikos sich gegenseitig beeinflussen. So können veraltete Systeme bzw. Sicherheitsvorkehrungen oder menschliche Fehler einen Hackerangriff erleichtern oder erst ermöglichen, wie der folgende Abschnitt zeigt.

²³¹ Vgl. OICV-IOSCO; WFE (Cyber-crime 2013), S. 22; BAFIN (Jahresbericht 2015), S. 106; EBA (Risk Assessment 2015), S. 66.

²³² Vgl. o. V. (Cyber-Angriffe 2015), S. 55.

mer ausgereifteren Methoden aus.²³³ Heutzutage ist fast jedes System über das Internet zu erreichen, was zu einer größeren Verwundbarkeit führt.²³⁴ Die Cyberrisiken sind laut BaFin-Präsident FELIX HUFELD auf einem alarmierend hohen Niveau und werden auch in Zukunft zunehmen.²³⁵ IBEL sagt diesbezüglich, dass bisher noch kein Vorfall eingetreten ist, der ein großes Kreditinstitut lahmgelegt hat, es aber vermutlich irgendwann in Zukunft dazu kommen wird.²³⁶ Schätzungen gehen von Kosten i. H. v. 2,1 Bio. USD aus, die bis zum Jahr 2019 durch Cyberkriminalität entstehen werden.²³⁷ Cyberrisiken haben nicht nur Einfluss auf die Geschäftsentwicklung, sondern auch auf die Reputation.²³⁸ Sie werden durch Schwächen in den institutsinternen Prozessen, den Systemen oder durch Fehler von Mitarbeitern gefördert.²³⁹ Wie bereits im Hinblick auf die sachlich-technischen Risiken angesprochen ist der Mitarbeiter hier eine große Gefahrenquelle, da bei Cyberangriffen oftmals weniger die IT-Systeme, sondern die Nutzer die Sicherheitslücke darstellen.²⁴⁰ Einige Hauptursachen für Verlustfälle sind Unachtsamkeit und Fehlverhalten von Mitarbeitern, Sabotage, Phishing²⁴¹ oder Social Engineering²⁴². Das Bewusstsein für die Schwachstelle Mensch, die durch die

²³³ Vgl. ABENTHUM-FEIL, SABINE (Betrugsprävention 2014); HIRSCHMANN, STEFAN (IT-Risikomanagement 2015); BAFIN (Jahresbericht 2016), S. 42.

²³⁴ Vgl. BAFIN (Jahresbericht 2016), S. 42.

²³⁵ Vgl. FELIX HUFELD, zitiert in NISSEN, MADELEINE (Cyber-Risiko 2015).

²³⁶ Vgl. KORBINIAN IBEL, zitiert in O. V. (Aufseher 2015).

²³⁷ Vgl. O. V. (Kosten 2015), S. 54.

²³⁸ Vgl. FLICKE, FLORIAN (Cyberkriminalität 2015), S. 42.

²³⁹ Vgl. SCHÄL, INGO (Risiken 2011), S. 125.

²⁴⁰ Vgl. hierzu und zu den nächsten beiden Sätzen WENDT, CARSTEN; HOFFRITZ, FRANK (Bedrohung 2016), S. 72.

²⁴¹ Beim Phishing erhält das Opfer ein offiziell wirkendes Schreiben, das dazu verleiten soll, vertrauliche Informationen wie Benutzernamen, Passwörter oder PINs preiszugeben. Vgl. LORY, ROLF (IT-Sicherheit 2006).

²⁴² Social Engineering bezeichnet das Ausspähen von Daten durch direkten manipulativen Kontakt zu Informationsträgern. Es wird ein psychologisches Beziehungsverhältnis konstruiert, mit dessen Hilfe das Opfer unwissend sicherheitskritische Informationen preisgibt. Vgl. BÉDÉ, AXEL (Engineering 2012), S. 73.

Unkenntnis oder das Ignorieren von Vorschriften möglichen Angreifern die Türen öffnet, fehlt in einigen Banken. Durch Informationen aus sozialen Netzwerken können personalisierte E-Mails erstellt werden, die Malware enthalten.²⁴³ Trotz des Wissens über die Gefahr unbekannter Anhänge werden diese trotzdem oftmals geöffnet. Manchmal wird damit nicht einmal ein Risiko assoziiert. Eine steigende Anzahl von Mitarbeitern gibt Angreifern unbewusst wertvolle Informationen preis, wobei Banken eine Sonderstellung einnehmen, da sie enorme Mengen an Geld und sensiblen Daten sichern.²⁴⁴ Kreditinstitute sind deshalb begehrte Ziele von Cyberangriffen.²⁴⁵ Fast jedes dritte Unternehmen in Deutschland, darunter auch Kreditinstitute wurde in den vergangenen Jahren Opfer eines Cyberangriffs.²⁴⁶ So wurde J. P. Morgan im Jahr 2014 Opfer eines Hackerangriffs, der den Angreifern über einen mit Malware infizierten Computer eines Mitarbeiters, einen umfangreichen Zugang zu den Systemen ermöglicht hatte.²⁴⁷ Laut deren Pressesprecherin werden Unternehmen ihrer Größe fast täglich Opfer von Cyberangriffen.

²⁴³ Vgl. hierzu und zu den nächsten beiden Sätzen O. V. (Arbeitsplatz 2015), S. 63.

²⁴⁴ Vgl. SIDL, ROBIN (Cyberrisiken 2015). Zu den Angriffszielen in Kreditinstituten vgl. HELD, MARKUS (Aktivitäten 2015), S. 14–16.

²⁴⁵ Vgl. HIRSCHMANN, STEFAN (IT-Risikomanagement 2015).

²⁴⁶ Vgl. HELD, MARKUS (Aktivitäten 2015), S. 13.

²⁴⁷ Vgl. hierzu und zu dem nächsten Satz O. V. (Hackerangriff 2014).

Die Steuerung operationeller Risiken in Kreditinstituten

Eine kritische Analyse des neuen Standardansatzes

Kiszka, S.

2018, XXIV, 235 S. 12 Abb., Softcover

ISBN: 978-3-658-20216-3