JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL C. SCHWICKERT

Falk, Michael; Hofmann, Marc

Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 6 / 2006
ISSN 1613-6667

Arbeitspapiere WI Nr. 6 / 2006

Autoren: Falk, Michael; Hofmann, Marc

Titel: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben

Zitation: Falk, Michael; Hofmann, Marc: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, in: Arbeitspapiere WI, Nr. 6/2006, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2006, 103 Seiten, ISSN 1613-6667.

Kurzfassung: Die gestiegene Bedeutung sowie die zunehmende Abhängigkeit der Unternehmen von der Informationstechnologie bergen ein erhöhtes Gefährdungspotenzial in sich, dem die Unternehmen im Rahmen des Risikomanagements und IT-Sicherheitsmanagements entgegentreten. Die Bemühungen zur Reduktion der Gefährdungen werden flankiert von der Aufgabe, wachsende regulatorische Anforderungen zu erfüllen. Operationelle Risiken sind im Bankensektor durch die Baseler Eigenkapitalverordnung verstärkt in den Blickpunkt der Diskussion geraten. IT-Risiken als wesentliches Teilgebiet operationeller Risiken gewinnen deshalb weiter an Bedeutung. In der unternehmerischen Praxis sind die Bereiche IT-Risikomanagement und IT-Sicherheitsmanagement oft in Organisation, Verantwortung und Methodik getrennt voneinander angesiedelt. Die Entwicklung eines methodisch integrierten Risikomanagements in der Abkehr von dezentralisierten Verantwortlichkeiten erscheint deshalb zweckmäßig. Die vorliegende Arbeit untersucht die beiden Bereiche IT-Sicherheitsmanagement und IT-Risikomanagement und identifiziert Schnittmengen, die die Basis für eine integrierte Gesamtsicht auf die beiden Aufgabengebiete sind. Zusammenfassend wird das Effizienzpotenzial aus der integrierten Betrachtungsweise dargestellt und Empfehlungen für eine angemessene Ausgestaltung eines ganzheitlichen IT-Risikomanagements gegeben.

Schlüsselwörter: IT-Sicherheit, Risikomanagement, Risk Management, Compliance, Basel II, Sarbanes-Oxley Act, SOX, MaRisk, ISO 17799, BS 7799, KonTraG, integrierte Betrachtungsweise, Integrationspotenzial, bankaufsichtsrechtliche Vorgaben

Inhaltsverzeichnis

Abkürzungsverzeichnis

AktG ..... Aktiengesetz

AMA..... Advanced Measurement Approach

AT..... Allgemeiner Teil (der MaRisk)

BaFin ..... Bundesanstalt für Finanzdienstleistungsaufsicht

BDSG ..... Bundesdatenschutzgesetz

BITKOM ..... Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

BS ..... British Standard

BT..... Besonderer Teil (der MaRisk)

BSI..... Bundesamt für Sicherheit in der Informationstechnik

CCSC..... Commercial Computer Security Centre

CEO ..... Chief Executive Officer

CFO ..... Chief Financial Officer

CRD..... Capital Requirements Directive

CSO ..... Chief Security Officer

DaKOR ..... Datenkonsortium zu operationellem Risiko

DTI ..... (British) Department of Trade and Industry

DFÜ ..... Datenfernübertragung

EDV ..... Elektronische Datenverarbeitung

GOLD ..... Global Operational Loss Database

HGB..... Handelsgesetzbuch

IDW ..... Institut der Wirtschaftsprüfer

IS..... International Standard

ISMS..... Informationssicherheits-Managementsystem

ISO..... International Organization for Standardization

IT ..... (1) Informationstechnologie

IT ..... (2) Informationstechnik

IKS..... Internes Kontrollsystem

IV ..... Informationsverarbeitung

KonTraG..... Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

KWG..... Gesetz über das Kreditwesen

MaRisk ..... Mindestanforderungen an das Risikomanagement

NCC..... National Computing Centre

ORM ..... Operationelles Risikomanagement

ORX..... Operational RiskData eXchange Association

PDCA ..... Plan – Do – Check - Act

PS..... Prüfungsstandard

Rn ..... Randnummer

SEC..... Security and Exchange Commission

SOA ..... Sarbanes-Oxley Act (1)

SolvV ..... Solvabilitätsverordnung

SOX ..... Sarbanes-Oxley Act (2)

TR ..... Technical Report

VPN ..... Virtual Private Network

WpHG..... Wertpapierhandelsgesetz

ZSI ..... Zentralstelle für Sicherheit in der Informationstechnik

1 Problemstellung, Ziel und Aufbau

Die gestiegene Bedeutung sowie die zunehmende Abhängigkeit der Unternehmen von der Informationstechnologie bergen ein erhöhtes Gefährdungspotenzial in sich, dem die Unternehmen im Rahmen des Risikomanagements und IT-Sicherheitsmanagements entgegentreten. Wachsende Komplexität der IT-Systeme, verstärkte Durchdringung der Geschäftsprozesse mit Informationstechnologie, die sich einer Vollautomation annähert, und nicht zuletzt die zunehmende Öffnung von Unternehmensnetzwerken steigern die Bedeutung der Informationsverarbeitung im Unternehmensbereich.[1]

Die Bemühungen zur Reduktion der Gefährdungen werden flankiert von der Aufgabe, wachsende regulatorische Anforderungen zu erfüllen. Die sog. operationellen Risiken sind durch die Baseler Eigenkapitalvereinbarung (auch kurz Basel II genannt) verstärkt in den Blickpunkt der Diskussion gerückt. IT-Risiken als wesentliches Teilgebiet operationeller Risiken gewinnen deshalb weiter an Bedeutung.[2] Gerade dieser Bereich wird in der Regulation aber meist eher undifferenziert betrachtet.

Das Management operationeller Risiken gilt als relativ jung. Die Methoden und die Implementierung eines Operational Risk Management ist im Bankenbereich deshalb wenig fortgeschritten. Insbesondere fehlen Risikomodelle zur Bewertung und Steuerung operationeller Risiken.[3]

In der unternehmerischen Praxis sind die Bereiche IT-Risikomanagement und IT-Sicherheitsmanagement oft in Organisation, Verantwortung und Methodik getrennt voneinander angesiedelt.[4] Ein methodisches Risikomanagement in Abkehr von dezentralisierten Verantwortlichkeiten in verschiedenen Abteilungen wird in der Literatur schon

---

1 Vgl. Rauschen, Thomas; Disterer, Georg: Identifikation und Analyse von Risiken im IT-Bereich, in: HMD: Praxis der Wirtschaftsinformatik, Bd. 236, Hrsg.: Mörike, Michael, Heidelberg: dpunkt 2004, S. 19.

2 Vgl. Hirschmann, Stefan; Romeike, Frank: IT-Sicherheit als Rating-Faktor, in: RATINGaktuell, 01/2004, S. 13.

3 Vgl. Romeike, Frank: Banken unterschätzen operationelle Risiken, Online im Internet: http://www.risknet.de/RiskNET_News.29.0.html?&tx_ttnews[backPid]=1&tx_ttnews[tt_news]=328&cHash=ff9b0f2a8a&type=123, 25.06.2006.

4 Die funktionalen Commitees der Deutschen Bank Gruppe trennen bspw. die Bereiche „IT & Operations“ und „Risk“. Vgl. Deutsche Bank Gruppe (Hrsg.): Investor Relations – Konzerninformationen - Organisationsstruktur, Online im Internet: http://www.deutsche-bank.de/ir/494.shtml, 25.06.2006.

länger diskutiert und erscheint zweckmäßig.[5] Da aufsichtsrechtliche Vorgaben die Bereiche IT-Sicherheitsmanagement und IT-Risikomanagement teilweise sehr undifferenziert gemeinsam behandeln und das IT-Sicherheitsmanagement von der Methodik her gesehen eine große Schnittmenge mit dem Management operationeller Risiken aufweist, erscheint es sinnvoll, beide Bereiche zu integrieren. Nur eine ganzheitliche Betrachtung aller Facetten der Bereiche IT-Sicherheit, IT-Projektmanagement und nicht zuletzt der Risiken, die im IT-Bereich vom Faktor „Mensch" ausgehen, ermöglicht eine aussagekräftige Analyse der Risikosituation und kann damit einen Beitrag zur Sicherung und Steigerung des Unternehmenswertes leisten.[6]

IT-Systeme müssen im Zusammenhang mit dem Schlagwort *Compliance*[7] in einer Doppelrolle untersucht werden: Zum einen sind sie unterstützend in einer Vielzahl von Geschäftsprozessen integriert und stellen damit einen Teil der operationellen Risiken eines Unternehmens dar (Systemausfall, Datenmanipulation, Fehlfunktionen). Zum anderen ist die IT ein wesentliches Instrument zur Gewinnung von Rating- und Risikoinformationen im Rahmen der gesetzlich vorgeschriebenen Risikofrüherkennungssysteme und in den Ratingverfahren der Banken.[8]

Die vorliegende Arbeit setzt sich deshalb zum Ziel, zunächst die bankregulatorischen Vorgaben hinsichtlich ihrer Relevanz für die IT-Sicherheit zu untersuchen, im zweiten Schritt ein Modell eines idealtypischen Risikomangements darzustellen und in der Folge ein Rahmenwerk für die Integration beider Bereiche zu entwickeln. Schnittmengen zwischen dem IT-Sicherheitsmanagement und dem Risikomanagement sollen identifiziert werden und daraus Handlungsempfehlungen und Strategien für eine übergreifende Gesamtsicht auf die beiden Aufgabenbereiche abgeleitet werden.

---

5 Vgl. Schaumüller-Bichl, Ingrid: Sicherheitsmanagement: Risikobewältigung in informationstechnologischen Systemen, Mannheim; Leipzig; Wien; Zürich: BI-Wissenschaftsverlag 1992, S. 34.

6 Vgl. Romeike, Frank: IT-Security-Ping-Pong – IT-Risk-Management muss ganzheitlich betrachtet werden, in: Risknews, 3/2004, S. 17.

7 Der Begriff „Compliance" bezeichnet allgemein die Erfüllung von Gesetzen und Regelungen, aber auch freiwilligen Kodizes in Unternehmen. Vgl. o. V.: Gabler Wirtschaftslexikon, 16., vollständig überarbeitete und aktualisierte Auflage, Wiesbaden: Gabler 2004, S. 604.

8 Vgl. Buchner, Manfred: Höchste Zeit für Basel II, in: Computerwoche, 21/2005, S. 27.

IT-Sicherheit und Risikomanagement werden seit einiger Zeit wissenschaftlich diskutiert und können als weit entwickelte Wissenschaftsfelder betrachtet werden. Diese Arbeit liefert einen Ansatz zur Integration der beiden Bereiche.

Dabei konzentrieren sich die Ausführungen zur IT-Sicherheit auf den Banken- und Finanzdienstleistungssektor. Die Abgrenzung wird vorgenommen, um die besonderen Anforderungen in diesem Bereich detailliert darzustellen. Neben der extremen Abhängigkeit der Geschäftsprozesse von der Funktionsfähigkeit der IT sind hier auch Sonderprobleme, wie die Integration extern erbrachter Leistungen (Outsourcing) und die zunehmende Vernetzung im Rahmen des elektronischen Datenaustausch zwischen den Finanzinstitutionen und beim Online-Banking im Privatkundenbereich zu berücksichtigen. Bei der Darstellung des Risikomanagements wird keine branchenspezifische Abgrenzung vorgenommen. Die darzustellende „best-practice“ gilt als Leitfaden für das Risikomanagement in unterschiedlichen Industriezweigen und ist - nach Anpassung an das spezifische Risikoumfeld – allgemein gültig.

Um eine ganzheitliche Darstellung von IT-Sicherheit und Risikomanagement zu entwickeln, werden in Kapitel 2 die für Kreditinstitute geltenden Vorgaben hinsichtlich ihrer Relevanz für die IT-Sicherheit untersucht. Dieser erste Schritt betrachtet Gesetze und Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und des Instituts der Wirtschaftsprüfer (IDW). Da in den Verlautbarungen der BaFin Anforderungen an die IT selten konkretisiert werden, sollen auch die oft zitierten „gängigen Standards“ in die Betrachtung mit eingehen. Als Zusammenfassung des Kapitels wird eine Konsolidierung der Vorgaben vorgenommen und es werden die Handlungsfelder für die Erfüllung der gestellten Anforderungen identifiziert und beschrieben.

Kapitel 3 stellt das Risikomanagement als idealtypisches System mit den wesentlichen Bestandteilen und Prozessschritten in einem Modell dar. Risikomanagement wird als iterativer Prozess der Strategieformulierung, Risikoidentifikation, -bewertung und -kontrolle verstanden. Zudem werden die Frühwarnsysteme und die Risikoüberwachung dargestellt und die Handlungsfelder im Bereich der IT-Sicherheit herausgestellt.

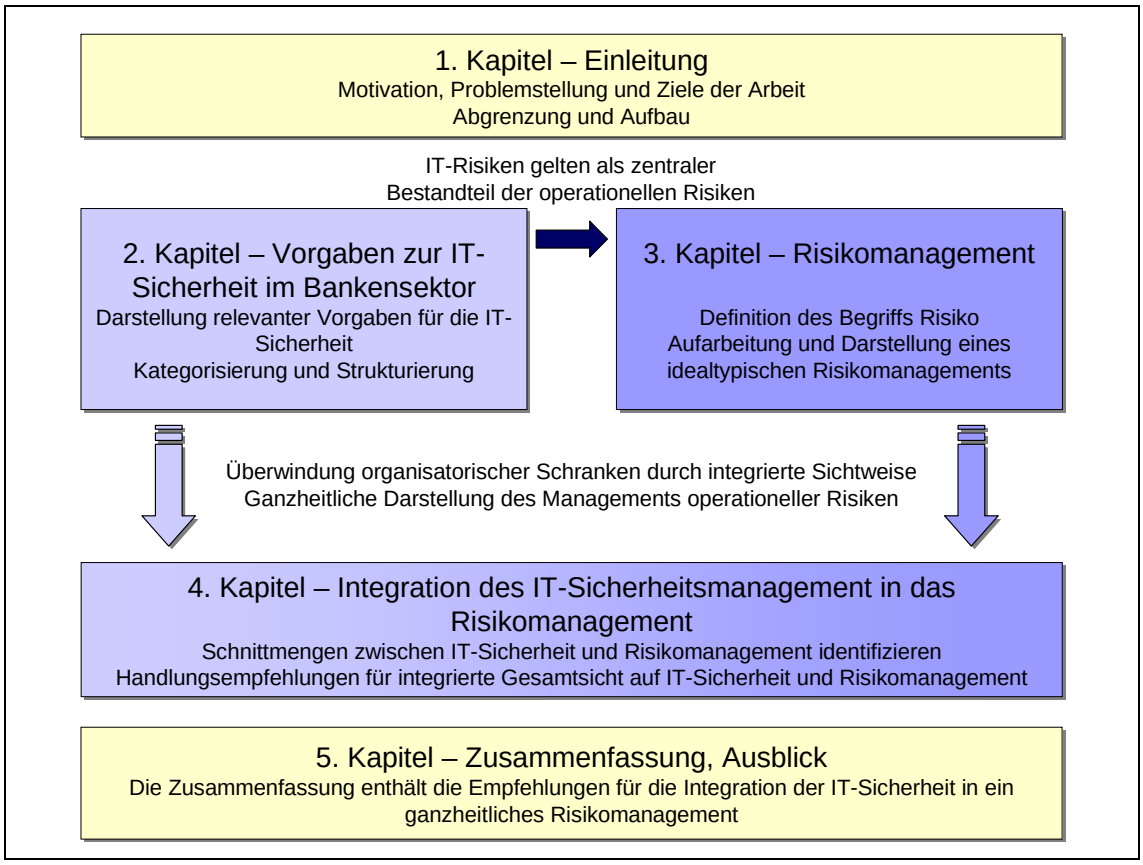

Abb. 1: Aufbau der Arbeit[9]

Die Zusammenführung der beiden vorangegangenen Kapitel in einen ganzheitlichen Ansatz ist eine wesentliche Leistung dieser Arbeit. Ein entsprechendes Konzept zur Eingliederung des IT-Sicherheitsmanagements in das Risikomanagement wird in Kapitel 4 entwickelt. Die gestellten regulatorischen Anforderungen (aus Kapitel 2) werden in das Modell des idealtypischen Risikomanagements (aus Kapitel 3) integriert. Diese übergreifende Sichtweise ermöglicht die Überwindung der in der Praxis häufig existierenden organisatorischen Schranken und stellt damit einen Beitrag zu einem effektiven Management operationeller Risiken dar.

Die Zusammenfassung in Kapitel 5 stellt abschließend die gewonnenen Ergebnisse und Handlungsgebiete dar. Empfehlungen für die Integration der IT-Sicherheit werden formuliert und damit Handlungsfelder für die Entwicklung eines effizienteren Risikomanagements aufgezeigt.

9 Zur Aussage „IT-Risiken gelten als zentraler Bestandteil der operationellen Risiken“ vgl. Hirschmann, Stefan; Romeike, Frank: IT-Sicherheit als Rating-Faktor, a. a. O., S. 13.

2 Vorgaben zur IT-Sicherheit im Bankensektor

2.1 Grundlagen und Definitionen

2.1.1 Informationstechnik, -verarbeitung und -technologie

Begriffe und Definitionen rund um die elektronische Datenverarbeitung haben sich ebenso wie die eingesetzten Verfahren und Techniken seit Mitte des letzten Jahrhunderts stetig weiterentwickelt. Der nachfolgende Abschnitt enthält das in der vorliegenden Arbeit verwendete Begriffsverständnis der Abkürzung *IT* und Vorüberlegungen zum Begriff *Sicherheit*. Diese sind als Grundlage für die weiteren Ausführungen zu verstehen.

Die Abkürzung IT wird sowohl für *Informationstechnik* als auch für *Informationstechnologie* gebraucht. In der Verwendung als *Informationstechnik* werden darunter alle mit der elektronischen Datenverarbeitung (EDV) und Datenfernübertragung (DFÜ) zusammenhängenden Techniken verstanden.[10] Technische Systeme sind gekennzeichnet durch die Funktion, „Stoff (Masse), Energie und/oder Information zu wandeln, zu transportieren und/oder zu speichern."[11] Auch wenn damit ein technisches System explizit mit der Verarbeitung von Informationen in Verbindung gebracht wird, ist die getroffene, eher naturwissenschaftlich geprägte Abgrenzung, für die vorliegende Arbeit wenig geeignet.

Stahlknecht verwendet ebenfalls den Begriff Informationstechnik, der die Verfahren der Kommunikationstechnik (Netze, Übertragungsverfahren usw.) einschließt. Informationsverarbeitung (IV) als zeitgemäße Formulierung für EDV gebraucht Stahlknecht, „wenn die betriebliche Informationsstruktur, d. h. die Geschäftsprozesse und Arbeitsabläufe unterstützenden Anwendungssysteme einschließlich der zu ihrer Entwicklung und Einführung eingerichteten Projekte im Vordergrund steht, und Informationstechnik, wenn es sich um die zugehörige Infrastruktur, d. h. zur Realisierung der betrieblichen Informationsstrukturen benötigten Plattformen (Hardware, Software, Netze) und personellen Ressourcen (…) einschließlich des dazu erforderlichen Managements handelt."[12]

---

10 Vgl. Brauner, Detlef-Jürgen; Raible-Besten, Robert; Weigert, Martin M.: PC-Anwender-Lexikon, München, Wien: Oldenbourg 1999, S. 230.

11 Vgl. o. V.: Brockhaus Enzyklopädie, 19.Auflage, Mannheim: Brockhaus 1993, Bd. 19, S. 672.

12 Stahlknecht, Peter; Hasenkamp, Ulrich: Einführung in die Wirtschaftsinformatik, 10. Auflage, Berlin et al.: Springer 2001, S. 13.

Technische Systeme allein sind nicht Betrachtungsobjekt der nachfolgenden Ausführungen. Die Systemumwelt und die Nutzer werden in die Betrachtung mit einbezogen. Der Zusammenhang zwischen Technik und ihrer Umwelt wird mit dem Begriff Informationstechnologie erfasst. Technologie wird verstanden als „Lehre von der Entwicklung der Technik in ihren gesellschaftlichen Zusammenhängen“.[13] Der Mensch mit seiner Fähigkeit, Informationen (Daten) aufzunehmen, diese verarbeiten, nutzen und weitergeben zu können muss als interpretierende und kommunizierende Instanz in die Betrachtung einbezogen werden.[14]

Daraus leitet sich das Verständnis für den Begriff IT in der vorliegenden Arbeit ab:

Informationstechnologie (IT) umfasst sowohl die Informationsverarbeitung als auch die Informationstechnik.

Damit ist der Bestandteil IT des Schlagwortes IT-Sicherheit im Rahmen dieser Arbeit abgegrenzt. Etwas komplexer gestaltet sich die Definition des zweiten Wortbestandteils. Konzepte zur Sicherheit und die Zusammenführung der Begriffe IT und Sicherheit werden im nachstehenden Kapitel 2.1.2 beschrieben.

2.1.2 Sicherheit in der Informationstechnologie

Allgemein bezeichnet Sicherheit einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird. Allerdings ist bei komplexen Systemen das Risiko nicht vollständig zu eliminieren. Sicherheit ist folglich nur sinnvoll als relativer Zustand zu verstehen, der für einen bestimmten Zeitraum, in einer bestimmten Umgebung und unter bestimmten Bedingungen erfüllt ist.[15]

In der englischsprachigen Literatur wird Sicherheit (in der IT) unterteilt in die beiden Teilbereiche *security* und *safety*. Dieses Begriffspaar findet häufig Verwendung in der Informationstechnik, da hier eine Abgrenzung nach der Intention des Angriffes auf die

13 Vgl. o. V.: Brockhaus Enzyklopädie, a. a. O., S. 680.

14 Vgl. Dierstein, Rüdiger: Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, in: Informatik Spektrum, Band 27, Heft 4, S. 344.

15 Vgl. o. V.: Wikipedia – Die freie Enzyklopädie: Sicherheit, Online im Internet: http://de.wikipedia.org/wiki/Sicherheit, 25.06.2006.

IT-Systeme vorgenommen wird. Es wird unterschieden zwischen intentionalen (absichtlichen, vorsätzlichen, gezielten) Beeinträchtigungen, deren Abwehr durch den Begriff *security* abgedeckt wird und den nichtintentionalen (zufälligen, fahrlässigen, unbeabsichtigten, gar unvermeidbaren) Beeinträchtigungen, deren Vorbeugung mit dem Begriff *safety* erfasst wird. Für die Vertrauenswürdigkeit eines Systems ist die Intention der Beeinträchtigung jedoch nachrangig. Ob die auslösende Instanz absichtlich oder unabsichtlich handelt, ist für resultierende Fehlfunktionen, falsche Ergebnisse und eventuelle Ausfallzeiten unerheblich.[16] Die hier zu behandelnden Sicherheitskonzepte können keine der beiden Intentionen bewusst ausklammern. Beide Teilgebiete sind zu betrachten.

In der IT wurde Sicherheit lange Zeit im Wesentlichen mit Geheimhaltung gleichgesetzt. Heute hat sich die Auffassung durchgesetzt, dass mindestens drei Aspekte gleichrangig zu behandeln sind:

- **Vertraulichkeit**: Vertrauliche Informationen stehen nur den autorisierten Benutzern zur Verfügung.
- **Verfügbarkeit**: Dienstleistungen und Funktionen eines IT-Systems stehen dem autorisierten Nutzer zum geforderten Zeitpunkt zur Verfügung.
- **Integrität**: Daten sind vollständig und unverändert.[17]

Diese drei Grundwerte der IT-Sicherheit wurden vom Bundesamt für Informationssicherheit (BSI) bzw. dessen Vorgängerorganisation, der Zentralstelle für Sicherheit in der Informationstechnologie (ZSI), formuliert.[18] Verschiedene Autoren erweitern diese Kriterien, um das weite Spektrum der Sicherheitsanforderungen an moderne IT-Systeme abzudecken. Während Schaumüller-Bichl (1992) als vierte Grundbedrohung den Verlust der Originalität und damit die unbefugte Duplikation von Informationen auf-

16 Vgl. Dierstein, Rüdiger: Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, a. a. O.: S. 343 f.

17 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzhandbuch: Stand 2005, Online im Internet: http://www.bsi.de/gshb/deutsch/download/itgshb_2005.pdf, 25.06.2006, S. 41 ff.

18 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) – Version 1.0, Online im Internet: http://www.bsi.de/literat/bsi_standard/standard_1001.pdf, 25.05.2006.

nimmt,[19] wird in aktuellen Publikationen vor allem auf die rechtliche Verwertbarkeit der Information abgestellt. So nennen Laudon et al. als viertes Schutzziel der IT-Sicherheit die Zurechenbarkeit und erläutern dazu, dass Kommunikation gerichtsverwertbar dem ausführenden Kommunikationsteilnehmer zuzuordnen sein sollte.[20]

Die Diskussion um die Erweitung der bekannten Grundwerte nimmt Dierstein als Grundlage für seine Überlegungen zur Semantik des Begriffs IT-Sicherheit. Die bisher vorherrschende Sicht der *Verlässlichkeit* (dependability) mit den drei Dimensionen Vertraulichkeit, Integrität und Verfügbarkeit muss ergänzt werden. Die Abwicklung von Rechtsgeschäften auf elektronischem Wege bedingt eine Erweiterung um eine neue Sichtweise, die explizit den Schutz der Betroffenen vor dem System einbezieht. Diese neue semantische Dimension wird mit *Beherrschbarkeit* (controllability) bezeichnet.

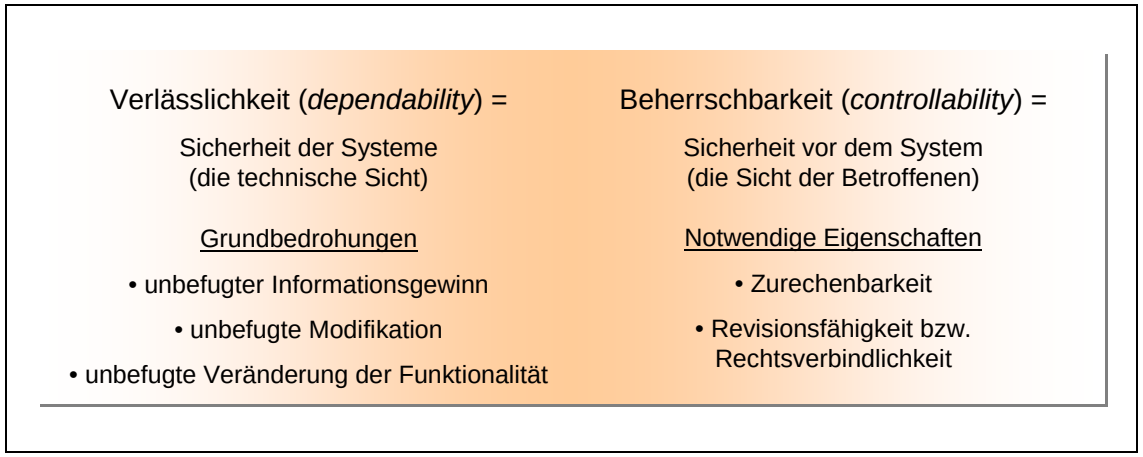

Abb. 2: Konzept der dualen Sicherheit[21]

Daraus ergibt sich das *Konzept der dualen Sicherheit*. Sicherheit wird auf der einen Seite als Sicherheit der Systeme (Verlässlichkeit), auf der anderen Seite als Sicherheit vor dem System (Beherrschbarkeit) verstanden. Die oben genannten Grundwerte der IT-Sicherheit werden um zwei wesentliche Komponenten erweitert: die Zurechenbarkeit der Vorgänge und Ergebnisse zu definierbaren Veranlassern (auslösende Instanz) und

19 Vgl. Schaumüller-Bichl, Ingrid: Sicherheitsmanagement: Risikobewältigung in informationstechnologischen Systemen, a. a. O., S. 40.

20 Vgl. Laudon, Kenneth C.; Laudon, Jane P.; Schoder, Detlef: Wirtschaftsinformatik – Eine Einführung, München, Boston: Pearson Studium 2006, a. a. O., S. 654.

21 Eigene Darstellung, in Anlehnung an: Dierstein, Rüdiger: Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, a. a. O., S. 346 ff.

die Beweisbarkeit aller Daten und Vorgänge gegenüber Dritten.[22] Die rechtliche Verwertbarkeit von Informationen ist gerade im Bankgeschäft mit den global vernetzten Systemen von hoher Relevanz.

Neben der ausgedehnten Diskussion zur Semantik der IT-Sicherheit existiert als „klassische Sichtweise“ zur Systemsicherheit eine weitere Einteilung, die sich an der Umsetzung von Sicherheit in der Praxis orientiert. Lösungen für die Probleme der IT-Sicherheit sind demnach in

- organisationstechnischen Maßnahmen,
- baulichen Maßnahmen,
- organisatorischen Maßnahmen und
- personellen Maßnahmen

zu suchen.[23] Diese Klassifikation nach Art der getroffenen Vorkehrungen zeigt erneut, dass neben der Technik die Systemumwelt Teil der Sicherheitskonzeption sein muss.

Die allgemeinen Aussagen zur Sicherheit in der Informationstechnologie dokumentieren, wie umfassend IT-Sicherheit zu betrachten ist. Es muss auch festgehalten werden, dass Vorgaben zur IT-Sicherheit wohl nie alle Aspekte der Sicherheit abdecken werden. Im Bankensektor fokussieren viele Gesetze und Verlautbarungen auf allgemeine Anforderungen zur Kompatibilität der Systeme im Zahlungsverkehr zwischen Geschäftsbanken. Sicherheitsanforderungen an Gesamtsysteme werden oft nur abstrakt formuliert. Für die folgenden Unterkapitel zur IT-Sicherheit im Bankensektor muss folglich die Idealvorstellung aufgegeben werden, bankenübergreifende, verbindliche und detaillierte Anforderungskataloge zur IT-Sicherheit aufstellen zu können. Vielmehr betrachten die nachfolgend aufgeführten Gesetzte, Verlautbarungen und Standards verschiedene Aspekte aus teilweise unterschiedlichen Blickwinkeln. Die verschiedenen Beiträge von Gesetzgeber und Standardsettern erheben nicht den Anspruch, das Themengebiet IT-Sicherheit vollständig abzudecken.[24]

---

22 Vgl. Dierstein, Rüdiger: Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, a. a. O., S. 345 ff.

23 Vgl. Schaumüller-Bichl, Ingrid: Sicherheitsmanagement: Risikobewältigung in informationstechnologischen Systemen, a. a. O., S. 17.

24 Vgl. Münch, Isabel; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, Bonn: SecuMedia 2002, S. 30.

Mit den angeführten Überlegungen zu IT und IT-Sicherheit ist der definitorische Hintergrund für die weitere Darstellung geschaffen. Es wird nun dargestellt, welche gesetzlichen Anforderungen, Vorgaben und Konzepte für das Themengebiet der IT-Sicherheit zu beachten sind. Die in den letzten Jahren stark ansteigende Zahl der regulatorischen Anforderungen wird als abschließende Zusammenfassung des zweiten Kapitels in Kapitel 2.5 kategorisiert werden, um Überschneidungen in den Anforderungen und Zusammenhänge zwischen den einzelnen Regelungen herauszuarbeiten.

2.2 Gesetzliche Vorgaben

2.2.1 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurde 1998 verabschiedet und enthält als sog. Artikelgesetz Ergänzungen und Änderungen zu anderen Wirtschaftsgesetzen. Neuregelungen finden sich u. a. im Aktiengesetz (AktG) sowie im Handelsgesetzbuch (HGB). Der Anwendungsbereich umfasst Aktiengesellschaften sowie Gesellschaften, die die Merkmale einer mittelgroßen Kapitalgesellschaft nach § 267 HGB erfüllen.[25]

Das KonTraG verfolgt zwei grundsätzliche Regelungsziele: Die (1) Kontrollsysteme des deutschen Aktienrechts sollen verbessert werden und (2) deutsche Publikumsgesellschaften sollen den Informationsanforderungen internationaler Kapitalmärkte besser Rechnung tragen. Eine wesentliche Änderung nach KonTraG findet sich im Aktiengesetz. § 91 Abs. 2 AktG fordert ein Überwachungssystem, das die den Fortbestand der Gesellschaft gefährdenden Entwicklungen früh erkennen lässt (Frühwarnsystem). Das KonTraG erwähnt die Möglichkeit von Schadensersatzforderungen gegenüber den Vorstandsmitgliedern, falls diese ihre Pflichten verletzen. Verstärkt wird die Wirkung des § 91 Abs. 2 AktG durch die Formulierung aus dem HGB, die für börsennotierte Aktiengesellschaften in § 317 HGB im Rahmen der Abschlussprüfung vom Wirtschaftsprüfer zu prüfen verlangt, (…) ob der Vorstand die ihm nach § 91 Abs. 2 des AktG obliegenden Maßnahmen in geeigneter Form getroffen hat und ob das danach einzurichtende

25 Vgl. Heinrich, Robert; Lang, Franz-Josef: DV und Recht/Risikobewertung und Frühwarnsysteme – Ein neues Gesetz macht die IT-Sicherheit zur Pflicht, in: Computerwoche, 24/1999, S. 71.

Überwachungssystem seine Aufgaben erfüllen kann. Auch die Risiken der zukünftigen Entwicklung sind nach § 289 Abs. 1 HGB zu beachten.[26]

Das KonTraG liefert mit den Novellierungen in HGB und AktG keine konkreten Anforderungen an die IT-Sicherheit. Vielmehr werden hier grundsätzliche Anforderungen an ein Risikofrüherkennungssystem formuliert. Diese Anforderungen werden im Rahmen dieser Arbeit in Kapitel 3 als Teilgebiet eines idealtypischen Risikomanagements ausführlich behandelt. Die Einbeziehung des Risikomanagementsystems im Rahmen der Abschlussprüfung börsennotierter Kapitalgesellschaften nach § 317 HGB führt dazu, dass sich auch das IDW in seinen Prüfungsstandards mit der ordnungsmäßigen Geschäftsorganisation befasst. Die für die IT-Sicherheit relevanten Verlautbarungen des IDW werden deshalb in Kapitel 2.3.2 dieser Arbeit einbezogen.

2.2.2 Gesetz über das Kreditwesen

Dem Gesetz über das Kreditwesen (KWG) unterliegen alle Kredit- und Finanzdienstleistungsinstitute mit Sitz in der Bundesrepublik Deutschland sowie inländische Zweigstellen von Instituten mit Sitz in Drittstaaten. Ziel des KWG ist die Sicherung und Erhaltung der Funktionsfähigkeit der Kreditwirtschaft und der Schutz der Gläubiger von Kreditinstituten. Das KWG stellt zudem die gesetzliche Grundlage für die Bankenaufsicht durch die BaFin dar. Die BaFin hat das Ziel, ein funktionsfähiges, stabiles und integres deutsches Finanzsystem zu gewährleisten. Sie ist als Nachfolgeorganisation des 1962 gegründeten Bundesaufsichtsamtes für das Kreditwesen seit 2002 (zusammen mit den Bundesämtern für Wertpapierhandel und Versicherungswesen) als selbstständige Anstalt des öffentlichen Rechts für die Allfinanzaufsicht in der Bundesrepublik Deutschland zuständig.[27]

Mit der 6. Novelle des KWG von 1997 wurde der vor dem Hintergrund der IT-Sicherheit wesentliche § 25a KWG eingeführt. Die hinzugekommenen Regelungen entspre-

26 Münch, Isabel; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, a. a. O., S. 32 f.

27 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Aufgaben und Ziele: Bundesanstalt für Finanzdienstleistungsaufsicht, online im Internet: http://www.bafin.de/cgi-bin/bafin.pl?verz=0201000000&sprache=0&filter=a&ntick=0, 25.06.2006.

chen in der rechtlichen Bedeutung weitgehend dem durch das KonTraG eingeführten § 91 Abs. 2 AktG. Die Anforderungen des KWG gehen in Bezug auf Inhalt, Ausgestaltung und Konkretisierung aber über das Aktienrecht hinaus. In § 25a Abs. 1 werden besondere organisatorische Pflichten für die beaufsichtigten Institute aufgestellt. Subsumiert werden die Anforderungen unter dem Begriff *Ordnungsmäßigkeit der Geschäftsorganisation*. Der BaFin wird dabei die Möglichkeit eingeräumt, nähere Anordnungen zu erlassen, wie die organisatorischen Pflichten auszugestalten sind. Auch bei der Umsetzung hat die BaFin erweiterte Möglichkeiten Verstöße zu ahnden. Diese Sanktionen können bis zur Einschränkung bzw. Versagung der Erlaubnis zum Betreiben von Bankgeschäften bzw. zum Erbringen von Finanzdienstleistungen nach § 35 KWG reichen.[28]

Zu den Pflichten aus § 25a KWG gehören explizit auch angemessene Sicherheitsvorkehrungen für den Einsatz elektronischer Datenverarbeitung (§ 25a Abs. 1 Nr. 2 KWG). Vor dem Hintergrund des möglichen Zusammenbruchs eines Instituts bei Ausfall der EDV fordert der Gesetzgeber die Angemessenheit der Sicherheitsvorkehrungen in der EDV. Anhand der vorgegebenen aufsichtsrechtlichen Ziele

- Sicherung der anvertrauten Vermögenswerte,
- Sicherung der ordnungsgemäßen Durchführung der Bankgeschäfte und Finanzdienstleistungen und
- Vermeidung von Nachteilen für die Gesamtwirtschaft durch Missstände im Kredit- und Finanzdienstleistungswesen

sind die getroffenen Maßnahmen zu bewerten. Die Ausgestaltung der einzelnen Sicherheitsvorkehrungen richtet sich nach Art und Umfang des Einsatzes der EDV.[29] Sicherheitsmaßnahmen werden in zweierlei Hinsicht klassifiziert. Eine Übersicht über die Aspekte der Sicherheitsmaßnahmen mit typischen Beispielen liefert Tab. 1.

28 Vgl. Braun, Ulrich: § 25a KWG – Besondere organisatorische Pflichten von Instituten, in: Kreditwesengesetz – Kommentar zu KWG und Ausführungsvorschriften, Hrsg.: Boos, Karl-Heinz; Fischer, Reinfried; Schulte-Mattler, Hermann, 2. Auflage, München: C. H. Beck 2004, Rn 1 ff.

29 Vgl. Braun, Ulrich: § 25a KWG – Besondere organisatorische Pflichten von Instituten, a. a. O., Rn. 142 ff.

	Organisatorisch	Physisch-technisch	System-technisch
Fehler-/Schadens-verhindernde Maßnahme	Vorkontrolle	Closed-shop	Zugriffsschutz
Fehler-/Schadens-aufdeckende Maßnahme	Nachkontrolle	Rauchmelder	Programmierte Kontrolle
Vorsorgemaßnahme	Back-up-Vereinbarungen	Datenauslagerung	Datensicherung
Eventualplanung	Datenrekonstruktionen, Wiederanlaufverfahren, Back-up-Betrieb		

Tab. 1: Aspekte von Sicherheitsmaßnahmen und typische Beispiele[30]

§ 25a Abs. 2 KWG beschäftigt sich mit besonderen organisatorischen Anforderungen an die Ausgestaltung und Zulässigkeit der Auslagerung bestimmter Bereiche auf andere Unternehmen (Outsourcing). Die Auswirkungen des KWG auf IT-Dienstleister leiten sich aus den allgemeinen Anforderungen des KWG an die IT-Sicherheit ab. Neben Sicherheitsmaßnahmen zur Garantie geschützter Zugriffe auf vertrauliche Daten fordert die BaFin insbesondere eine hohe Verfügbarkeit der Systeme. Bei Systemausfall muss die ordnungsgemäße Fortführung des Geschäftsbetriebs möglich sein. Werden entsprechende Bereiche eines Finanzinstituts auf einen Dienstleister ausgelagert, so unterliegt dieser der Überprüfung durch die BaFin im Rahmen der Allfinanzaufsicht. Das Dienstleistungsunternehmen steht gegenüber der Bank in einer permanenten Informations- und Handlungspflicht. Insbesondere müssen Dienstleister im Bankensektor besondere Qualitäts- und Sicherheitsstandards einhalten.[31] Die hohen Anforderungen des § 25a Abs. 2 KWG führten in der Vergangenheit dazu, dass Banken nur relativ wenige Bereiche und dabei vor allem unterstützende Tätigkeiten an externe Anbieter auslagerten. Kernprozesse wie die Kredit- und Hypothekenabwicklung sowie das damit verbundene Risikomanagement werden als Kernkompetenzen der Banken für nicht auslagerungsfähig angesehen.[32]

30 Vgl. Tappert, Rainer: EDV-System-Prüfung – Bankbetriebliche Revisionsinformatik, Köln: Bank-Verlag 1994, S. 57 f.

31 Vgl. Mohr, Sonja: Outsourcing nach Bankenart - § 25a KWG als Grundlage für sichere IT-Dienstleistungen, in: <kes> Die Zeitschrift für Informations-Sicherheit, 6/2005, S. 85.

32 Vgl. Prehl, Sabine: Outsourcing: Für Banken eine harte Nuss, in: Computerwoche, 2/2005, S. 32.

Für die konkrete Umsetzung der Anforderungen des KWG an sichere IT-Systeme liefert der Gesetzgeber nur wenige Anhaltspunkte. Es wird vor allem auf die Angemessenheit der Systeme abgestellt. Bei Auslagerung von bestimmten Datenverarbeitungs- und Datensicherungsvorgängen kann diese Angemessenheit bspw. ein rund um die Uhr stabil funktionierendes Rechenzentrum, das höchste Ansprüche an Sicherheit und Verfügbarkeit von Daten und Systemen erfüllt, umfassen. Dazu gehört u. a. eine permanente Gebäude- und Technikü̈berwachung, überwachte Sicherheitszonen, Sicherheitskonzepte zur Vermeidung unberechtigter Zugriffe (Umsetzung: Firewalls), Rechnerzellen mit vollkommen autonomer Technik und Versorgung, automatisierte Datensicherungsverfahren sowie 100-prozentige Kapazitätsreserven im Katastrophenfall. Zusätzlich verlangt das KWG Regelungen für die rechtliche Verbindlichkeit von Informationen, die vor allem die (ggf. gerichtlich) nachweisbare Autorisierung von Transaktionen abzielt. Zu einer sicheren IT-Landschaft nach Vorstellungen der BaFin gehören außerdem umfassende Notfallpläne und Sicherungsmaßnahmen für Extremsituationen, die die zeitnahe Wiederherstellung der Systeme unter Vermeidung von Inkonsistenzen ermöglichen.[33] Damit decken die im KWG genannten Anforderungen weite Teile des oben dargestellten Konzeptes dualer Sicherheit ab.

Die vorangegangenen Ausführungen machen deutlich, dass das KWG weit reichende Anforderungen an die IT-Sicherheit stellt. Bei der konkreten Umsetzung und Ausgestaltung der Maßnahmen liefert der Gesetzestext allerdings kaum Hilfestellung für die Praxis. Unterstützung bei der praktischen Umsetzung geben sowohl die Verlautbarungen von Aufsichtsorganen, die in Kapitel 2.3 behandelt werden, als auch national und international anerkannte Sicherheitsstandards, die Bestandteil von Kapitel 2.4 sind.

2.2.3 Anforderungen des Baseler Ausschuss für Bankenaufsicht

Der Baseler Ausschuss für Bankenaufsicht ist eine 1974 gegründete Organisation (Mitglieder sind Zentralbanken und Aufsichtsinstanzen führender Industrieländer, für Deutschland bspw. die Deutsche Bundesbank und die BaFin), deren Ziel die Entwick-

33 Vgl. Mohr, Sonja: Outsourcing nach Bankenart - § 25a KWG als Grundlage für sichere IT-Dienstleistungen, a. a. O., S. 85 f.

lung umfassender aufsichtsrechtlicher Standards, Richtlinien und Empfehlungen ist.[34] Formal gesehen hat der Ausschuss keine aufsichtsrechtliche Legitimierung und ist deshalb auch nicht als supranationaler Gesetzgeber anzusehen. Vielmehr zeigt sich, dass die entwickelten Empfehlungen von den nationalen Gesetzgebern nach und nach in geltendes Recht umgesetzt werden und somit Verbindlichkeit für die weltweite Bankenlandschaft als internationale Standards erreichen. Unter der Bezeichnung „Neue Baseler Eigenkapitalvereinbarung“ (kurz Basel II) hat der Baseler Ausschuss für Bankenaufsicht ein neues Regelwerk für die Erfassung und Behandlung von Risiken in der Finanzdienstleistungsbrache aufgestellt.

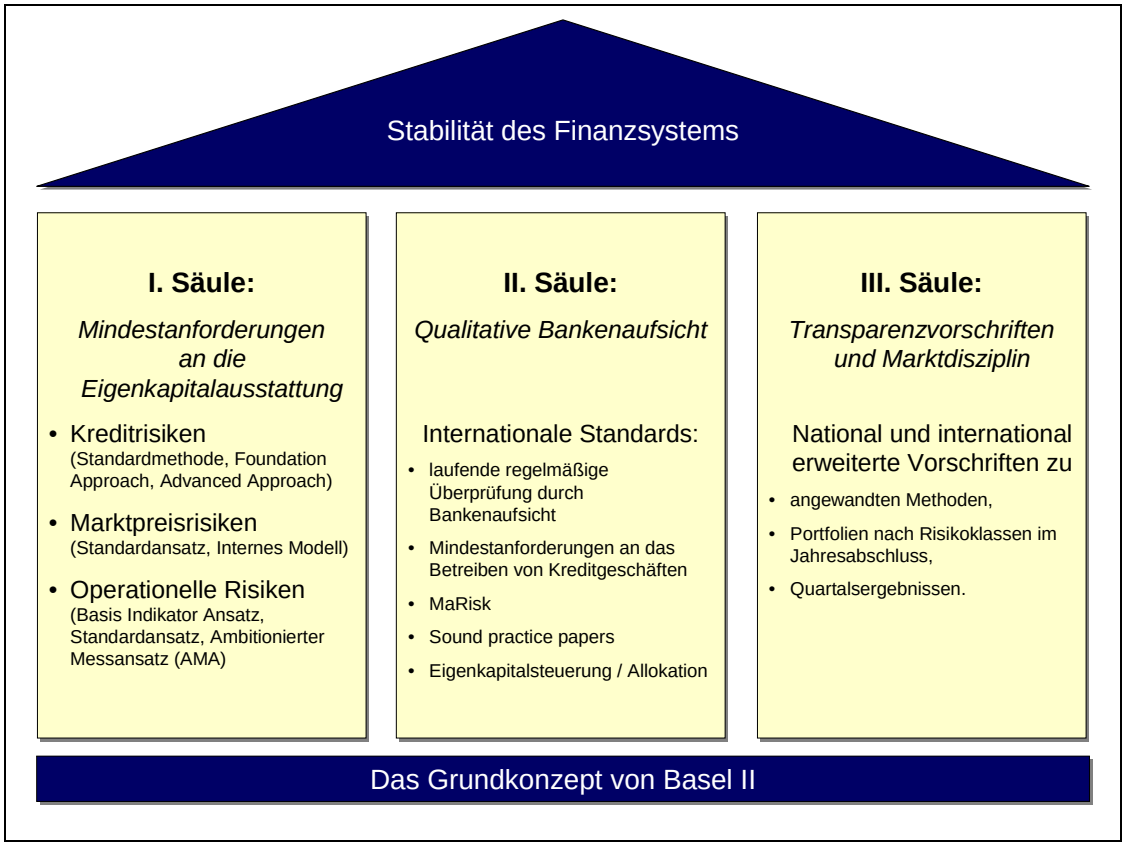

Abb. 3: 3-Säulen-Konzept von Basel II

Die Teilgebiete von Basel II werden häufig in Form von drei Säulen (siehe Abb. 3) dargestellt. Zur Sicherung der Stabilität der Finanzsysteme werden Anforderungen zur angemessenen Unterlegung von Risiken mit Eigenkapital formuliert (Säule I) sowie eine

34 Vgl. Baseler Ausschuss für Bankenaufsicht (Hrsg.): The Basel Committee on Banking Supervision, Online im Internet: http://www.bis.org/bcbs/aboutbcbs.htm, 25.06.2006.

qualitative Aufsicht (Säule II) neben erweiterten Transparenzvorschriften (Säule III) eingeführt.

Die Umsetzung von Basel II in deutsches Recht erfolgt im Rahmen der Solvabilitätsverordnung (SolvV) und den Mindestanforderungen an das Risikomanagement (MaRisk). Die SolvV überführt als Gesetz die erste und dritte Säule in deutsches Recht und liegt bisher als Entwurf vor.[35] Da sie keine konkreten Anforderungen an die IT-Sicherheit enthält, wird die SolvV im Rahmen dieser Arbeit nicht näher behandelt. Die MaRisk werden als Verlautbarung der BaFin im Kapitel 2.3.1 ausführlich dargestellt.

Mit der Neufassung der Eigenkapitalvereinbarung von 1988 werden explizit eine Quantifizierung der operationellen Risiken und die Eigenkapitalhinterlegung für diese gefordert. Operationelles Risiko umfasst in der Definition des Baseler Ausschusses „die Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten. Diese Definition schließt Rechtsrisiken ein, beinhaltet aber nicht strategische Risiken oder Reputationsrisiken."[36] Erstmals werden mit Basel II auch Mindeststandards für das Risikomanagement gesetzt.[37]

Risiken aus der IT gelten als zentraler Bestandteil der operationellen Risiken, da die IT heute die Geschäftsprozesse der Banken in vielen Fällen vollständig determiniert.[38] Zu beachten sind hier sowohl aktive Angriffe auf die IT in Form von Viren und Trojanischen Pferden als auch insbesondere solche Risiken, die aus der wachsenden Komplexität der Gesamtsysteme und dem Parallelbetrieb von heterogenen Standardanwendungssystemen entstehen.[39]

---

35 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Entwurf: Verordnung1 über die angemessene Eigenkapitalausstattung (Solvabilität) von Kreditinstituten – Solvabilitätsverordnung, Online im Internet: http://www.bafin.de/verordnungen/solvv/01_entwurf.pdf, 31.03.2006.

36 Baseler Ausschuss für Bankenaufsicht (Hrsg.): Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen – überarbeitete Rahmenvereinbarung (Juni 2004), Online im Internet: http://www.bis.org/publ/bcbs107ger.pdf, 25.06.2006, S. 127.

37 Weite Ausführungen zum Risikomanagement sind Inhalt von Kapitel 3 dieser Arbeit.

38 Vgl. Hirschmann, Stefan; Romeike, Frank: IT-Sicherheit als Rating-Faktor, a. a. O., S. 13.

39 Vgl. Mehlau, Jens Ingo: Die Bedeutung des IT-Sicherheitsmanagement für Finanzdienstleister, in: Banking and Information Technologie (BIT), 3/2001, S. 11.

Sicherheitsrisiken aus der IT werden in Basel II allerdings nicht in einer oder mehreren eigenen Risikokategorien berücksichtigt, sondern finden sich verteilt über andere Kategorien (bspw. werden die „Schäden durch Hackeraktivitäten“ neben Diebstahl und Betrug in die Ereigniskategorie „Externe betrügerische Handlungen“ eingeordnet).[40] Die IT-Sicherheit ist folglich wesentlich für die Begrenzung des operationellen Risikos. Konkrete Maßnahmen beinhaltet der Baseler Eigenkapitalakkord nicht. Sie sind teilweise Inhalt anderer Publikationen, wie den „Risk Management Priciples for Electronic Banking.“[41]

Der Baseler Ausschuss berücksichtigt aus den bekannten Teilaspekten Verfügbarkeit, Integrität und Vertraulichkeit primär Aspekte der Verfügbarkeit. Diese sind relativ einfach zu quantifizieren und lassen sich somit in die Eigenkapitalberechnung einbeziehen.[42] Trotz dieser Fokussierung auf einen leicht messbaren Teil von IT-Sicherheit bleibt festzuhalten, dass mit sicheren IT-Systemen das operationelle Risiko begrenzt wird.

2.2.4 Bundesdatenschutzgesetz

Die Verarbeitung personenbezogener Daten unterliegt den Regelungen des Bundesdatenschutzgesetztes (BDSG). Das Gesetz schützt den Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinen Persönlichkeitsrechten beeinträchtigt wird (§ 1 Abs. 1 BDSG). Für die meisten Unternehmen (und damit auch für Finanzdienstleistungsinstitute) sind die Regelungen der §§ 3a, 4, 9 (samt Anlage), 28 und 31 des BDSG einschlägig. Die Grundsätze der Datenvermeidung und Datensparsamkeit sind generell zu beachten. Zudem sind personenbezogene Daten nur auf Basis einer Rechtsgrundlage (gesetzliche Vorschrift, Vertragsverhältnis, vertragsähnliches

40 Vgl. Baseler Ausschuss für Bankenaufsicht (Hrsg.): Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen – überarbeitete Rahmenvereinbarung (Juni 2004), a. a. O., S. 210.

41 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, in: Innovationen im Retail-Banking: der Weg zum erfolgreichen Privatkundengeschäft, Hrsg.: Bartmann, Dieter, Weinheim : Wiley-VCH, 2005, S. 483.

42 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 483.

Vertrauensverhältnis oder Einwilligung des Betroffenen) zu erheben, zu verarbeiten oder zu nutzen.[43]

In Bezug auf IT-Sicherheit und die zu treffenden organisatorischen und technischen Maßnahmen ist § 9 BDSG und dessen Anlage einschlägig. Die getroffenen Maßnahmen unterstehen nach Satz 2 dem Grundsatz der Verhältnismäßigkeit. In der Anlage zu § 9 Satz 1 BDSG werden die sog. „acht goldenen Regeln zur IT-Datensicherheit“[44] formuliert. Diese umfassen im Einzelnen:

1) *Zutrittskontrollen:* Unbefugten ist der „körperliche“ Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Damit soll von vorneherein die Möglichkeit unbefugter Kenntnis- oder Einflussnahme verhindert werden.

2) *Zugangskontrolle:* Sie verhindert den unbefugten Zugang externer Personen auf das EDV-System.

3) *Zugriffskontrolle:* Gewährleistet, dass berechtigte Nutzer nur auf die ihren Zugriffsberechtigungen unterliegenden Daten zugreifen können. Die Organisation muss sicherstellen, dass der einzelne Mitarbeiter nur auf die zur Erledigung seiner Aufgaben benötigten Daten zugreifen kann.

4) *Weitergabekontrolle:* Verhindert das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern.

5) *Eingabekontrolle:* Gewährleistet, dass nachträglich die Veränderung personenbezogener Daten mit personeller und zeitlicher Zuordnung festgestellt werden kann. Dies ist in der Regel durch Protokollierung der Zugriffe zu realisieren. Unverzichtbar ist diese Kontrolle insbesondere, wenn die Eingabe zum Zwecke der Änderung von mehreren Arbeitsplätzen aus erfolgen kann.

6) *Auftragskontrolle:* Die im Rahmen eines Auftrags zu verarbeitenden Daten sind nur entsprechend der Weisung des Auftraggebers zu verarbeiten.

---

43 Vgl. Witt, Bernhard C.: Rechtliche Anforderungen an die Informations-Sicherheit, in: <kes> Die Zeitschrift für Informations-Sicherheit, 1/2006, S. 95.

44 Vgl. Anduleit, Manfred: IT-Sicherheit ist Chefsache, in Computerwoche, 21/2005, S. 41.

7) *Verfügbarkeitskontrolle:* Daten sollen vor zufälliger Zerstörung durch externe Einflüsse (Brand, Wasserschäden, Blitzschlag, Stromausfall) geschützt werden. Dazu sind bspw. ausgelagerte Sicherheitskopien anzulegen oder eine Notstromversorgung einzurichten.

8) *Trennungsgebot:* Eine zweckbestimmte Verarbeitung soll auch technisch sichergestellt werden. Dieses Gebot greift nicht, wenn die Zusammenführung der Daten vorgesehen ist. Es verlangt auch keine räumliche Trennung der Datenbestände.[45]

Für die Umsetzung der Regeln werden neben Restriktionen vielfach Protokollierungsaufgaben zum Nachweis des ordnungsmäßigen Betriebs vorgegeben. Diese Protokolle dienen ausschließlich der Beweissicherung in Missbrauchsfällen und sind streng zweckgebunden.[46]

Die Erfüllung der Anforderungen des BDSG muss bei Banken in einer hohen Prioritätsstufe angesiedelt werden. Die Sicherheit der vorliegenden Daten ist für das Vertrauensverhältnis zwischen Banken und deren Kunden essenziell. Es muss festgehalten werden, dass das BDSG gemessen am Konzept der dualen Sicherheit eher den Bereich *Beherrschbarkeit (Sicherheit vor dem System)* adressiert und damit einen anderen Teilbereich abdeckt als das KonTraG und das KWG.

2.2.5 Wertpapierhandelsgesetz

Die Bestimmungen des Wertpapierhandelsgesetztes (WpHG) dienen der Kontrolle von Dienstleistungsunternehmen, die Wertpapierhandel sowie Finanztermingeschäfte betreiben. Ein wesentliches Ziel ist die Verhinderung des Insiderhandels. Die BaFin überwacht als Allfinanzaufsichtsbehörde die Einhaltung der Vorschriften und ist befugt, Anordnungen zu treffen, die geeignet oder erforderlich sind, Missstände zu beseitigen oder zu verhindern (§ 4 Abs. 1 S. 3 WpHG).

Zur Verbesserung des Anlegerschutzes wurde der § 15b WpHG (Führung von Insiderverzeichnissen) eingeführt. Der Emittent von Finanzinstrumenten, die an einem inländi-

45 Vgl. Gola, Peter; Schomerus, Rudolf: Bundesdatenschutzgesetzt – Kommentar, 7. völlig neu bearbeitete Auflage, München: C. H. Beck 2002, S. 316 ff.

schen organisierten Markt gehandelt werden bzw. werden sollen, muss ein Verzeichnis der Mitarbeiter, die Zugriff auf Insiderinformationen haben, führen. Um sicherzustellen, dass tatsächlich nur dieser Kreis von Mitarbeitern Zugriff erhält, ist entsprechende Sicherheitstechnik (z. B. gruppenorientierte Dateiverschlüsselung) notwendig.[47]

2.2.6 Sarbanes-Oxley Act

Der Sarbanes-Oxley Act (SOA oder auch SOX) wurde Mitte 2002 vom US-Präsidenten unterzeichnet. Das Gesetz soll das Vertrauen der Anleger in die Rechnungslegung der Unternehmen nach den Bilanzskandalen der jüngeren Vergangenheit (z. B. Enron, WorldCom) wieder herstellen. Im SOA werden insbesondere die Verantwortlichkeiten der Unternehmensführung und der Wirtschaftsprüfer grundlegend neu definiert. Die Regelungen des SOA sind Teil dieser Arbeit, da sie nicht nur für US-amerikanische Unternehmen gelten. Sie betreffen vielmehr alle Unternehmen, die an einem amerikanischen Börsenplatz notiert sind und damit bei der Security and Exchange Commission (SEC)[48] registriert sind.[49] Aus dem im Rahmen dieser Arbeit betrachteten Finanzdienstleistungssektor sind als deutsche Unternehmen die Allianz (mit ihrer Konzerntochter Dresdner Bank) und die Deutsche Bank von den Regelungen des SAO betroffen.[50]

Der SOA beinhaltet Maßnahmen mit Auswirkungen auf verschiedene Gebiete: die Verantwortung des Managements (incl. Schadensersatzansprüchen der Shareholder), die internen Kontrollen im gesamten Unternehmen und die Rolle der Wirtschaftsprüfer. Die jeweiligen Regelungen werden in elf Abschnitte unterteilt. Von besonderer Bedeutung sind die Sections 302 und 404 des SOA. Diese beschäftigen sich mit den Anforderungen und die Ausgestaltung eines Internen Kontrollsystems (IKS) im Unternehmen. Insbesondere die Finanzberichterstattung muss durch ein System kontrolliert werden, das

46 Vgl. Witt, Bernhard C.: Rechtliche Anforderungen an die Informations-Sicherheit, a. a. O., S. 95 f.

47 Vgl. Anduleit, Manfred: IT-Sicherheit ist Chefsache, a. a. O., S. 41.

48 Die SEC ist die amerikanische Börsenaufsichtsbehörde. Sie kontrolliert die Zulassung zum Handel an der New York Stock Exchange.

49 Vgl. Foit, Mihael: Management operationeller IT-Risiken in Banken, Regensburg: Universitäts-Verlag Regensburg, 2005, S. 97 f.

50 Vgl. o. V.: US-Listing: Einbahnstraße New York, Online im Internet: http://www.manager-magazin.de/geld/artikel/0,2828,321440,00.html, 04.10.2004.

regelmäßiger Pflege und Überwachung unterliegt. Für die Ordnungsmäßigkeit des IKS ist das Management verantwortlich.[51]

Konkret verlangt der SOA eine eidesstattliche Erklärung des Managements (CEO und CFO) zur Korrektheit der Angaben in der Finanzberichterstattung. Zudem sind die Kontrollen durch einen externen Wirtschaftsprüfer in ihrer Wirksamkeit zu bewerten. Daraus ergibt sich für die Ausgestaltung der IT-Prozesse die Anforderung, dass Daten ordnungsmäßig verarbeitet werden und die Integrität der Daten jederzeit gewährleistet werden kann.[52]

Sichere IT-Systeme sind folglich auch eine Anforderung des SOA. Es lassen sich allerdings wenige konkrete Anforderungen an die IT herausfiltern. Der SOA fordert in der IT (wie auch in allen für die Finanzberichterstattung relevanten Bereichen des Unternehmens) ausführliche Prozessdokumentationen und Beschreibungen der in den Prozessen verankerten Kontrollen. Diese Kontrollen müssen hinsichtlich ihrer Eignung, ein adressiertes Risiko zu minimieren (Test of Design) bewertet werden. Zudem ist ihre Funktionsfähigkeit (Test of operating effectiveness) zu überprüfen. Die Effektivität der Kontrollen muss durch CEO und CFO bestätigt werden und ist durch den Abschlussprüfer zu kontrollieren.

Der SOA erhöht folglich die Anforderungen an die Dokumentation der Sicherheitsvorkehrungen der IT-Landschaft. Die sog. IT General Controls müssen im Unternehmen implementiert sein, um weit verbreitete Sicherheitsrisiken im IT-Bereich zu minimieren. Hervorzuheben ist die erweiterte Haftung des Managements bei mangelhaften internen Kontrollen.

2.3 Verlautbarungen mit Bezug zur IT-Sicherheit

2.3.1 Mindestanforderungen an das Risikomanagement (MaRisk)

Mit den MaRisk konkretisiert die BaFin ihre Anforderungen an das Risikomanagement im Finanzsektor. Darin konsolidiert die BaFin die Anforderungen aus den älteren Ver-

51 Vgl. Foit, Mihael: Management operationeller IT-Risiken in Banken, a. a. O., S. 98 ff.

52 Vgl. o. V.: CIOs liefern Tools für die Risikovorsorge, in: Computerwoche, 27/2005, S. 31.

öffentlichungen der Mindestanforderungen an das Kreditgeschäft (MaK), den Mindestanforderungen an das Handelsgeschäft (MaH) und Mindestanforderungen an die interne Revision (MaIR). Die im Dezember 2005 veröffentlichte endgültige Fassung der MaRisk ist ab 2007 rechtlich bindend.[53]

Inhaltlich beziehen sich die MaRisk auf die im KWG[54] verwendeten Begriffe „ordnungsmäßige Geschäftsorganisation“ und „angemessene interne Kontrollverfahren“. Zudem setzen die MaRisk Teile der zweiten Säule von Basel II[55] in deutsches Recht um. Die Anforderungen der MaRisk gelten als zentraler Bestandteil der qualitativen Bankenaufsicht in Deutschland und stellen die Abkehr von der bisher regelungsorientierten Aufsicht hin zu einem prinzipien-basierten Ansatz dar. Dadurch werden den Instituten Handlungsspielräume eröffnet, gleichzeitig aber auch deren Eigenverantwortung gestärkt und betont.[56]

Die MaRisk sind modular aufgebaut. Der allgemeine Teil (AT) enthält grundlegende Prinzipien, der besondere Teil (BT) umfasst die spezifischen Anforderungen an die Organisation des Kredit- und Handelsgeschäfts beziehungsweise die Identifizierung, Beurteilung, Steuerung sowie die Überwachung und Kommunikation von Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken sowie operationellen Risiken.[57] Im allgemeinen Teil zum Risikomanagement fordern die MaRisk die Festlegung der Risikotragfähigkeit und die Definition einer Risikostrategie. Ein nach Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten angemessenes internes Kontrollsystem ist einzurichten. Zudem sind Aufbau- und Ablauforganisation zu definieren und zu

53 Vgl. Bundesanstalt für Finanzdienstleisungsaufsicht (Hrsg.): Anschreiben zum Rundschreiben 18/2005: Veröffentlichung der Endfassung der MaRisk, Online im Internet: http://www.bafin.de/schreiben/89_2005/051220.htm, 20.12.2005.

54 Vgl. Kapitel 2.2.2.

55 Vgl. Kapitel 2.2.3.

56 Vgl. Bundesanstalt für Finanzdienstleisungsaufsicht (Hrsg.): Anschreiben zum Rundschreiben 18/2005: Veröffentlichung der Endfassung der MaRisk, a. a. O.

57 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Rundschreiben 18/2005: Mindestanforderungen an das Risikomanagement, Online im Internet: http://www.bafin.de/rundschreiben/89_2005/051220.htm, 20.12.2005, AT 1.

koordinieren sowie Risikosteuerungs- und Risikocontrollingprozesse einzurichten. Ferner wird eine funktionsfähige Interne Revision verlangt.[58]

Im Bezug auf IT-Risiken müssen insbesondere die Abschnitte AT 7.2: Technisch-organisatorische Ausstattung und AT 7.3: Notfallkonzept beachtet werden. Allgemein hat sich die technisch-organisatorische Ausstattung an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten, der Strategie und der Risikosituation auszurichten. IT-Systeme müssen nach AT 7.2 die Integrität, Vertraulichkeit, Verfügbarkeit und Authentizität der Daten sicherstellen. Bei der Ausgestaltung der Systeme und Prozesse ist auf gängige Standards abzustellen, deren Eignung regelmäßig von fachlich und technisch qualifizierten Mitarbeitern zu prüfen ist. Das in AT 7.3 geforderte Notfallkonzept muss Pläne für die Geschäftsfortführung sowie Wiederanlaufpläne umfassen. Die Maßnahmen des Konzeptes müssen geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Überdies ist die Wirksamkeit der Notfallvorsorge regelmäßig in Notfalltests zu überprüfen.[59]

2.3.2 Prüfungsstandards des IDW

Das Institut der Wirtschaftsprüfer (IDW) konkretisiert in den Prüfungsstandards die gesetzlichen Anforderungen an die Rechnungslegungsinformationen der prüfungspflichtigen Unternehmen. Die Pflicht zur Prüfung des Jahresabschlusses ergibt sich aus den Vorschriften des HGB. Gleich mehrere Standards des IDW befassen sich entweder explizit mit der IT (IDW PS 330, IDW PS 880) oder haben indirekt Bezug zu Fragen der IT-Sicherheit (IDW PS 720). Die Prüfung bezieht sich jeweils auf die rechnungslegungsrelevanten IT-Systeme und –Prozesse.

Der IDW PS 330 - Abschlussprüfung bei Einsatz von Informationstechnologie - umfasst einen Teilbereich der Prüfung des IKS. Dabei werden die rechnungslegungsrelevanten Elemente der IT-Geschäftsprozesse, IT-Anwendungen und IT-Infrastruktur betrachtet und auf ihre Übereinstimmung mit gesetzlichen Anforderungen (insbesondere Ord-

58 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Rundschreiben 18/2005: Mindestanforderungen an das Risikomanagement, a. a. O., AT 4.

59 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Rundschreiben 18/2005: Mindestanforderungen an das Risikomanagement, a. a. O., AT 7.

nungsmäßigkeits- und Sicherheitsanforderungen) überprüft. Als Risikoindikatoren im Rahmen eines risikoorientierten Prüfungsansatzes werden folgende Punkte beachtet:

- Abhängigkeit der Untenehmen von der IT
- Änderungen in den Systemen
- Know-How und Ressourcen
- Ausrichtung der IT auf Geschäftsstrategien und Prozessanforderungen[60]

Diese Indikatoren stellen für den Prüfer Anhaltspunkte für mögliche Schadenspotenziale dar. Bei der Prüfungsdurchführung werden im Teilbereich Infrastruktur physische Sicherheitsmaßnahmen, logische Zugriffskontrollen, Datensicherungs- und Auslagerungsverfahren sowie Maßnahmen für den geordneten Regelbetrieb beurteilt. Zusätzlich sind die Verfahren für den Notfallbetrieb und die Maßnahmen zur Sicherung der Betriebsbereitschaft vom Prüfer einzubeziehen. Im Bereich Anwendungen werden die Programmfunktionen, Auswahl-/Entwicklungs- und Änderungsprozesse sowie die Implementierungsprozesse bewertet. IT-gestützte Geschäftsprozesse sind vor allem hinsichtlich ihrer Schnittstellen, der implementierten anwendungsbezogenen Kontrollen und Plausibilitätsprüfungen sowie der Programmparameter zu begutachten.[61] Die Programmfunktion von Standardanwendungen muss nicht für jedes Unternehmen neu geprüft werden, dass die jeweilige Software einsetzt. Softwarehersteller können ihre Produkte nach dem IDW PS 880 (Erteilung und Verwendung von Softwarebescheinigungen) vor dem Einsatz im Unternehmen einer Prüfung unterziehen.

Zusammenfassend kann festgestellt werden, dass die Anforderungen an die IT-Sicherheit im Rahmen des IDW PS 330 sich mit den Bereichen Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit befassen. Damit werden alle Teilbereiche des Konzeptes dualer Sicherheit behandelt. Als Prüfungsstandard gibt IDW PS 330 allerdings keine Hinweise für die Ausgestaltung, Einführung und den Betrieb sicherer IT-Systeme. Eine Prüfung der IT-Systeme nach IDW PS 330 bietet sich wegen des relativ geringen zeitlichen und finanziellen Aufwands im Gegensatz zu den

60 Vgl. Institut der Wirtschaftsprüfer (Hrsg.): IDW-Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330), WPg 2002, Heft-Nr. 21/2002, S. 1167ff, Kapitel 2.1, Tz. 18.

61 Vgl. Institut der Wirtschaftsprüfer (Hrsg.): IDW-Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330), a. a. O., Kapitel 3.

umfassenden Sicherheitszertifikaten wie BS 7799 (bzw. ISO 27001) und dem Grundschutzzertifikat ggf. für kleinere Institute an.

Als weitere Verlautbarung des IDW ist die Stellungnahme IDW RS FAIT 1 - Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie - zu beachten. Darin werden Sicherheitsanforderungen an alle mit der Rechnungslegung in Verbindung stehenden Hard- und Softwarekomponenten formuliert. Sie umfassen die gleichen Sicherheitsanforderungen wie IDW PS 330 (Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit).[62] In der Stellungnahme wird gefordert, dass die IT-Strategie eng mit der Unternehmensstrategie abgestimmt wird, um Risiken frühzeitig zu erkennen. „IT-Risiken können für Unternehmen, deren Geschäftstätigkeit weitgehend von der IT abhängt, bestandsgefährdend sein."[63] Der großen Bedeutung der IT-Risiken trägt das IDW damit Rechnung, dass für sechs Elemente des IT-gestützten Rechnungslegungssystems Anforderungen formuliert werden:

- **IT-Umfeld und IT-Organisation:** Ein geeignetes IT-Umfeld umfasst eine angemessene Grundeinstellung zum Einsatz von IT sowie das zugehörige Risikobewusstsein. Die Überwachung der IT-Strategie durch entsprechende Kontrollen ist Aufgabe der gesetzlichen Vertreter. Zudem wird eine funktionale Trennung innerhalb der IT und zu anderen Fachabteilungen gefodert.
- **IT-Infrastruktur:** Technische Ressourcen und Verfahren sollen insbesondere die Verfügbarkeit und die Integrität der IT sichern. Dies umfasst physische Sicherheitsmaßnahmen, logische Zugriffskontrollen sowie Datensicherungs- und Auslagerungsverfahren. Zudem ist neben dem geordneten Regelbetrieb auch ein Vorgehen für Notfälle mit dokumentierten Wiederanlaufplanungen zu erstellen.
- **IT-Anwendungen:** Eingabe-, Verarbeitungs- und Ausgabekontrollen sichern als anwendungsbezogene Überwachungsmaßnahmen die Ordnungsmäßigkeit hinsichtlich der Buchführung. Zudem sind Verfahren für die Entwicklung von Individualsoft-

62 Vgl. Institut der Wirtschaftsprüfer (Hrsg.): IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), WPg 2002, Heft-Nr. 21/2002, S. 1157 ff, Tz. 23.

63 Institut der Wirtschaftsprüfer (Hrsg.): IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), a. a. O., Tz. 76.

ware, die Beschaffung von Standardsoftware sowie die Test- und Implementierungsprozesse zu etablieren.

- **IT-gestützte Geschäftsprozesse:** Sowohl bei funktionaler als auch bei geschäftsprozessorientierter Organisation sind IT-gestützte Kontrollen zu implementieren, die an die besonderen Anforderungen der Organisationsform angepasst sind.
- **Überwachung des IT-Kontrollsystems:** Funktionsfähigkeit und Angemessenheit der IT-Systeme werden kontinuierlich überwacht um die Wirksamkeit des IT-Kontrollsystems gewährleisten zu können.
- **IT-Outsourcing:** Bei der Auslagerung von Teilbereichen auf andere Unternehmen müssen auch die Auswirkungen auf die IKS beachtet werden.[64]

Auch diese zweite Verlautbarung des IDW umfasst alle im Konzept dualer Sicherheit enthaltenen Sicherheitsaspekte. Damit gehen die Ausführungen in ihrer Konkretisierung weit über die Inhalte der für die Abschlussprüfung relevanten Gesetzestexte hinaus. Dabei ist eine Prüfung allerdings immer eine ex-post stattfindende Maßnahme und kann nicht mit einer Risikoanalyse zum Aufbau eines ISMS verglichen werden. Die Erstellung eines Sicherheitskonzeptes (als Prozess) kann sich folglich nicht an Prüfungsstandards ausrichten. Dazu bieten sich verschiedene IT-Sicherheitsstandards an, die im folgenden Kapitel dargestellt werden.

2.4 IT-Sicherheitsstandards

2.4.1 BS 7799 / ISO 17799 / ISO 27001

Der Standard BS 7799 basiert auf der Arbeit des britischen Department of Trade and Industry (DTI) Commercial Computer Security Centre (CCSC). Eine der Schwerpunktaufgaben des CCSC war die Aufstellung des sog. sog. „code of good security practice“.. Durch die Weiterentwicklung dieser Verhaltensrichtlinie durch das National Computing Centre (NCC) und führender Unternehmen und Organisationen wurde das

64 Vgl. Institut der Wirtschaftsprüfer (Hrsg.): IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), a. a. O., Kapitel 4.

Rahmenwerk zu einem aus Benutzersicht anwendbaren Standard weiterentwickelt und schließlich nach Überarbeitung durch das British Standard Institute (BSI[65]) als Standard BS 7799 Teil 1 (BS 7799-1) veröffentlicht. In der Überarbeitung des Jahres 1998 wurden neuere Entwicklungen im Bereich E-Commerce und mobiler Arbeitsplätze ergänzt und zudem „UK-spezifische Verweise“ entfernt um die internationale Akzeptanz des Standards zu erhöhen.[66]

Das wachsende internationale Interesse führte schließlich dazu, dass im Rahmen eines sog. „Fast Track“[67] der Standard BS 7799-1 in einen international verbindlichen Standard ISO 17799 („Code of Practice for Information Security Management“) überführt wurde. Teil 2 des britischen Standards (BS 7799-2) beschreibt die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS), die Gegenstand einer Zertifizierung sein können. Auch dieser Standard wurde 2005 in einen internationalen Standard, den ISO 27001 überführt. Eine Zertifizierung nach BS 7799-2 bzw. ISO 27001 kann ausschließlich durch entsprechend akkreditierte Stellen durchgeführt werden.[68] Durch die Übernahme der britischen Standards in international anerkannte Standards entstehen teilweise begriffliche Verwirrungen. Sowohl BS 7799-1 / ISO 17799 als auch BS 7799-2 / ISO 27001 sind inhaltlich bis auf unwesentliche redaktionelle Änderungen deckungsgleich. Mittelfristig ist zu erwarten, dass die Standards unter dem Dach einer ISO 27000er-Familie als ISO 27001 und ISO 27002 zusammengefasst werden.

65 Bei der Abkürzung BSI besteht die Gefahr der Verwechselung mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik. Die Abkürzung wird an dieser Stelle nur der Vollständigkeit halber erwähnt und findet in der vorliegenden Arbeit Verwendung für das Bundesamt für Sicherheit in der Informationstechnik.

66 Vgl. Völker, Jörg: BS 7799 – Von „Best Practice“ zum Standard – Secorvo White Paper – Informationssicherheits-Management nach BS 7799 im Überblick, Online im Internet: http://www.secorvo.de/whitepapers/secorvoo-wp10.pdf, 25.06.2006, S. 4.

67 Im Rahmen der „Fast-Track Procedure“ wird ein Standard mit Ausnahme einiger unbedeutender redaktioneller Änderungen in einem Eilverfahren übernommen („Fast Track“ kann aus dem Englischen wörtlich mit „Überholspur“ übersetzt werden).

68 BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hrsg.): Kompass der IT-Sicherheitsstandards – Ein Leitfaden für mittelständische Unternehmen, Stand März 2005, Online im Internet: http://www.bitkom.org/files/documents/BITKOM_ Broschuere_ Sicherheitsstandard_V1.1f.pdf, 25.06.2006, S 11 f.

BS 7799-1 / ISO 17799

Als Leitfaden zum Management von Informationssicherheit umfasst ISO 17799 gesammelte Empfehlungen zu Verfahren und Methoden der Informationssicherheit. Als Top-Down-Ansatz umfasst der Standard praxiserprobte „best-practice"-Empfehlungen, die von Unternehmen an deren jeweils spezifische Anforderungen anzupassen sind. ISO 17799 adressiert kein bestimmtes Sicherheitsniveau, so dass eine Verwendung in verschiedenen Branchen mit unterschiedlichen Sicherheitsbedürfnissen möglich ist. Bei der Auswahl der Maßnahmen gibt der Standard keine konkreten Sicherheitslösungen und technischen Implementierungen vor, sondern formuliert vielmehr kritische Erfolgsfaktoren, die bei der Etablierung eines ISMS zu beachten sind. Diese Erfolgsfaktoren werden in elf Managementgebiete unterteilt, die in der Folge kurz erläutert werden:[69]

Security Policy

Die Sicherheitspolitik umfasst die strategische Ausrichtung und die Dokumentation der Managementunterstützung in allen Bereichen der Informationssicherheit. Eine regelmäßige Pflege und Überarbeitung der Policy sichert deren Aktualität und Angemessenheit. Die Security Policy dokumentiert die Unterstützung der obersten Managementebene und unterstreicht die Wichtigkeit von Sicherheitsfragen für das Unternehmen. Sie ist an alle Mitarbeiter zu verteilen und von diesen gegenzuzeichnen.

Organization of information security

Im Unternehmen ist ein Rahmenwerk für die organisatorische Behandlung aller mit IT-Sicherheit in Verbindung stehenden Fragestellungen zu erstellen. Es umfasst Methoden, Verfahren und Prozesse zur Initiierung, Implementierung und Kontrolle von Informationssicherheit. Neben Verantwortlichkeiten und der (internen) organisatorischen Struktur ist auch der Zugriff durch Dritte im Rahmen von Outsourcingvereinbarungen zu adressieren.

Asset Management

Das Asset Management umfasst die Erhebung und Klassifizierung aller materiellen und immateriellen Werte. Zur Einordnung und Zuordnung in Sicherheitsmaßnahmen sollte ein Klassifikationsschema erarbeitet werden. Jeder Vermögensgegenstand ist zudem einem eindeutigen Eigner zuzuordnen.

69 Vgl. Völker, Jörg: BS 7799 – Von „Best Practice" zum Standard – Secorvo White Paper – Informationssicherheits-Management nach BS 7799 im Überblick, a a. O., S. 5 ff.

Human Resources Security

Die Reduzierung von Risiken aus dem „Faktor Mensch“ ist zentraler Ansatzpunkt dieses Managementgebietes. Daneben werden auch die Bereiche Diebstahl, Betrug und Missbrauch von Einrichtungen adressiert. Die Maßnahmen untergliedern sich in Regelungen für interne und externe Mitarbeiter sowie sonstige Auftraggeber und enthalten Regelungen bei Eintritt ins Unternehmen, für die Phase als Beschäftigter sowie für die Beendigung des Beschäftigungsverhältnisses. Beispielhaft seien als Regelungsgebiete die Sicherheitsklauseln in Personalverträgen, die Reaktion auf Sicherheitsvorfälle (Sanktionen) und standardisierte Vorgehensweisen bei Austritt aus dem Unternehmen (Deaktivierung von Benutzerkonten, Rückgabe von Zugangsberechtigungen) angeführt.

Physical and Environmental Security

Die Einrichtung von Sicherheitszonen dient als vorbeugende Maßnahme, um unberechtigten Zugang zu Gebäuden, Systemen und Informationen zu verhindern. Darin enthalten sind auch Maßnahmen die Verlust, Beschädigung und Kompromittierung von Wirtschaftsgütern verhindern sollen.

Communications and Operations Management

Die Kommunikation und Verwaltung von IT-Betriebsabläufen ist einer der umfassendsten Managementbereiche von ISO 17799. Hingewiesen wird auf Vorgehensverfahren und Zuständigkeiten, das Servicemanagement bei der Bereitstellung von Leistungen durch Dritte sowie die Schutzmaßnahmen vor Viren und anderen bösartigen Programmen (Malicicious Code). Durch Systemplanung und geregelte Abnahmen von Systemen ist eine Minimierung des Ausfallrisikos zu erzielen. Daneben behandelt der Managementbereich die Themengebiete Backup-Prozeduren und damit die Integrität und Verfügbarkeit von IT-Systemen, den Schutz von Informationen in Netzwerken und Infrastruktur (Datensicherheit und Logging), den Umgang mit Datenträgern sowie den damit zusammenhängenden Austausch von Daten und Software. Unautorisierte Aktivitäten sollen mit den getroffenen Maßnahmen erkannt werden. Zu beachten ist vor allem die vorbeugende und überwachende Wirkung, mit der der Verlust, die nicht autorisierte Modifikation sowie der Austausch von Informationen verhindert werden.

Access Control

Der Bereich Zugriffskontrolle bezieht sich auf die Bedeutung von Kontroll- und Überwachungsmaßnahmen für den Zugriff auf Informationen und Systeme. Darunter

fallen das Benutzermanagement, die Benutzerverantwortung sowie der allgemeine Systemzugriff und der Zugriff auf spezifische Anwendungen und Daten. Die Maßnahmen müssen geeignet sein, externe Angriffe zu identifizieren und abzuwehren. In diesem Zusammenhang müssen auch Sicherheitsaspekte des Mobile Computing und der Telearbeit einbezogen werden.

Informations systems acquisition, development & maintainence

Bei der Auswahl, Entwicklung und Wartung von IT-Systemen sind Sicherheitsanforderungen bereits in frühen Planungsphasen zu berücksichtigen. Insbesondere sind in den genannten Phasen negative Einflüsse auf Benutzerdaten zu verhindern, kryptographische Verfahren zu Sicherung von Vertraulichkeit, Integrität und Authentizität anzuwenden sowie der Schutz der Systemdateien sicherzustellen. Sicherheit ist in allen Entwicklungs- und Supportprozessen zu integrieren und darf nicht der Bequemlichkeit der Nutzer untergeordnet werden.

Information security incident management

Der Managementbereich wurde erst mit dem Release von 2005 in den Standard aufgenommen. Damit wird die Wichtigkeit von Prozessen zur Meldung, Behebung und Weiterverfolgung von Sicherheitsvorfällen herausgehoben. Insbesondere ist dabei die Beweissicherung zu beachten (Zurechenbarkeit).

Business Continuity Management

In der Notfallplanung sind präventive und reaktive Maßnahmen zu treffen, um kritische Geschäftsprozesse vor den Auswirkungen von Ausfällen und Katastrophen zu schützen.

Compliance

Compliance bezeichnet die Einhaltung von Regelungen und Gesetzen. Die Empfehlungen des Standards dienen der Vermeidung von Verletzungen jeglicher Gesetze zum Thema Informationssicherheit, der Sicherstellung der eigenen Regelungen (Policies) sowie die Optimierung des System-Audit.[70]

70 Zu allen elf angeführten Managementgebieten: Vgl. Völker, Jörg: BS 7799 – Von „Best Practice“ zum Standard – Secorvo White Paper – Informationssicherheits-Management nach BS 7799 im Überblick, a. a. O., S. 6 ff. Vgl. auch Münch, Isabel; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, a. a. O., S. 53 f.

BS 7799-2 / ISO 27001

Der britische Standard BS 7799-2 wurde im Oktober 2005 ebenfalls in den internationalen Standard ISO 27001 überführt. Dieser liefert einen systematischen Ansatz zum Management kritischer Informationen und ist stets im Zusammenhang mit den Managementgebieten aus ISO 17799 zu betrachten.[71]

ISO 27001 beschreibt das Vorgehen zur Implementierung eines ISMS. Dabei wird auf das aus anderen Qualitätssicherheitsstandards (z. B. der ISO 9000-Familie) bekannte Plan – Do – Check – Act (PDCA) Modell zurückgegriffen. Die PDCA-Vorgehensweise geht auf den amerikanischen Statistiker Deming zurück, der mit seiner Arbeit den heutigen Stellenwert des Qualitätsmanagement maßgeblich beeinflusst hat. Das Modell dient der strukturierten Vorgehensweise und damit als Mittel zum Zweck, der als „ökonomische Erzielung eines angemessenen Sicherheitsniveaus für die betrachteten IT-Systeme“[72] benannt werden kann.

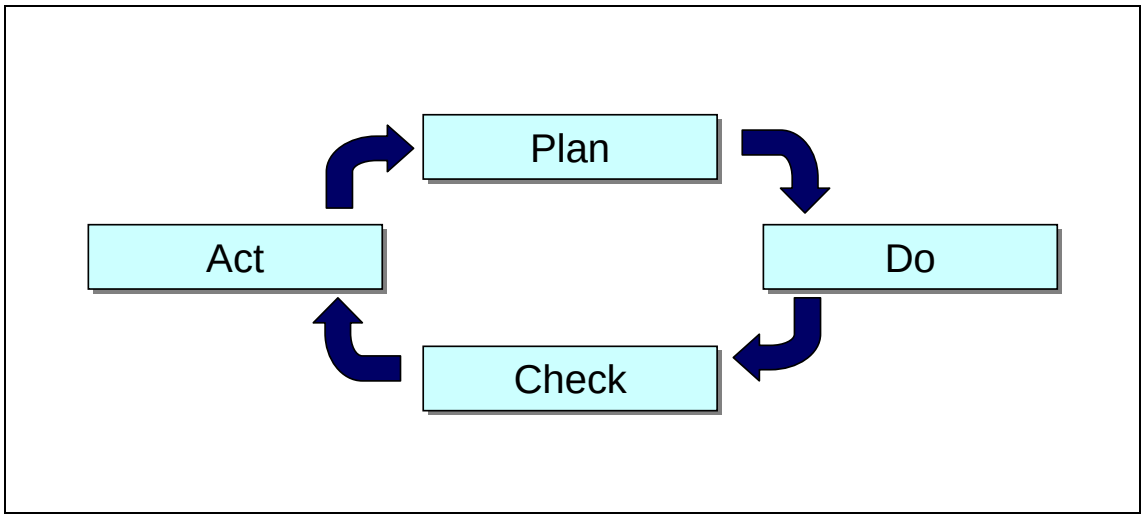

Abb. 4: Kontinuierlicher Verbesserungsprozess nach PDCA[73]

71 Vgl. International Standard Organization (Hrsg.): State-of-the-art information security management systems with new ISO/IEC 27001:2005 standard, Online im Internet: http://www.iso.org/iso/en/commcentre/pressreleases/archives/2005/Ref976.html, 24.05.2006.

72 Pohlmann, Norbert; Blumberg, Hartmut F.: Der IT-Sicherheitsleitfaden – Das Pflichtenheft zur Umsetzung von IT-Sicherheitsstandards im Unternehmen, Bonn: mitp 2004, S. 33.

73 Vgl. Becker, Peter: Prozessorientiertes Qualitätsmanagement, 4., vollständig überarbeitete Auflage, Renningen: expert 2005, S. 4.

Das in Abb. 4 dargestellt Vorgehensmodell der kontinuierlichen Prozessverbesserung wird in ISO 27001 auf die Managementgebiete des ISO 17799 angewendet und liefert damit die Basis für die Zertifizierung von ISMS.

Schwerpunkt der Planungsphase (*Plan*) ist die Etablierung einer Sicherheitspolitik mit Definition der strategischen Sicherheitsziele sowie die Einführungen von Prozessen und Abläufen, die Relevanz für das Risikomanagement besitzen. Das Risk Management ist zentraler Bestandteil des Vorgehens nach ISO 27001. Durch Identifizierung von Bedrohungen und Schwachstellen soll eine Auswahl geeigneter Maßnahmen getroffen werden um die Gefährdungen auf ein akzeptables Restrisiko zu minimieren. Im Rahmen des Risikomanagements sind folgende Prozessschritte zu durchlaufen:

1) Identifikation der Risiken
2) Bewertung der Risiken
3) Identifikation und Bewertung der Möglichkeiten, mit den Risiken umzugehen
4) Auswahl von Maßnahmenzielen und Maßnahmen
5) Erstellen eines Eignungsberichts
6) Zustimmung des Managements[74]

Die anschließende *Do*-Phase beinhaltet die Umsetzung der Planung. Die Sicherheitspolitik ist zu implementieren und angemessene Kontrollen sind umzusetzen. In der *Check*-Phase wird die Prozessperformanz den Sicherheitszielen gegenübergestellt. Darin sind Monitoringprozesse zur Erkennung von Prozessfehlern, Sicherheitslücken und Sicherheitsverletzungen ebenso enthalten wie ein regelmäßiges Review der Wirksamkeit des ISMS. Die *Act*-Phase dient der kontinuierlichen Verbesserung des ISMS und befasst sich mit der Korrektur und vorbeugenden Maßnahmen basierend auf den Erkenntnissen der vorangegangenen Prozessschritte. Es gilt geeignete korrigierende Maßnahmen zu ergreifen, die notwendigen Schritte abzustimmen und zu kommunizieren und daran anschließend erneut den Erfolg zu prüfen.[75]

74 Vgl. Völker, Jörg: BS 7799 – Von „Best Practice“ zum Standard – Secorvo White Paper – Informationssicherheits-Management nach BS 7799 im Überblick, a. a. O., S. 11 f.

75 Vgl. Völker, Jörg: BS 7799 – Von „Best Practice“ zum Standard – Secorvo White Paper – Informationssicherheits-Management nach BS 7799 im Überblick, a. a. O., S. 12 f.

Der Standard ISO 17799 (BS 7799-1) sowie die Möglichkeit zur Zertifizierung nach ISO 27000 (BS 7799-2) finden im Bankenumfeld durchaus Beachtung. ISO 17799 kann sowohl inhaltlich als auch strukturell wertvolle Anhaltspunkte für die Erstellung eigener Sicherheitsrichtlinien liefern. Sowohl technisch als auch organisatorisch gibt der Standard allerdings wenige bis keine konkreten Vorgaben zur Realisierung der Anforderungen. Die Managementbereiche liefern folglich lediglich ein Gerüst, auf dessen Basis eine individuelle Ausgestaltung erfolgen kann. Gegebenenfalls ist dabei auch auf weitere spezialisierte Sicherheitsrichtlinien zurückzugreifen.[76]

2.4.2 ISO/TR 13569

Als sog. Technical Report bietet der ISO/TR 13569 Orientierungshilfen für die Umsetzung eines Programms zur Informationssicherheit. Neben den Komponenten eines Sicherheitskonzeptes werden hier auch die Tätigkeitsprofile der an der Umsetzung beteiligten Mitarbeiter beschrieben. Der volle Titel des Reports in seiner aktuellen dritten Überarbeitung vom November 2005 lautet ISO/TR 13569:2005 – Financial services – Information security guidelines und ist bisher nur in englischer Sprache verfügbar.[77]

ISO/TR 13569 setzt folgende Ziele:

- Definition eines ISMS im Unternehmen
- Darstellung der Sicherheitsrichtlinie, Sicherheitsorganisation und der notwendigen Strukturen
- Hilfestellung bei der Auswahl angemessener Sicherheitskontrollen im Bankenbereich
- Unterstreichung der Notwendigkeit eines ISMS, um die Managementunterstützung bei der Adressierung rechtlicher und regulatorischer Anforderungen zu sichern

76 Vgl. Münch, Isabel; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, a. a. O., S. 54 f.

77 Vgl. Münch, Isabel; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, a. a. O., S. 56.

Dabei soll kein allgemeingültiges Lösungskonzept vorgeschrieben werden, sondern vielmehr ein Leitfaden für die Entwicklung eines angepassten Konzeptes dargestellt werden. Zur Erfüllung der aufsichtsrechtlichen Anforderungen muss eine *Information-Security-Policy* entwickelt werden. Sie soll neben den externen Anforderungen auch an die Geschäftsziele angepasst werden. Die *Policy* steht hierarchisch an der Spitze der Sicherheitsdokumentation des Unternehmens und enthält die klare Aussage, dass der Schutz und die Bereitstellung von Informationen Aufgabe und erklärtes Ziel der obersten Managementebene ist. Dieses Dokument ist allen Stakeholdern des Unternehmens zur Verfügung zu stellen. Auf Basis der allgemeinen Sicherheitspolitik werden Methoden (Practices) und Verfahren (Procedures) entwickelt, die der Durchsetzung der Sicherheitsziele dienen.[78]

Der Report enthält neben den Empfehlungen für Inhalt und Aufbau der oben genannten Dokumente Anregungen zur organisatorischen Verankerung der Informationssicherheit. Dabei wird vor allem das klare Bekenntnis aller Managementebenen zur Umsetzung der Sicherheitsrichtlinien eingefordert und das Rollenverständnis sowie die Verantwortlichkeit der einzelnen Ebenen festgeschrieben. ISO/TR 13569 liefert zudem Hinweise für die Risikoanalyse und die Auswahl und Implementierung von angemessenen Sicherheitskontrollen (bspw. zur Identifikation und Authentifizierung von Benutzern).[79]

ISO/TR 13569 stellt folglich eine praxisnahe und weitgehend konkretisierte Hilfestellung für die Implementierung eines Programms zur Informationssicherheit dar. Die im Anhang beigefügten Beispieldokumente helfen bei der Realisierung von Sicherheitskonzepten. Auch diese Dokumente und Handlungsempfehlungen müssen natürlich an das jeweilige Bankinstitut angepasst werden.[80]

78 Vgl. International Standard Organisation (Hrsg.): ISO/TR 13569 – Financial Services – Information Security Guidelines, Online im Internet (kostenpflichtig): www.iso.org, 25.05.2006, S. 11 ff.

79 Vgl. International Standard Organisation (Hrsg.): ISO/TR 13569 – Financial Services – Information Security Guidelines, a. a. O., 20 ff.

80 Vgl. Münch, Isabel; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, a. a. O., S. 57.

2.4.3 IT-Grundschutzhandbuch

Das BSI stellt generelle Informationen zur IT-Sicherheit zur Verfügung und kann als Dienstleister von anderen Bundesbehörden in Anspruch genommen werden. Als wichtigste Veröffentlichung des BSI ist das IT-Grundschutzhandbuch anzuführen, das Hinweise und Empfehlungen zu häufigen Gefährdungen weit verbreiteter IT-Komponenten und entsprechenden Gegenmaßnahmen in der IT beinhaltet.

Das Grundschutzhandbuch enthält als Bottom-Up-Ansatz Standardsicherheitsmaßnahmen, Umsetzungshinweise und Hilfsmittel für zahlreiche IT-Konfigurationen. Damit erleichtert das BSI den arbeitsintensiven Prozess der Erstellung eines Sicherheitskonzeptes und die aufwendige Analyse von Bedrohungen und deren Eintrittswahrscheinlichkeiten. Ersetzt wird diese Analyse durch das systematische Abarbeiten der Kataloge von Grundschutzmaßnahmen. Daraus resultiert auch der spezifische Vorteil des Grundschutzgedankens: der geringe Aufwand für die Erstellung eines Sicherheitskonzeptes und das Erreichen eines vorgegebenen Sicherheitsniveaus.[81]

Kritisch ist anzumerken, dass stets die Gefahr einer Über- oder Untersicherung besteht, da keine unternehmensspezifische Analyse der Gefährdungen vorgenommen wird. Weiterhin ist bei Einsatz neuer Techniken mit einer zeitlichen Verzögerung in der Überarbeitung der Grundschutzmaßnahmen zu rechnen. Im Rahmen des Grundschutzes erfolgt auch keine Differenzierung nach der individuellen Bedeutung eines IT-Systems für den Geschäftsbetrieb. Die Gefährdungskataloge des Grundschutzhandbuches enthalten keine Hinweise auf eine mit den Gefährdungen verbundene Eintrittswahrscheinlichkeit oder eine mögliche Schadenshöhe.[82]

Die Gefährdungskataloge stellen insgesamt eine wertfreie Sammlung häufiger Gefährdungen in ihrer Nutzung weit verbreiteter IT-Komponenten dar. Trotz der oben angeführten Kritik stellt das Grundschutzhandbuch einen akzeptierten Standard für die Entwicklung von Sicherheitskonzepten mit Grundschutz und Risikoanalyse dar. Der An-

81 Vgl. Hofmann, Marc: Management operationeller IT-Risiken im Kontext von Basel II, MaRisk und anderen aufsichtsrechtlichen Vorgaben, Hamburg: Dr. Kovac 2006, S. 69.

82 Vgl. Hofmann, Marc: Management operationeller IT-Risiken im Kontext von Basel II, MaRisk und anderen aufsichtsrechtlichen Vorgaben, a. a. O., S. 70.

spruch des BSI ist dabei, eine qualitativ hochwertige und stets aktuelle Sammlung der Gefährdungen bereitzustellen.[83]

Für das im Rahmen dieser Arbeit betrachtete Management von Risiken aus der IT ist der Grundschutzansatz des BSI nur eingeschränkt hilfreich. Bei der Untersuchung von Gefährdungen geben lediglich die fünf folgenden Gefährdungskataloge einen Anhaltspunkt zur Kategorisierung:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen[84]

Diese Kategorisierung ist nicht trennscharf. Die Ursache einer Gefährdung ist in der Realität meistens in verschiedenen Kategorien zu suchen. Vorsätzliche Handlungen werden oft nur durch organisatorische Mängel ermöglicht. Es ist zudem unklar, ob es sich bei der Kategorie um Ursache, Auslöser oder das Risikoereignis handelt.

2.5 Abgrenzung und Kategorisierung

2.5.1 Abgrenzung nach inhaltlicher Reichweite

Die im Rahmen dieses Kapitels behandelten Gesetze, Verlautbarungen und Standards unterschiedlicher Organisationen wurden vor unterschiedlichen Hintergründen verfasst und betrachten das Thema IT-Sicherheit folglich aus verschiedenen Perspektiven. Gesetze und Verlautbarungen zur IT-Sicherheit bleiben zu Fragen der technischen Sicherheit ausnahmslos sehr abstrakt. Nahezu alle ausführlichen Regelungen für den Bankbetrieb beziehen sich auf Fragestellungen der Bereiche Kreditabsicherung, Liquidität,

83 Vgl. Hofmann, Marc: Management operationeller IT-Risiken im Kontext von Basel II, MaRisk und anderen aufsichtsrechtlichen Vorgaben, a. a. O., S. 72.

84 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzhandbuch: Stand 2005, a. a. O., S. 16.

Transparenz und wirtschaftliche Kontrolle. Die Forderung nach *sicheren* IT-Systemen ist allerdings allen Regelungen gemein.

Um für die genannten Gesetze und Verlautbarungen eine erste Kategorisierung abzuleiten, werden sie inhaltlich am Konzept der dualen Sicherheit und den darin enthaltenen fünf Schutzzielen gemessen (siehe Tab. 2).

	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit	Rechtsverbindlichkeit
KonTraG					
KWG	X	X	X	X	X
Basel II			X		
BDSG	X			X	X
WpHG				X	X
SOA	X	X	X		
MaRisk	X	X	X		
IDW PS 330	X	X	X	X	X
IDW RS FAIT 1	X	X	X	X	X

Tab. 2: Reichweite von Gesetzen/Verlautbarungen im Konzept dualer Sicherheit

Das KonTraG formuliert keine konkreten Anforderungen an die IT-Sicherheit. Sein Ziel ist vielmehr die Einrichtung eines Risikofrüherkennungssystems, welches sinnvoll durch IT-Komponenten gestützt wird. Die Einrichtung eines Früherkennungssystems ist Teil der ordnungsmäßigen Geschäftsorganisation und gehört somit zu den allgemeinen Sorgfaltspflichten des Vorstands.

Das KWG ist im Bezug auf IT-Sicherheit wesentlich konkreter und die zugehörigen Kommentare leiten aus § 25a KWG zahlreiche Sicherheitsanforderungen bei Einsatz elektronischer Datenverarbeitung ab. Zusätzlich wird in § 25a Abs. 2 KWG die Auslagerung von Teilbereichen der IT (Outsourcing) behandelt. Sowohl für die eigenen als auch für die ausgelagerten IT-Systeme müssen alle fünf Schutzziele beachtet werden. Zur Kontrolle der Vorgaben hat die BaFin ein uneingeschränktes Einsichts- und Prüfungsrecht. Können die Anforderungen nicht erfüllt werden, drohen Sanktionen gemäß § 35 KWG. Zudem hat die BaFin zuletzt vermehrt ihr Veto bei Outsourcingvorhaben

eingelegt und damit gezielt bestimmte (IT-) Bereiche innerhalb des Kerngeschäfts der Finanzdienstleistungsinstitute als nicht auslagerungsfähig eingestuft.[85]

Der Baseler Ausschuss für Bankenaufsicht hat mit der neuen Eigenkapitalverordnung Basel II das Management operationeller Risiken in den Fokus der Banken gerückt. Die Forderung operationelle Risken - und als Teilmenge der operationellen Risiken auch IT-Risiken – mit Eigenkapital zu hinterlegen ist eine wesentliche Neuerung in Basel II. Die Zusammenhänge zwischen operationelle Risiken und IT-Risiken und damit der IT-Sicherheit müssen im Risikobewusstsein der Banken verankert werden. Im Rahmen der ersten Säule müssen für die ambitionierten Ansätze zur Berechnung der Eigenkapitalanforderungen (AMA = Advanced Measurement Approach)[86] leicht quantifizierbare Größen der IT-Sicherheit herangezogen werden. Diese leichte Messbarkeit erfüllt insbesondere der Bereich Verfügbarkeit, auf den sich Basel II in der ersten Säule konzentriert. Weitere Anforderungen von Basel II im Bereich Risikomanagements sind im deutschen Rechtsraum durch die MaRisk konkretisiert worden und werden weiter unten erläutert.

Das BDSG regelt den Umgang mit personenbezogenen Daten und deckt damit den Bereich „Sicherheit vor dem System“ und die darin enthaltenen Schutzziele Zurechenbarkeit und Rechtsverbindlichkeit ab. Betont wird vor allem, dass personenbezogene Daten nur auf Basis einer rechtlichen Grundlage zu erheben, zu verarbeiten und zu nutzen sind. Die Vertraulichkeit der Daten ist Basis für den verantwortungsvollen Umgang mit personenbezogenen Informationen.

Das WpHG beinhaltet Vorgaben zur IT-Sicherheit, die sich insbesondere auf Rollenkonzepte und Zugriffsrechte beziehen. Es wird ein Verzeichnis derjenigen Mitarbeiter gefordert, die Zugriff auf Insiderinformationen haben. Damit soll Insiderhandel verhindert werden bzw. der Zugriff auf die Informationen Personen zugeordnet werden können. Das WpHG umfasst somit die Schutzziele Zurechenbarkeit und rechtliche Verbindlichkeit.

85 Vgl. Prehl, Sabine: Outsourcing: Für Banken eine harte Nuss, a. a. O., S. 32.

86 Zu den verschiedenen Ansätzen zur Berechnung der Eigenkapitalanforderungen vgl. Hofmann, Marc: Management operationeller IT-Risiken im Kontext von Basel II, MaRisk und anderen aufsichtsrechtlichen Vorgaben, a. a. O., S. 100 ff.

Der SOA erweitert die Pflichten des Managements für in den USA börsennotierte Unternehmen. Insbesondere müssen CEO und CFO die Korrektheit der Angaben in der Finanzberichterstattung eidesstattlich erklären. Folglich müssen die IT-Prozesse eine ordnungsmäßige Verarbeitung der Daten und damit deren Integrität gewährleisten. Verfügbarkeit und Vertraulichkeit der Systeme sind ebenfalls notwendig.

In den MaRisk werden die Anforderungen der BaFin an das Risikomanagement formuliert und damit die zweite Säule von Basel II in deutsches Recht umgesetzt. Sowohl im allgemeinen als auch im besonderen Teil der MaRisk werden Anforderungen an die IT-Sicherheit gestellt. Die technisch-organisatorische Ausstattung hat sich dabei immer an den betriebsinternen Erfordernissen, der Strategie und der Risikosituation auszurichten. Von den MaRisk abgedeckt werden die Bereiche Integrität, Vertraulichkeit und Verfügbarkeit. Bei der Ausgestaltung sicherer IT-Systeme ist laut MaRisk auf gängige Standards abzustellen.

Die hier betrachteten Prüfungsstandards und Stellungnahmen des IDW (IDW PS 330, IDW PS 880, IDW RS FAIT 1) umfassen alle Bereiche des Konzeptes dualer Sicherheit. Es ist allerdings zu beachten, dass der Prüfer im Rahmen des risikoorientierten Prüfungsansatzes zunächst die Relevanz der IT-Systeme für die Rechnungslegung einschätzt. Er wird folglich keine Vollprüfung der IT durchführen.

Die im Kapitel 2.4 behandelten IT-Sicherheitsstandards nehmen für sich in Anspruch, alle Teilbereich der Sicherheit abzudecken. Sie unterscheiden sich lediglich in der Vorgehensweise und im Branchenfokus. Sowohl ISO 17799 als auch BS 7799-2 (ISO 27001) und dem Grundschutzhandbuch des BSI werden im Bereich Banken/Versicherungen eine hohe Relevanz bestätigt.[87]

2.5.2 Abgrenzung nach rechtlicher Verbindlichkeit

Die zweite vorzunehmende Kategorisierung ordnet die genannten aufsichtsrechtlichen Vorgaben den verschiedenen Sektoren der deutschen Bankenlandschaft zu. Die Bun-

87 Vgl. BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hrsg.): Kompass der IT-Sicherheitsstandards – Ein Leitfaden für mittelständische Unternehmen, a. a. O., S. 9.

desbank unterscheidet zunächst in Universalbanken und in Spezialbanken. Zu den Spezialbanken gehören auf der einen Seite bestimmte Hypothekenbanken und Schiffspfandbriefbanken sowie öffentlich-rechtliche Grundkreditanstalten. Auf der anderen Seite finden sich sog. Banken mit Sonderaufgaben, wie die Kreditanstalt für Wiederaufbau. Die Arbeit dieser Spezialbanken wird in teilweise sehr spezifischen Rechtsvorschriften geregelt. Deshalb werden sie im Rahmen dieser Arbeit nicht weiter betrachtet.

Universalbanken sind dadurch gekennzeichnet, dass sie alle in § 1 KWG genannten Bankgeschäfte durchführen. Hier wird weiter in drei Säulen unterschieden (siehe auch Abb. 5):

- **Kreditbanken** betreiben grundsätzlich alle Bankgeschäfte. Sie unterhalten Niederlassungen bzw. Repräsentanzen an den wichtigsten ausländischen Börsenplätzen und betreiben internationale Bankgeschäfte. Im Kreditgeschäft überwiegt das kürzerfristige Geschäft. Alle Arten von Wertpapiergeschäften werden durchgeführt und ein Großteil der Institute ist im Emissionsgeschäft tätig.
- **Sparkassen und Girozentralen** sind gemeinnützige Kreditinstitute mit gesetzlich festgelegtem öffentlichem Auftrag. Sie dienen der sicheren Geldanlage und fördern die Vermögensbildung der Bevölkerung. Oberstes Wirtschaftsprinzip ist nicht die Gewinnerzielung, sondern die Sicherung des Geschäftsbetriebs.
- **Kreditgenossenschaften und genossenschaftliche Zentralbanken** sind Kreditinstitute, die den Erwerb und die Wirtschaft ihrer Mitglieder mittels gemeinschaftlichen Geschäftsbetriebs fördern sollen. Sie sind einerseits „Banken für jedermann“, andererseits besonders den Mitgliedern verpflichtet, die das Eigenkapital aufbringen. Kreditgenossenschaften bemühen sich traditionell um die Betreuung des Mittelstandes. Zudem bieten sie ihren Kunden die Möglichkeit zur aktiven Mitbestimmung in der Generalversammlung und die Einflussnahme als zu wählendes Mitglied des Aufsichtsrates.[88]

88 Vgl. Grill, Wolfgang; Perczynski, Hans (Hrsg.): Wirtschaftslehre des Kreditwesens, 35., überarbeitete Auflage, Bad Homburg vor der Höhe: Gehlen 2001, S. 42ff.

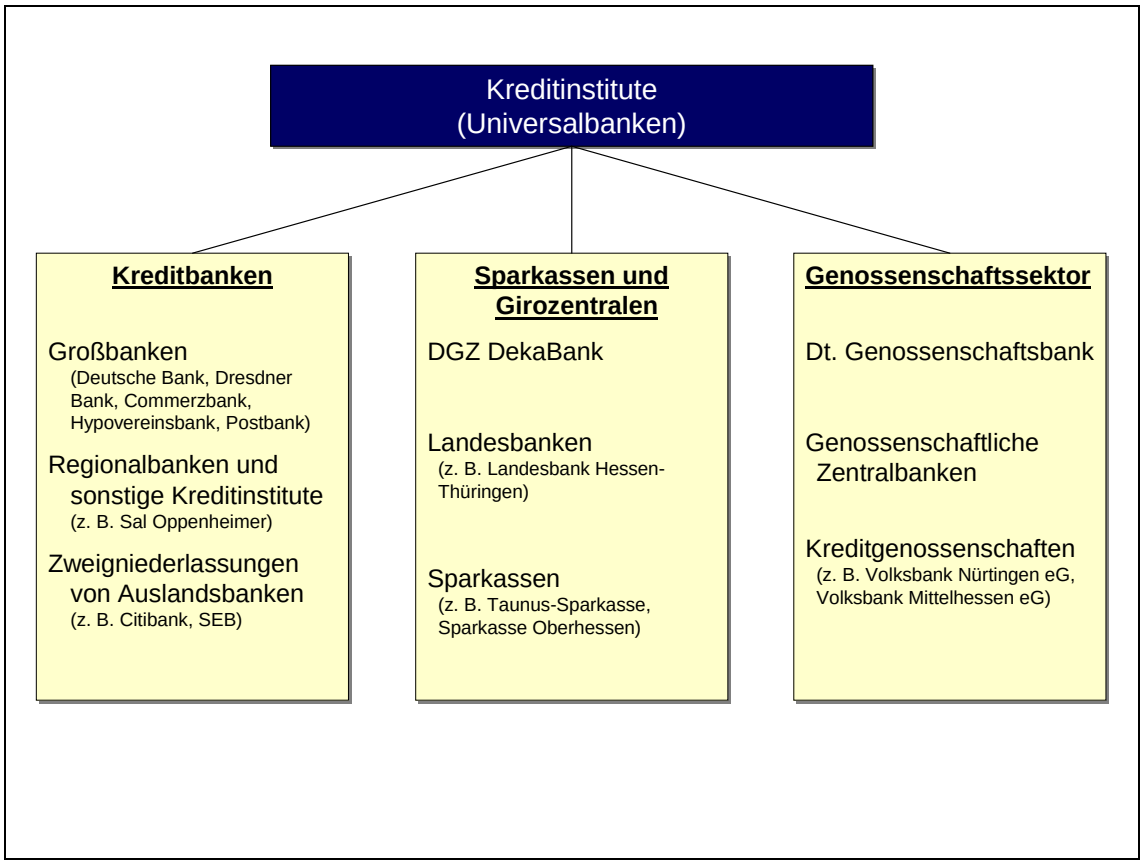

Abb. 5: Drei Säulen der deutschen Bankenlandschaft[89]

Um auf Grundlage der „Drei-Säulen"-Darstellung eine Kategorisierung vorzunehmen werden in der Folge zunächst die Vorgaben genannt, die alle Kreditinstitute erfüllen müssen. Anschließend erfolgt die Einteilung in mehreren Schichten, die unter anderem wesentlich von der Rechtsform und der Größe der betrachteten Institute abhängen. Dabei ist zu beachten, dass die Abgrenzung nicht an allen Stellen vollkommen trennscharf erfolgen kann. Eine grafische Darstellung der Ergebnisse zeigt Abb. 6.

Für alle Institute der deutschen Bankenlandschaft sind die Regelungen des KWG einschlägig (vgl. Anwendungsbereich §§ 1 Abs. 1, 1a, 1b KWG). Das KWG ist Grundlage der Bankenaufsicht in der Bundesrepublik. Ebenso müssen alle Institute die Regelungen des BDSG erfüllen, dass „für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch (…) nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen" gilt (§ 1 Abs. 2 BDSG). Aus der obigen Definition der Universalbanken ist zu

entnehmen, dass diese unter anderem dadurch charakterisiert werden, dass sie alle Bankgeschäfte ausführen. Folglich sind auch die Regelungen des WpHG zu beachten. Auch die Regelungen des neuen Baseler Eigenkapitalakkords sind von allen Instituten einzubeziehen. Die Umsetzung in nationales Recht erfolgt auf Basis der Capital Requirements Directive (CRD) in europäisches und darüber sukzessive in nationales Recht.

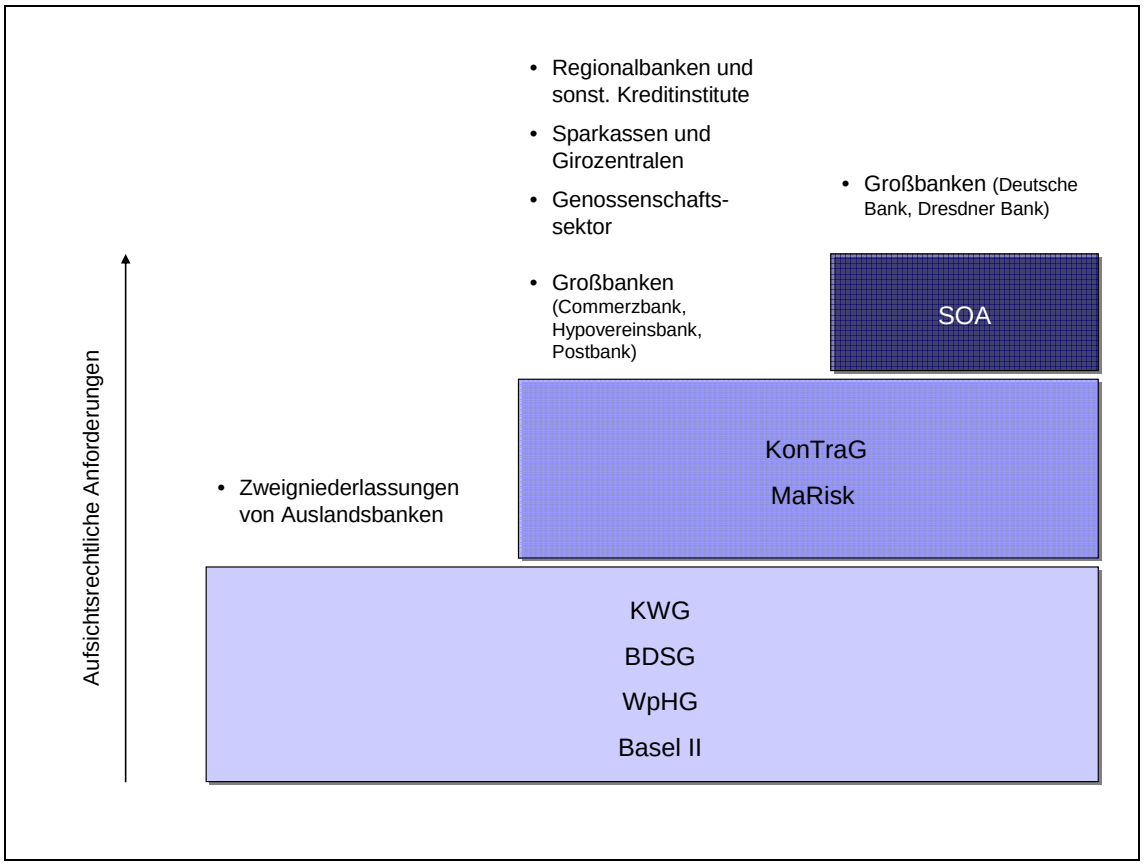

Abb. 6: Rechtliche Verbindlichkeit der Anforderungen

Es verbleiben die Regelungen des KonTraG, die MaRisk und der SOA. Davon ausgenommen sind (sofern die Muttergesellschaften nicht an einer US-Börse gelistet sind), die Zweigniederlassungen von Auslandsbanken.

Das KonTraG und die MaRisk sind durch den Fokus auf Risikomanagement und insbesondere Früherkennungssysteme für alle weiteren Institute zu beachten. Auch Unternehmen, die nicht in der Rechtsform der Aktiengesellschaft geführt werden haben diese

89 Vgl. Grill, Wolfgang; Perczynski, Hans (Hrsg.): Wirtschaftslehre des Kreditwesens, a. a. O., S. 43.

Regelungen zu beachten, da die Anforderungen den Begriff der „ordnungsmäßigen Geschäftsorganisation“ konkretisieren und damit eine Abstrahlwirkung auf andere Rechtsformen besitzen.

Es verbleibt schließlich der SOA mit seinen hohen Anforderungen an die Internen Kontrollsysteme und deren Dokumentation. Dem SOA unterliegen wegen des Listing an der New Yorker Wertpapierbörse NSYE die Deutsche Bank und die Dresdner Bank (als Konzerntochter der Allianz). Die anderen deutschen Großbanken haben „den Schritt nach New York“ noch nicht gewagt und sind deshalb von den weit reichenden Anforderungen bisher verschont geblieben.[90]

Die Prüfungsstandards des IDW sowie die diskutierten IT-Sicherheitsstandards können nicht sinnvoll in die obige Klassifizierung eingebracht werden. Der Wirtschaftsprüfer hat seine Prüfungshandlungen nach Art und Umfang der Geschäftstätigkeit anzupassen. Die Sicherheitsstandards sind in keiner Weise verpflichtend, sondern liefern lediglich Ansätze zur Realisierung sicherer IT-Systeme.

3 Risikomanagement

3.1 Zur Bedeutung des Risikomanagements

Die Internationalisierung der Kapitalmärkte und die Börsengänge der jüngeren Vergangenheit, die bei einem breiten Publikum das Interesse an Investitionen in Aktien geweckt haben, bringen für das Management der Aktiengesellschaften neue Pflichten mit sich. Insbesondere steht das Management in der Verantwortung, die Interessen der Eigenkapitalgeber als wichtigste Gruppe der Stakeholder stärker zu beachten.[91] Auch der teilweise Rückzug der Banken aus der Unternehmensfinanzierung und die daraus resultierende Kapitalmarktabhängigkeit der Unternehmen bringt – zusammen mit den zunehmenden gesetzlichen Anforderungen (z. B. KonTraG) – neue Impulse für das Risikomanagement. Um Anleger von einer Investition zu überzeugen, muss das systemati-

90 Vgl. o. V.: US-Listing: Einbahnstraße New York, a. a. O.

91 Vgl. Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc: Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, in: Controlling, 7/1999, S. 317.

sche Management von Chancen und Risiken zwangsläufig ein Bestandteil wertorientierter Unternehmenssteuerung in allen Branchen sein.[92] Die Erwartungen der Investoren beinhalten angemessene Erfolge und die damit verbundene Rentabilität der Investition in Form von Dividenden oder Kurssteigerungen möglichst ohne das Risiko von Kursverlusten oder dem Totalverlust.[93] Effektives Risikomanagement schafft Vertrauen und ist gleichzeitig eine wichtige Grundlage für den Erfolg eines Unternehmens. Durch Optimierung des Risiko-Chancen-Profils wird das Überleben am Markt gesichert.[94] Dagegen beinhaltet eine Insolvenz immer auch ein Scheitern des Risikomanagements.[95]

Die zunehmende Bedeutung des Risikomanagements ist offensichtlich. Die jüngeren Unternehmenskrisen in der Zeit nach KonTraG (Berliner Bankgesellschaft, Comroad, Flowtex) offenbaren erneut Schwächen in der Überwachung und Kontrolle der Unternehmen.[96] Aber nicht nur die klassischen Risikomanagementindustrien – Bankinstitute und Versicherungsgesellschaften – müssen sich mit der Thematik auseinandersetzen. Auch andere Industrien sehen sich vermehrt Situationen ausgesetzt, die neben bekannten Risikokategorien (Nichterfüllungs-, Marktpreis- und Wechselkursrisiko) bisher unterschätzte Risikosituationen enthalten. Die Terroranschläge von 11. September 2001 und die in letzter Zeit mit verheerenden Folgen aufgetretenen Naturkatastrophen bilden ein neues Feld des Risikomanagements.[97] Hier müssen neue Methoden des Risikomanagements angewandt werden, da Eintrittswahrscheinlichkeiten und Schadenshöhen in anderen Relationen zueinander stehen, als in den bisher bekannten Risikokategorien.

---

92 Vgl. Gehrke, Wolfgang: Das Pflichtenheft des Risikomanagements – Für eine vollständige Erfassung und Steuerung der Gesamtrisikoposition eines Unternehmens, in: Frankfurter Allgemeine Zeitung, 28.04.2003, S. 26

93 Vgl. Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc: Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, a. a. O., S 317.

94 Vgl. Romeike, Frank: Risiko-Management als Grundlage einer wertorientierten Unternehmenssteuerung, in: RATINGaktuell, 02/2002, S. 13.

95 Vgl. Gehrke, Wolfgang: Das Pflichtenheft des Risikomanagements – Für eine vollständige Erfassung und Steuerung der Gesamtrisikoposition eines Unternehmens, a. a. O., S. 26.

96 Vgl. Gehrke, Wolfgang: Das Pflichtenheft des Risikomanagements – Für eine vollständige Erfassung und Steuerung der Gesamtrisikoposition eines Unternehmens, a. a. O., S. 26.

97 Vgl. Brehmke, Kirsten; Meyer, Ralf: Strategisches Risikomanagement, in: Frankfurter Allgemeine Zeitung, 13.02.2006, S. 24.

Risikomanagement ist aber nicht nur Thema in kapitalmarktorientierten Unternehmen. In der Literatur besteht Einigkeit darüber, dass ein effizientes Risikomanagement auch Bestandteil der allgemeinen Sorgfaltspflicht des GmbH-Geschäftsführers ist.[98]

Das weite Feld des Risikomanagements wird in Kapitel 3.2 durch eine begriffliche Einführung in Risiko und Risikomanagement eröffnet. Daran schließt sich eine Kategorisierung der Risiken an. Ziel und Hauptteil dieses Kapitels ist die Darstellung des Risikomanagements in idealtypischer Form als permanenter, aktiver und systematischer Prozess.[99] Diese „best-practice" des Risikomanagement wird in Kapitel 3.3 abgebildet und ist die Grundlage für die Zusammenführung von IT-Sicherheit und Risikomanagement in Kapitel 4.

3.2 Risiko, Risikomanagement und Risikokategorien

Für den Terminus **Risiko** lassen sich in der Literatur vielfältige Definitionen finden. Angefangen vom sehr allgemein gehaltenen Verständnis des *„Risikos als Gefahr eines Verlustes oder Schadens"*[100] betonen andere Autoren den Zukunftsbezug im Rahmen der Entscheidungsfindung und verknüpfen beide Ansichten zum Risikobegriff als *„Gefahr einer Fehlentscheidung mit der Folge eines Schadens."*[101] Risiko als die *„Gefahr einer negativen Abweichung des tatsächlich erreichten Ergebniswertes vom erwarteten Ergebniswert"*[102] ist eine weitere allgemein gehaltene Begriffsbestimmung. Im mathematischen Gebrauch wird folgende Gleichung verwendet: *Risiko = Wahrscheinlichkeit x Schadensausmaß.*[103]

In Entscheidungsprozessen von Unternehmen ist bei der Wortbedeutung von Risiko jeweils das Eintreten bestimmter Umweltzustände und -ereignisse zu beachten. Risiken

98 Vgl. Romeike, Frank: Risiko-Management als Grundlage einer wertorientierten Unternehmenssteuerung, a. a. O., S. 13.

99 Vgl. Gehrke, Wolfgang: Das Pflichtenheft des Risikomanagements – Für eine vollständige Erfassung und Steuerung der Gesamtrisikoposition eines Unternehmens, a. a. O., S. 26.

100 Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, in: Risikomanagement, Hrsg.: Götze, Uwe; Henselmann, Klaus; Mikus, Barbara, Heidelberg: Physica 2001, S. 5.

101 Mag, Wolfgang: Unternehmensplanung, München: Vahlen 1995, S. 13.

102 Romeike, Frank: Lexikon Risikomanagement, Köln: Wiley 2004, S. 102.

103 Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 102.

sind an Entscheidungen gebunden und resultieren aus der Unsicherheit bei der Alternativenwahl. Risiken bringen aber nicht nur die eigentlichen Entscheidungsfindungen mit sich. Auch die Realisierung der ausgewählten Alternative ist regelmäßig mit bestimmten Risiken behaftet. Neben der Unsicherheit bei Entscheidungen wird im Unternehmensumfeld auch das menschliche Fehlverhalten als Risikoursache angeführt. Entscheidungsfindung und der Faktor „Mensch" finden sich in den Definitionen vom (1) Risiko als die *„Gefahr, dass Ereignisse und Handlungen ein Unternehmen daran hindern, seine Ziele zu erreichen bzw. seine Strategien erfolgreich umzusetzen"*[104] bzw. (2) Risiko als die *„Möglichkeit eines Schadens oder Verlustes als Konsequenz eines bestimmten Verhaltens oder Geschehens; dies bezieht sich auf die Gefahrensituationen, in denen nachteilige Folgen eintreten können, aber nicht müssen."*[105] Das unter (2) angeführte Begriffsverständnis bildet die Grundlage für die weiteren Ausführungen dieser Arbeit.

An den vorangegangenen Definitionen wird insofern Kritik geübt, als dass ausschließlich negative Abweichungen einbezogen werden. Im weiteren Sinne sind unter Risiken neben negativen auch positive Abweichungen (= Chancen) zu verstehen. Zum Ausdruck kommt dies bspw. wenn man vom Risiko als *„mögliche Abweichung von den den Unternehmenszielen zu Grunde liegenden Erwartungen"*[106] spricht. Da im Rahmen der in Kapitel 2 dargestellten Vorgaben zur IT-Sicherheit ausschließlich ungünstige Änderungen von Umweltzuständen beachtet werden, soll in der vorliegenden Arbeit der Chancenaspekt zwar nicht vollständig ignoriert, im Hinblick auf das hier dargestellte Grundverständnis von Risiko aber ausgeklammert werden. Werden ausschließlich negativen Abweichungen betrachtet wird der Terminus *reines Risiko* verwendet, während bei Einbeziehung von Chancen die Bezeichnung *spekulatives Risiko* gebraucht wird.[107] Reine

104 O. V.: Integriertes Risikomanagement, Online im Internet: http://www.kpmg.de/library/pdf/irm.pdf, S. 5, 25.06.2006.

105 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 102.

106 Huch, Burkhard; Tecklenburg, Thilo: Risikomanagement in der Bauwirtschaft, in: Risikomanagement, Hrsg.: Götze, Uwe; Henselmann, Klaus; Mikus, Barbara, Heidelberg: Physica 2001, S. 303.

107 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 7.

Risiken (wie z. B. Brandrisiken, Haftpflichtrisiken) können im Gegensatz zu spekulativen Risiken (z. B. das allgemeine Unternehmerrisiko) überwälzt werden.[108]

Management wird im funktionalen Sinn als Planung, Organisation, Führung und Kontrolle verstanden.[109] **Risikomanagement** kann in diesem einfachen Wortverständnis als Steuerung und Führung von Risiken bezeichnet werden, welche von einem effizienten Risikocontrolling zu unterstützen sind.[110] Dabei stellen die Unternehmen auf alle potenziellen Risiken ab, die die Vermögens-, Finanz- und Ertragslage des Unternehmens mittel- oder langfristig gefährden können. Ziel des Risikomanagements ist die Sicherung des Fortbestands des Unternehmens, die Absicherung des Unternehmens gegen störende Ereignisse sowie die Steigerung des Unternehmenswertes.[111]

Die Ursprünge des Risikomanagements sind in der Versicherungswirtschaft zu suchen. Beim Schutz von Vermögenswerten war es die primäre Aufgabe des Risikomanagements, die Höhe der zu zahlenden Prämien optimal zu gestalten. Behandelt wurden hier nur die reinen Risiken (nur reine Risiken sind versicherbar). Spekulative Risiken wurden ausgeklammert. Ergänzt um systematische Risikoanalysen und Maßnahmen zur Schadensverhütung wurde das Konzept zum *speziellen Risikomanagement* erweitert, welches auch als Risikomanagement im engeren Sinne bezeichnet wird. Es befasst sich mit der Sicherung gegen negative Veränderungen der Rahmenbedingungen der unternehmerischen Tätigkeiten und erhöht durch Beeinflussung von Risikoursachen und -wirkungen den Zielerreichungsgrad. Allerdings beschränkt sich das Risikomanagement weiterhin nur auf ein Teilgebiet der tatsächlich existierenden Risiken: die reinen Risiken sowie die Risiken *einer* Entscheidung, die sog. Einzelrisiken.[112]

---

108 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 101. Die risikopolitische Handlungsalternative „Überwälzen“ wird in Kapitel 3.3.4 dieser Arbeit näher erläutert.

109 Vgl. Staehle, Wolfgang H.; Conrad, Peter; Sydow, Jörg: Management – Eine verhaltenswissenschaftliche Perspektive, 8. Auflage, München: Vahlen 1999, S. 71.

110 Vgl. Biermann, Bernd: Modernes Risikomanagement in Banken, in: Eller, Roland; Gruber, Walter; Reif, Markus (Hrsg.): Handbuch des Risikomanagements: Analyse, Quantifizierung und Steuerung von Markt-, Kredit und operationellen Risiken, 2., überarbeitete und erweiterte Auflage, Stuttgart: Schäffer-Poeschel 2002, S. 121.

111 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 119.

112 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 10.

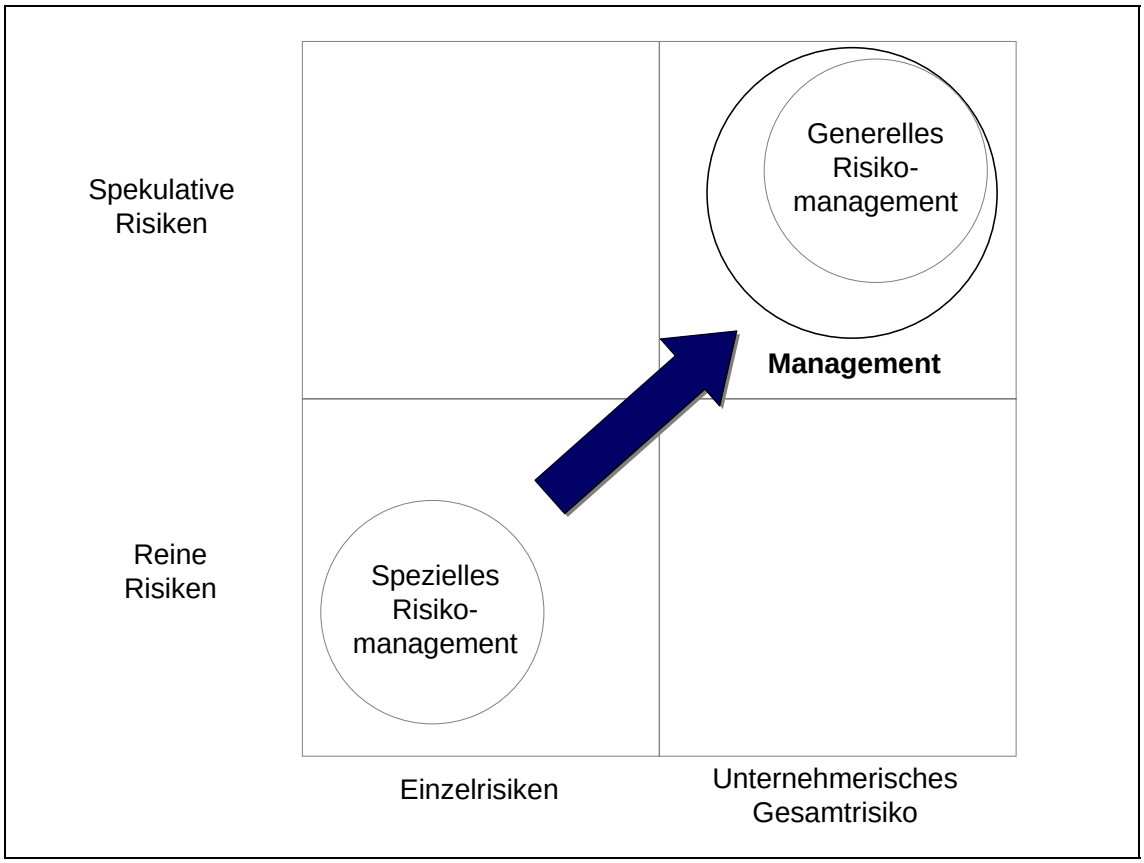

Abb. 7: Risikoarten und Risikomanagement-Konzepte[113]

Die Beschränkung auf bestimmte Risiken ist aus verschiedenen Gründen nicht sinnvoll. Zunächst sind dazu Probleme bei der Klassifizierung von Risiken anzuführen. Daneben finden sich aber auch zahlreiche Problemfelder, in denen reine und spekulative Risikobestandteile parallel auftreten. Die Fokussierung auf die negativen Auswirkungen und damit die Ausgrenzung von Chancenaspekten würde zudem den Schluss zulassen, dass sämtliche Risiken zu vermeiden sind. Eine Fokussierung auf Einzelrisiken verhindert die Beachtung von Risikozusammenhängen im Unternehmen. Um diesen Kritikpunkten am reinen Risikomanagement zu begegnen ist ein ganzheitlicher Ansatz des Risikomanagements entwickelt worden, der auch als *generelles Risikomanagement* bezeichnet wird. Diese weitere Konzeption des Risikomanagements ist eng mit der allgemeinen

113 Vgl. Marcharzina, Klaus; Wolf, Joachim: Unternehmensführung: das internationale Managementwissen; Konzepte – Methoden – Praxis, a. a. O., S. 655. Um einheitliche Begriffe zu verwenden wird in der Abbildung „strategisches Risikomanagement“ durch „generelles Risikomanagement“ sowie „traditionelles Risikomanagement“ durch „spezielles Risikomanagement“ ersetzt.

Unternehmensführung verbunden.[114] Da letztlich für den Gesamterfolg des Unternehmens vor allem das Gesamtrisiko und weniger das Einzelrisiko von Bedeutung ist, muss sich das Risikomanagement besonders auf die Steuerung des Gesamtrisikos konzentrieren.[115]

Effektives Risikomanagement verhindert im Idealfall durch die explizite Einbeziehung von Chancen- und Risikoaspekten in allen Entscheidungssituationen, dass Unternehmen in Krisensituationen geraten. Es dient damit der Sicherung des Fortbestands des Unternehmens. Als weitere Funktionen des Risikomanagements ist die Etablierung eines Risikobewusstseins bei den Mitarbeitern anzuführen. Zudem müssen einzelne Entscheidungen zur Optimierung des Gesamtrisikos des Unternehmensportfolios getroffen werden. Des Weiteren ist das Risikomanagement verantwortlich für die Bildung von Systemen, die Informationen zur Entscheidungsfindung sammeln und aufbereiten. Die Bereitstellung von Verfahren und Instrumenten zur Einbeziehung von Unsicherheitsfaktoren ist ebenfalls Aufgabe des Risikomanagements.[116] Die angeführten Aufgaben und Konzepte führen zum Verständnis des Begriffs Risikomanagement, das in dieser Arbeit Verwendung findet:

„Unter Risikomanagement wird der planvolle Umgang mit Risken in einem Unternehmen verstanden.“[117]

Dabei ist Risikomanagement als permanenter, aktiver und systematischer Prozess im Sinne eines Regelkreises zu verstehen.[118]

Bevor im folgenden Kapitel der Prozess des Risikomanagements detailliert beschrieben wird, müssen relevante Risikokategorien gegeneinander abgegrenzt werden. Die Risikoklassifikation dient der groben Vorstrukturierung von Risiken und ist als Grundlage für die Risikobewertung zu verstehen. Die Abgrenzung der Kategorien ist auf Grund der

114 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 11 f.

115 Vgl. Marcharzina, Klaus; Wolf, Joachim: Unternehmensführung: das internationale Managementwissen; Konzepte – Methoden – Praxis, 5., grundlegend überarbeitete Auflage, Wiesbaden: Gabler 2005, S. 653.

116 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 11f.

117 Vgl. Brehmke, Kirsten; Meyer, Ralf: Strategisches Risikomanagement, a. a. O., S. 24.

118 Vgl. Gehrke, Wolfgang: Das Pflichtenheft des Risikomanagements – Für eine vollständige Erfassung und Steuerung der Gesamtrisikoposition eines Unternehmens, a. a. O., S. 26.

Vielschichtigkeit und Komplexität, die aus unterschiedlichsten Risikosituationen entsteht, nicht unproblematisch. Unternehmensrisiken können prinzipiell in drei Teilbereiche eingeordnet werden:

- Risiken des leistungswirtschaftlichen Bereichs: Beschaffungs-, Produktions-, Absatz und Technologierisiken
- Risiken des finanzwirtschaftlichen Bereichs: Ausfall-, Zins-, Liquiditäts- Marktpreis-, Kapitalstrukturrisiken sowie politische Risiken
- Risiken aus Corporate Governance, Management etc.: Organisation, Führungsstil, Unternehmenskultur, Personal[119]

Die genannten Risiken können des Weiteren von internen oder externen Ereignissen und Störungen verursacht werden. Die genannte Risikokategorisierung lässt sich auf verschiedenste Branchen beziehen. Für den in dieser Arbeit betrachteten Finanzdienstleistungssektor ist die Einteilung aber weniger geeignet.

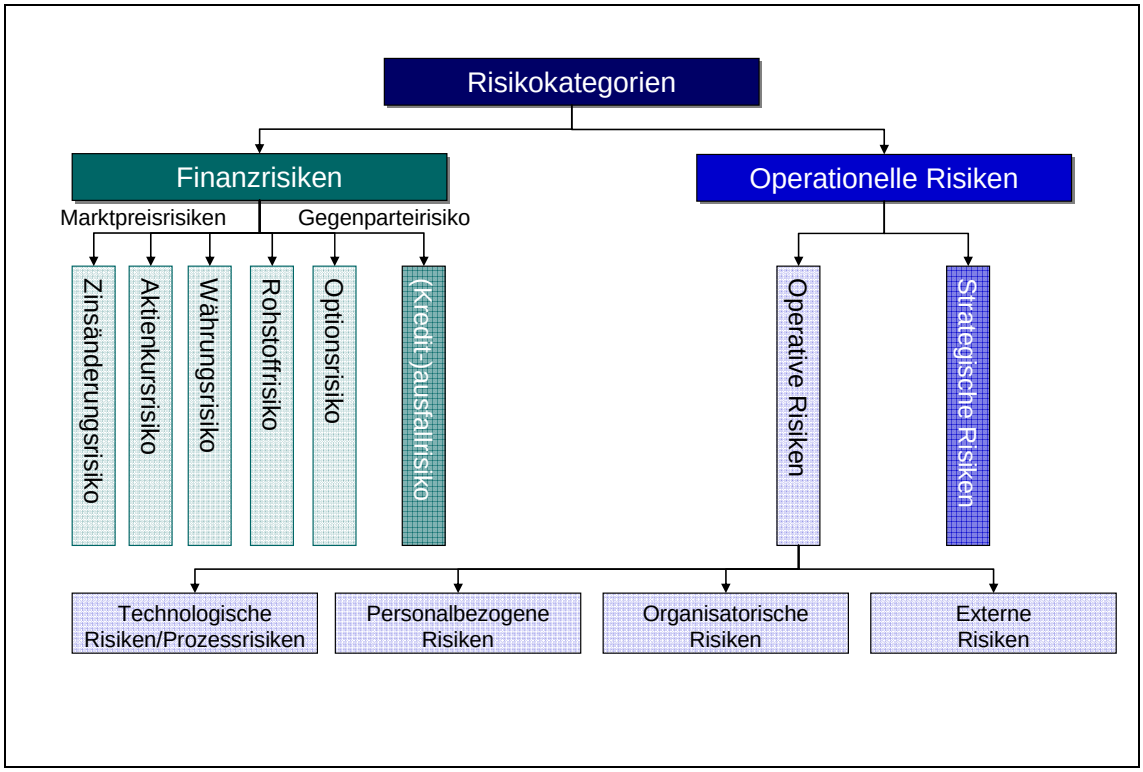

Abb. 8: Risikokategorisierung[120]

119 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 110f.

Die Risikokategorien in Abb. 8 liefert einen Überblick der verschiedenen Risikoarten im Bankensektor. Insbesondere die Trennung in Finanzrisiken und operationelle Risiken führt bereits zu einer Risikokategorisierung, auf die der Baseler Eigenkapitalakkord hinweist (siehe Abb. 9).

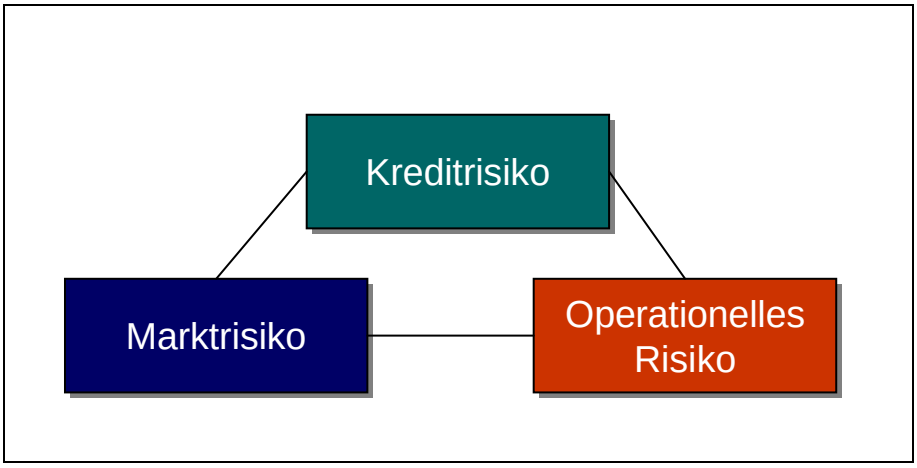

Abb. 9: Risikokategorisierung für Eigenkapitalanforderung in Basel II

Die drei Risikokategorien von Basel II beinhalten im Einzelnen:

- *Kreditrisiko*: Das mit dem Verleihen von Geld verbundene Risiko des Gläubigers, dass die Gegenpartei (der Schuldner) ausfällt und somit zur Rückzahlung des Kredits nicht mehr fähig ist.[121]
- *Marktrisiko*: Die Gefahr, dass bestehende Aktiva aufgrund negativer Entwicklungen des Marktes (bspw. Aktienmärkte, Gold- oder Rohstoffmärkte) an Wert verlieren und der Risikoträger als Eigner des jeweiligen Aktivums einen Verlust erleidet.[122]
- *Operationelles Risiko*: Von innen und außen kommende Störungen, die das Unternehmen bei der Erbringung der Leistungen behindern können.[123] Diese Risikokategorie umfasst technische und personelle Risiken sowie Ablauf-, Rechts-, Ver-

120 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 111.

121 Vgl. Romeike, Frank: Die ältesten Risiken der Welt, in: RiskNews, 01/2004, S. 16.

122 Vgl. Romeike, Frank: Die ältesten Risken der Welt, a. a. O., S. 16.

123 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 88.

trags- und Beratungsrisiken.[124] Die Definition aus Basel II lautet: „Operationelles Risiko ist die Gefahr von Verlusten, die infolge einer Unzulänglichkeit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten. Diese Definition schließt Rechtsrisiken ein, nicht jedoch strategische Risiken oder Reputationsrisiken."[125]

Das Risikomanagement in Banken konzentrierte sich lange Zeit auf Markt- und Kreditrisiken. Durch die Aufnahme der operationellen Risiken in Basel II entsteht teilweise der Eindruck, dass es sich dabei um eine neue Risikokategorie handelt. Dem hält Romeike entgegen, dass operationelle Risiken schon immer existieren und führt dazu das biblische Beispiel der Sintflut und Noahs Risikomanagement (Bau der Arche) an.[126] Banken müssen folglich diese „neue" Risikokategorie aufnehmen und ebenso managen, wie die bisher primär betrachteten Markt- und Kreditrisiken. Wie der Risikomanagementprozess ausgestaltet sein sollte zeigt das nachstehende Kapitel 3.3.

3.3 Der Prozess des Risikomanagements

3.3.1 Risikomanagement: permanenter, aktiver und systematischer Prozess

Für die Ausgestaltung eines effizienten Risikomanagements sind in der Literatur verschiedene Phasenschemata entwickelt worden. Sie dienen dazu, systematisch potenzielle Risiken zu identifizieren, zu bewerten und darauf basierend adäquate Sicherungsmaßnahmen auszuwählen und zu realisieren.[127] Grundsätzlich ist der Prozess des Risikomanagements in vier Phasen unterteilt, die als Kreislauf in Abb. 10 dargestellt sind.[128]

---

124 Vgl. Mauch, Peter: Risikomanagement in Banken, in: Risikomanagement, Hrsg.: Götze, Uwe; Henselmann, Klaus; Mikus, Barbara, Heidelberg: Physica 2001, S. 338.

125 Baseler Ausschuss für Bankenaufsicht (Hrsg.): Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen – überarbeitete Rahmenvereinbarung (Juni 2004), a. a. O., S. 127.

126 Vgl. Romeike, Frank: Die ältesten Risiken der Welt, a a. O., S. 16f.

127 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 13.

128 Vgl. Krystek, Ulrich; Fiege, Stefanie: Risikomanagement, in: Gabler Wirtschaftslexikon, 16. vollständig aktualisierte und überarbeitete Auflage, Wiesbaden: Gabler 2004, S. 2558.

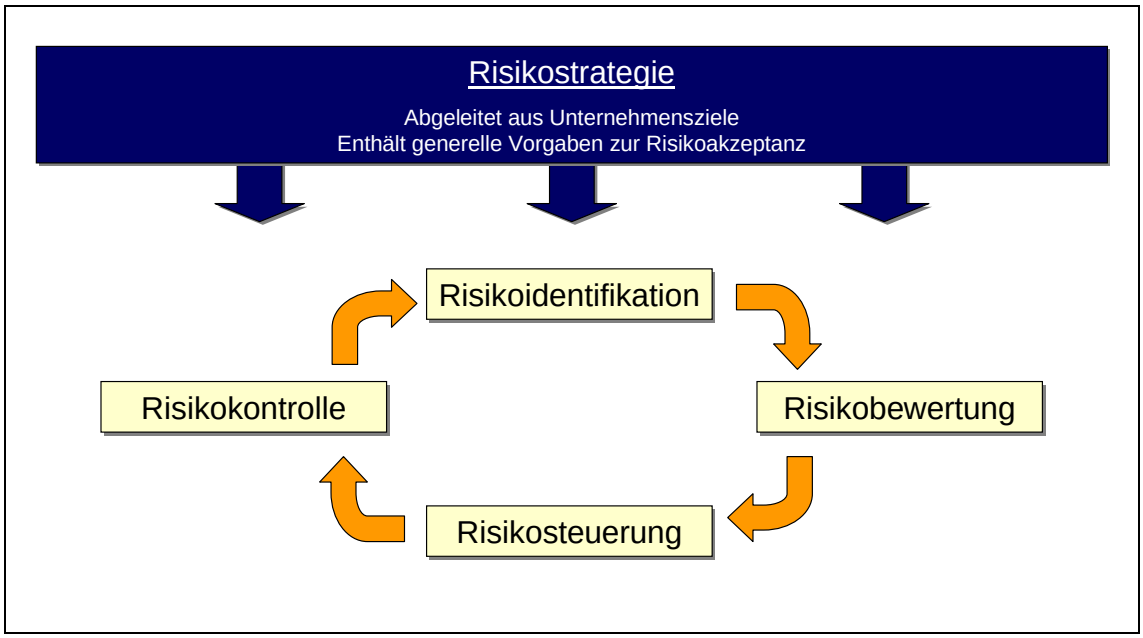

Abb. 10: Der Risikomanagement-Kreislauf

Grundlage für das Risikomanagement sind die Unternehmensziele und eine daraus abzuleitende *Risikostrategie*. Diese Risikostrategie beinhaltet die allgemeine Risikoakzeptanz des Unternehmens und definiert daraus Grundsätze für den Umgang mit Risiken - aber auch Chancen.[129] Im risikopolitischen Kontext ist die zu verfolgende Grundeinstellung (risikoneutral, risikofreudig, risikoscheu) festzulegen. Zudem werden Maßnahmen für die Verminderung, Begrenzung und Vermeidung von Risiken ausgewählt und die Möglichkeit der Externalisierung (Überwälzung) von Risiken einbezogen.[130] Für die operative Umsetzbarkeit der strategischen Ziele des Risikomanagements ist von großer Bedeutung, dass verständlich festgelegt wird, in welchem Verhältnis Chancen und Risiken eingegangen werden dürfen. Außerdem ist für unterschiedliche Hierarchiestufen eine maximal zu verantwortende Risikoausprägung zu quantifizieren.[131]

129 Vgl. Krystek, Ulrich; Fiege, Stefanie: Risikomanagement, a. a. O., S. 2558.

130 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 115 f.

131 Vgl. Krystek, Ulrich; Fiege, Stefanie: Risikomanagement, a. a. O., S. 2558.

3.3.2 Risikoidentifikation

Die Risikoidentifikation dient der möglichst vollständigen und kontinuierlichen Erfassung aller wesentlichen Risiken und Schadenspotenziale im Unternehmen. Dabei sind neben den aktuellen Risiken auch potenzielle und latente Risiken einzubeziehen. Die Aufnahme der Risiken ist die Informationsbasis für die nachfolgenden Schritte des Risikomanagementprozess.[132]

Die Informationsbeschaffung im Rahmen der Risikoidentifikation gilt als schwierigste Phase im gesamten Risikomanagementprozess. Sie erfordert eine systematische, prozessorientierte Vorgehensweise. Das Vorgehen kann nach Art des Wirtschaftens differieren. Mögliche Ansätze sind (1) eine Analyse ausgehend von den Risikokategorien (z. B. leistungswirtschaftliche, finanzwirtschaftliche, externe Risiken) oder (2) eine geschäftsfeldbezogene Untersuchung. Der dritte Ansatz sieht eine prozessorientierte Analyse der Risiken vor, die zwischen Kern- und Unterstützungsprozessen sowie Projekten unterscheidet.[133] Im Dienstleistungssektor und damit in den im Rahmen dieser Arbeit betrachteten Finanzdienstleistungsunternehmen scheint die prozessorientierte Vorgehensweise geeignet. Bei den identifizierten Risiken ist auch auf die Zusammenhänge zwischen den einzelnen Risiken zu achten.[134] Im Rahmen der Risikoanalyse haben sich Top-Down-gerichtete Ansätze bewährt, mit denen zunächst auf Vorstandsebene die möglicherweise bestandsgefährdenden Risiken betrachtet werden, um dann anhand der Wertschöpfungskette systematisch die Risiken in den Geschäftsprozessen zu analysieren. Nachfolgend gilt es, durch ungerichtete Suche Risiken zu identifizieren, die in den beiden ersten Phasen vernachlässigt wurden, um aus den drei Analysebereichen ein Gesamtbild der unternehmensweiten Risiken zu erhalten.[135]

Es existiert eine Vielzahl von Methoden für die Erfassung von Risiken. Dabei wird unterschieden zwischen den sog. Kollektionsmethoden, die sich zur Aufnahme von offensichtlich bestehenden Risiken eignen und den Suchmethoden, die im Rahmen eines pro-

132 Vgl. Krystek, Ulrich; Fiege, Stefanie: Risikomanagement, a. a. O., S. 2558.

133 Vgl. Romeike, Frank: Risiko-Management als Grundlage einer wertorientierten Unternehmenssteuerung, a. a. O., S. 15.

134 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 108.

aktiven Risikomanagements bisher unbekannte Risikopotenziale aufdecken sollen. In die Kategorie der Kollektionsmethoden fallen Checklisten, SWOT-Analysen, Interviews und Befragungen. Als Suchmethoden kommen im analytischen Bereich Fragenkataloge, Baumanalysen und morphologische Verfahren zum Einsatz, während in der kreativen Suche Techniken wie Brainstorming, die Delphi-Methode und die Synektik angewandt werden.[136]

Die identifizierten Risiken sind in der Folge zu kategorisieren. Allgemeine Klassifikationsschemata wurden im Rahmen dieser Arbeit bereits in Kapitel 3.2 eingeführt. Diese allgemeinen Ansätze sind in ein unternehmensspezifisches Risikoprofil zu überführen, das als universelle Grundlage für die konsistente, weitergehende Risikoanalyse in allen Unternehmensbereichen verwendet wird. Das spezifische Risikoprofil kann immer nur als Momentaufnahme angesehen werden. Dynamische Märkte mit kontinuierlich verändernden Bedingungen bringen die Notwendigkeit einer planvollen Aktualisierung mit sich.[137]

Ergebnis der Risikoidentifikation ist eine Sammlung der Risiken in einem Risikoinventar. Diese Bestandsaufnahme der Risiken bildet die Grundlage für die weiteren Prozessschritte und enthält zunächst als Risikokatalog eine ungeordnete Auflistung der identifizierten Risiken. In den folgenden Schritten wird es um Informationen zur Bewertung der Risiken, den risikopolitischen Maßnahmen und einer Priorisierung ergänzt. Nach Abschluss aller Prozessschritte liefert das Risikoportfolio (siehe Abb. 11) die Basis für eine kontinuierliche Verbesserung der Risikoposition.

3.3.3 Risikobewertung

Nach der Risikoidentifikation erfolgt im nächsten Schritt die Bewertung der Risiken. Die beiden Prozessphasen lassen sich allerdings nicht vollständig voneinander abgren-

135 Vgl. Füser, Karsten; Gleißner, Werner; Meier, Günter: Risikomanagement (KonTraG) – Erfahrungen aus der Praxis, in: Der Betrieb, 15/1999, S. 754.

136 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 109.

137 Vgl. Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc: Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, a. a. O., S. 320.

zen, sondern gehen in Teilbereichen ineinander über. Auf Basis der identifizierten Risiken wird eine möglichst vollständige und kontinuierliche qualitative Beurteilung und quantitative Bewertung vorgenommen.[138] Mit der Bewertung werden die Risiken hinsichtlich ihres Gefährdungspotenzials geordnet und in ein unternehmensindividuelles Risikoportfolio überführt. Der Erwartungswert für einen Schaden bestimmt sich als Multiplikation von der Eintrittswahrscheinlichkeit mit dem Risikoausmaß. Diese qualitativen Methoden beruhen auf mathematisch-statistischen Berechnungen und sind nur sinnvoll anwendbar, wenn ausreichend große Datenmengen existieren. Gerade in Risikokategorien mit geringer Eintrittswahrscheinlichkeit und hohem Schadensausmaß sind diese Vorraussetzungen jedoch regelmäßig nicht erfüllt.[139] Fehlen die messbaren Größen zur Quantifizierung, werden subjektive Bewertungsskalen aufgestellt (bspw. mit den Ausprägungen existenzbedrohend, schwerwiegend, mittel, gering, unbedeutend).[140] Diese quantitativen Bewertungsmethoden basieren primär auf erfahrungsbezogenen Einschätzungen und sind auch ohne eine statistisch auswertbare Datengrundlage durchführbar. Neben der Unterscheidung in quantitative und qualitative Bewertungsmethoden unterscheidet man zwischen Top-Down- und Bottom-Up-Vorgehensweisen in der Risikobewertung. Stehen die für das Unternehmen bekannten Folgen der Risiken im Vordergrund, spricht man von der Top-Down-Methode. Bei der Bottom-Up-Methode hingegen wird versucht anhand der Ursachen der Risiken durch Betrachtung der Wirkungsbeziehungen die Folgen für das Unternehmen abzuleiten. Dieses Vorgehen ist verglichen mit dem Top-Down-Ansatz wesentlich aufwendiger – es stellt allerdings für die Geschäftsführung ein Fundament zur Etablierung einer gelebten Risikokultur dar und ist somit Grundlage für ein aktives Risikomanagement zwischen Ertragschancen und Verlustpotenzialen.[141]

Eventuelle Wechselwirkungen zwischen Einzelrisiken sind zu beachten, da sich die Gesamtrisikoposition durch nicht perfekte Korrelationen der Einzelrisiken nicht als Summe der Erwartungswerte angeben oder messen lässt. Kurz gesagt: Zwei gegenläufige

138 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 103 f.

139 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 104 f.

140 Vgl. Romeike, Frank: Risiko-Management als Grundlage einer wertorientierten Unternehmenssteuerung, a. a. O., S. 15 f.

141 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 104 f.

Risiken können sich kompensieren.[142] Sowohl bei den monetär erfassbaren Schäden als auch bei den eher qualitativ zu bewertenden Beeinträchtigungen ist eine Visualisierung mittels eines Risikoportfolios hilfreich (vgl. Abb. 11).

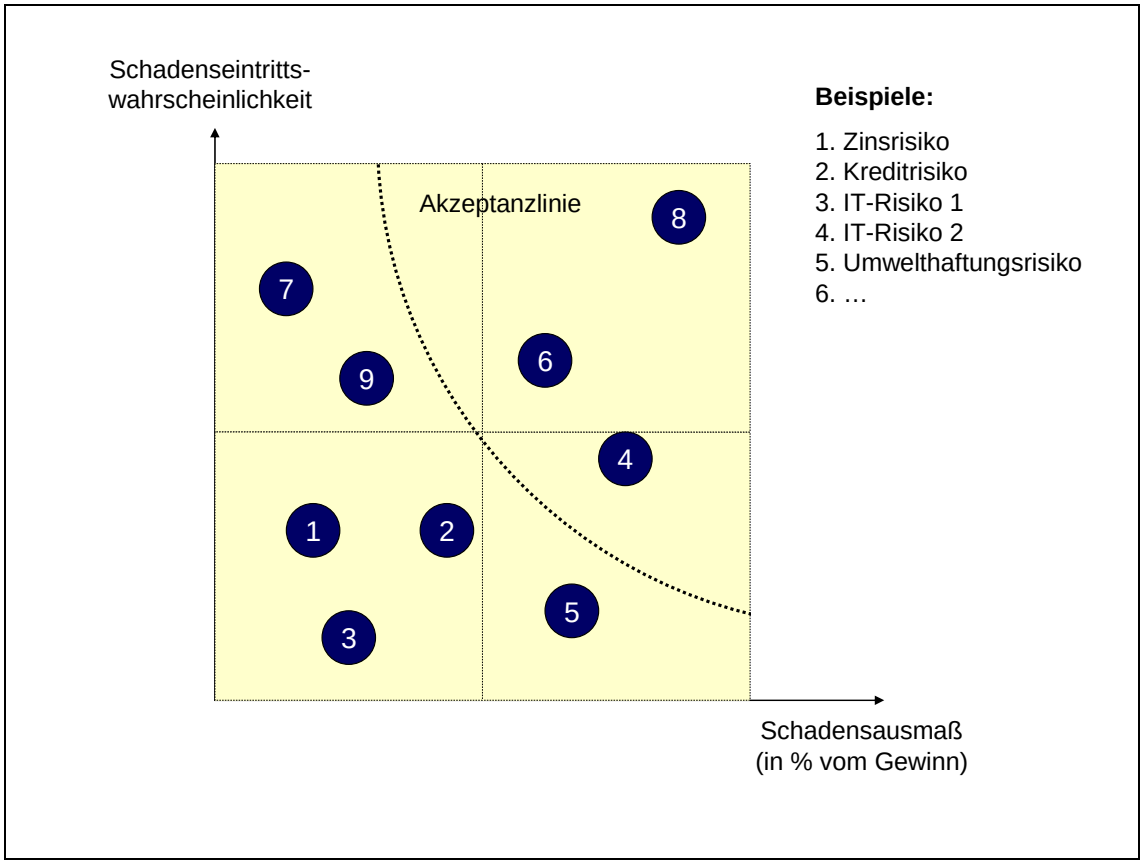

Abb. 11: Risikoportfolio[143]

Auf der Basis des Risikoportfolios kann in den anschließenden Phasen der Risikosteuerung eine Entscheidung über den Umgang mit den identifizierten Risiken getroffen werden. Das Risikoportfolio muss in der Folge ständig aktualisiert und ggf. um neue Risiken ergänzt werden um ein umfassendes Risikomanagement zu ermöglichen.

142 Vgl. Füser, Karsten; Gleißner, Werner; Meier, Günter: Risikomanagement (KonTraG) – Erfahrungen aus der Praxis, a. a. O., S. 755.

143 Entgegen gängiger Darstellungen mit einer konkav zum Ursprung verlaufenden Akzeptanzlinie (vgl. bspw. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 114) wird in der vorliegenden Arbeit die Ansicht vertreten, dass die Akzeptanzlinie streng konvex zum Ursprung verlaufen muss. Die Akzeptanzlinie stellt somit den geometrischen Ort aller Kombinationen von Schadenseintrittswahrscheinlichkeit und Schadensausmaß dar, der (als konstanter Wert) die Risikoneigung des Unternehmens ausdrückt.

3.3.4 Risikosteuerung

Die Risikosteuerung schließt sich an die Risikoanalyse an und beantwortet die Frage nach dem Umgang mit den identifizierten Risiken. Als aktive Beeinflussung wird dabei das Ziel verfolgt, alle wesentlichen Schadensgefahren und Verlustpotenziale durch gezielte steuernde Maßnahmen zu kontrollieren.[144]

Es existieren vier grundlegende risikopolitische Handlungsalternativen. Das (1) *Vermeiden* von Risiken muss in Erwägung gezogen werden, wenn das betroffene Geschäft die Existenz des Unternehmens gefährdet. Damit verbunden ist allerdings immer auch, dass die in dem Geschäft enthaltenen Chancen nicht realisiert werden können. Bei Vermeidung entsteht für das Unternehmen kein Risiko.[145] Das (2) *Vermindern* von Risiken soll die Wahrscheinlichkeit und/oder die Höhe des möglichen Schadens verringern. Das zugrunde liegende Geschäft wird eingegangen, jedoch durch geeignete Steuerungsmaßnahmen in seinem Risiko begrenzt. Die Verminderung ist insbesondere bei Bedrohungen aus menschlichen Fehlverhalten ein effektives Instrument des Risikomanagements.[146] Bei der (3) *Überwälzung* werden die Risiken eines Geschäfts auf ein anderes Unternehmen (meist Versicherungsunternehmen) übertragen. Die Überwälzung ist allerdings nur bei reinen Risiken möglich. Eine Versicherung spekulativer Risiken (wie bspw. dem Unternehmerrisiko) kann nicht erfolgen. Neben der Versicherung sind zur Überwälzung auch vertragliche Klauseln und alternative Finanzierungsmodelle (Futures, Optionen, Swaps) geeignet.[147] Die letzte Option für das Unternehmen ist schließlich, das (4) Risiko selbst zu tragen und damit zu akzeptieren. Das Selbsttragen geschieht einerseits unfreiwillig dann, wenn andere Maßnahmen fehlgeschlagen sind. In der Folge müssen für die akzeptierten Risiken Reserven für den Eintritt des Schadensfalls gebildet werden. Andererseits werden Risken, die unterhalb der Akzeptanzlinie

144 Vgl. Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc: Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, a. a. O., S. 321.

145 Vgl. Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc: Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, a. a. O., S. 321.

146 Vgl. Füser, Karsten; Gleißner, Werner; Meier, Günter: Risikomanagement (KonTraG) – Erfahrungen aus der Praxis, a. a. O., S. 757.

147 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 116 f.

(vgl. Abb. 11) liegen, bewusst akzeptiert. Den in Kauf genommenen Risiken gilt das besondere Augenmerk im Rahmen der Risikokontrolle (vgl. Kapitel 3.3.5).[148]

Durch die Risikosteuerung wird folglich das unternehmerische Chancen-Risiko-Profil optimiert. Unternehmen sollten keine Risiken auf sich nehmen, für deren Management sie nicht die notwendigen Kompetenzen besitzen. Unnötige Risiken - für die eine Erfolg versprechende Risikosteuerung nicht möglich ist - müssen vermieden werden um durch gezielte Steuerung das eigene Risikoportfolio in einer Zusammensetzung zu optimieren, in der die Gewinnchancen größer sind als die Verlustpotenziale. Ein in dieser Form intelligentes Risikomanagement sichert Wettbewerbsvorteile.[149]

3.3.5 Risikokontrolle

Die Risikokontrolle ist eine Art Risikoradar im gesamten Risikomanagementprozess.[150] Durch diese Überwachung der Maßnahmendurchführung kann der Erfolg des Risikomanagements zur Sicherstellung der Zielerreichung als Abweichung zwischen den tatsächlichen und den anhand risikopolitischer Grundsätze definierten Risikosituationen analysiert werden. Die Kontrolle hat auf übergreifender Ebene zu erfolgen und begleitet alle Phasen des Risikomanagementprozesses. Die besondere Aufmerksamkeit gilt dabei der Identifikation und Bewertung sowie der Auswahl der Steuerungsmaßnahmen. Damit gewährleistet die Prozessüberwachung Qualität, Eignung von Aufbau und Ablauf im Prozessablauf.[151]

Bei der Risikokontrolle müssen zwei Teilbereiche berücksichtigt werden: Zum einen ist die Kontrolle Teil des Prozesses zur kontinuierlichen Verbesserung der Risikosituation und stellt damit eine Komponente im Risikomanagementkreislauf dar. Dies wird auch als Risiko-Controlling bezeichnet. Auf der anderen Seite ergibt sich aus gesetzlichen Vorgaben (z. B. KonTraG) die Notwendigkeit einer unabhängigen Prozessüberwa-

148 Vgl. Füser, Karsten; Gleißner, Werner; Meier, Günter: Risikomanagement (KonTraG) – Erfahrungen aus der Praxis, a. a. O., S. 757.

149 Vgl. Brehmke, Kirsten; Meyer, Ralf: Strategisches Risikomanagement, a. a. O., S. 24.

150 Vgl. Romeike, Frank: Lexikon Risikomanagement, a. a. O., S. 112 f.

151 Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc: Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, a. a. O., S. 321 f.

chung. Als neutrale interne Prüfungsinstanz wird diese Überwachung meist von der Internen Revision durchgeführt. Das Risikomanagement und die Frühwarnsysteme sind auch Untersuchungsgegenstand für die externe Prüfung durch Wirtschaftsprüfer. Mit beiden Qualitätssicherungsmaßnahmen werden die Interessen der Stakeholder vertreten, die sich auf die Qualität, die Funktionsfähigkeit sowie die Adäquanz der eingesetzten Risikomanagementinstrumente verlassen müssen.[152]

3.4 Organisation des Risikomanagements

Die zunehmenden aufsichtsrechtlichen Anforderungen aus Basel II und die Komplexität des Risikomanagements als dezentraler Prozess stellt die Geschäftsleitung von Finanzinstituten vor neue organisatorische Herausforderungen. Das Risikomanagement beinhaltet längst mehr als das projektbezogene Berechnen von Ausfallwahrscheinlichkeiten. Vielmehr fordert Basel II eine Überprüfung aller mit dem Eingehen und der Erfassung von Risiken zusammenhängenden Abläufe und Prozesse in den Banken. Damit werden umfassende qualitative Anforderungen an Organisation, Risikokultur und Datenqualität in den Instituten gestellt.[153] Auch das KonTraG fordert die Einrichtung eines Überwachungssystems zur Erkennung existenzgefährdender Entwicklungen auf oberster institutioneller Ebene.[154]

Für die organisatorische Ausgestaltung des Risikomanagements bestehen die grundsätzlichen Alternativen der Integration oder der Verselbstständigung. Bei einem *integrativen Risikomanagementsystem* ist „jeder Entscheidungsträger für die Berücksichtigung von Risiken in seinem Kompetenzbereich verantwortlich."[155] Das Risikomanagement wird dezentral an den Stellen verankert, an denen die Entscheidungen getroffen werden. Dies bietet sich an, wenn die Entscheidungsträger die mit der Entscheidung verbundenen Risiken am besten einschätzen können sowie die geeigneten Maßnahmen

152 Vgl. Krystek, Ulrich; Fiege, Stefanie: Risikomanagement, a. a. O., S. 2558 f.

153 Vgl. Loch, Friedemann; Thelen-Pischke, Hiltrud: Basel II – Herausforderungen für die Geschäftsleitung der Institute, in: Zeitschrift für das gesamte Kreditwesen, 13/2001, S. 736.

154 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 23.

155 Vgl. Kupsch, Peter: Risikomanagement, in: Handbuch Unternehmensführung. Konzepte – Instrumente – Schnittstellen, Hrsg.: Corsten, Hans; Reiß, Michael, Wiesbaden: Gabler 1995, S. 541.

zur Risikosteuerung am besten erkennen und beurteilen können. Bei integrativem Risikomanagement werden bei allen Entscheidungen Chancen- und Risikoaspekte gegeneinander abgewogen. Dies entspricht der Vorstellung eines generellen Risikomanagements. Ein solches dezentrales Risikomanagement ist aufgrund der Komplexität der Risikozusammenhänge und der engen Verbindung mit der Risikopolitik nicht unproblematisch.[156]

Im Gegensatz zum oben erläuterten Konzept steht das *verselbstständigte Risikomanagement*. Dabei wird Risikomanagement als selbstständiger und von der eigentlichen Sachaufgabe und den damit verbundenen Entscheidungen unabhängiger Prozess verstanden. Die Vorteile dieser Ausgestaltung liegen in der Möglichkeit zur Spezialisierung sowie der Sicherung einer angemessenen Gewichtung von Risikofragenstellungen. Durch die zentrale Risikosteuerung können einheitliche Richtlinien entwickelt und durchgesetzt werden. Zudem ist ein Überblick über die Gesamtrisikoposition nur in einem verselbstständigten Bereich sinnvoll zu erlangen.[157]

Nach den Anforderungen aus dem Baseler Ausschuss unterliegen die Identifikation und das Management aller Risikoarten der Verantwortung und Überwachung der Geschäftsführung. Die Geschäftsführung hat mit der installierten Aufbau- und Ablauforganisation sicherzustellen, dass die qualitativen und quantitativen Ansprüche erfüllt werden.[158] Die Geschäftsführung muss folglich entscheiden, welche Komponenten des Risikomanagements auf welche Weise im Unternehmen verankert werden. Dabei hängt die Wahl zwischen den oben erläuterten Ansätzen des integrativen und des verselbstständigten Risikomanagement eng mit der der Einscheidung zwischen zentralen oder dezentralen Risikomanagementinstitutionen zusammen.

Eine vollständige Dezentralisierung im Rahmen eines verselbstständigten Risikomanagement ist aufgrund der aufsichtsrechtlichen Vorgaben nicht angemessen. Vielmehr werden sich hinsichtlich beider Gestaltungsfragen Mischformen herausbilden. Insbesondere Tätigkeiten, die Detailkenntnisse erfordern (Risikoanalyse, Entwicklung risiko-

156 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 24.

157 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 24.

158 Vgl. Loch, Friedemann; Thelen-Pischke, Hiltrud: Basel II – Herausforderungen für die Geschäftsleitung der Institute, a. a. O., S. 736.

politischer Maßnahmen, Überwachung der risikopolitischen Maßnahmen) werden sinnvoll dezentral und integriert ausgeführt. Die Risikopolitik enthält dazu klare Grenzen in denen das Risikoausmaß dezentral gemanagt wird. Bei Überschreitung der Grenzen muss die übergeordnete (zentrale) Einheit einbezogen werden. Verschiedene Aufgaben sind ausschließlich zentral zu erfüllen. Dazu gehört die Integration des Risikomanagements in die Unternehmenspolitik und grundsätzliche risikopolitische Entscheidungen (z. B. die Festlegung der Risikotragfähigkeit). Die zentrale Instanz sollte auch die Koordination von Aktivitäten der Risikoanalyse, die Aggregation von Risiken verschiedener Bereiche, die Beurteilung risikopolitischer Maßnahmen, die risikobezogene Berichterstattung an den Vorstand sowie dessen Beratung, die Überwachung und kontinuierliche Verbesserung des bestehenden Risikomanagementsystems übernehmen.[159]

4 Integration von IT-Sicherheits- und Risikomanagement

4.1 Effizienzpotenziale der integrierten Betrachtung

IT-Sicherheitsrisiken sind sowohl Betrachtungsobjekt des Risikomanagements als auch das zentrale Aufgabengebiet des IT-Sicherheitsmanagements. Die vorangegangenen Kapitel haben einen Überblick über die Bedeutung und die Methoden des IT-Sicherheitsmanagements sowie über die idealtypische Ausgestaltung des Risikomanagementprozesses gegeben. Im vorliegenden Kapitel werden die Effizienzpotenziale einer integrierten Betrachtungsweise aufgezeigt. Dabei werden die Prozesse, Instrumente und Prinzipien der Aufbauorganisation betrachtet und anhand des Risikomanagementkreislaufs aus Kapitel 3 Schnittmengen in den bisher meist isolierten Vorgehensweisen identifiziert.

Der hohe Stellenwert der Informationssicherheit in der Bankenlandschaft bringt der Branche den Ruf des „Informationsmanagers“ ein. Zusammen mit dem Umstand, dass Banken Geld und Vermögenswerte von Dritten (den Kunden) verwalten, begründet dies

159 Vgl. Mikus, Barbara: Risiken und Risikomanagement – ein Überblick, a. a. O., S. 24 f.

die existenzielle Bedeutung sicherer Informationsverarbeitung.[160] Sicherheit ist folglich bei Einsatz jedweder IT-Systeme in Banken ein wichtiges Thema. Die IT-Sicherheit hat sich parallel zu den eingesetzten Systemen vom Einsatz erster IT-Komponenten bis zum heutigen, hochgradig IT-abhängigen Geschäftsbetrieb entwickelt. Bestehende Lösungen haben allerdings oft nicht lange Bestand. Deshalb kann das Management in der Informationstechnologie auch als „Management des Wandels" bezeichnet werden.[161] Hinzu kommt gerade im Finanzdienstleistungssektor ein hoher Grad der Dezentralisierung durch die Verflechtung verschiedener Tochtergesellschaften unter einem Konzerndach und das für Banken typische weiträumig verteilte Filialnetz. Daraus resultiert eine komplexe Umgebung heterogener Informationssysteme, in der Sicherheitsprobleme von Teilsystemen die Sicherheit des Gesamtsystems gefährden können.[162]

IT-Sicherheitsmanagement ist unter den genannten Rahmenbedingungen in den meisten Unternehmen historisch gewachsen. Die so entstandenen Strukturen erfüllen allerdings gerade im Finanzdienstleistungssektor nicht die hohen Anforderungen, die aus dem gehobenen Stellenwert der Informationssicherheit resultieren. Sowohl die organisatorische Gestaltung als auch die eingesetzten Methoden können das Potenzial im Bereich IT-Sicherheit oft nicht umsetzen.[163]

Ganz anders stellt sich die Entwicklung des Managements operationeller Risiken dar. Durch die Einbeziehung der operationellen Risiken in Basel II hat sich erst in der jüngeren Vergangenheit innerhalb des Risikomanagements eine neue Teildisziplin entwickelt, die weitgehend neu konzipiert, mit Kompetenzen ausgestattet und in die bisherige Risikoorganisation eingebettet werden konnte: das operationelle Risikomanagement (ORM). Durch den breiten Fokus des ORM können Betriebsrisiken integriert betrachtet

160 Vgl. Nägli, Hans-Peter: Management der Informationssicherheit – Erfahrungen eines Finanzdienstleisters, in: HMD – Praxis der Wirtschaftsinformatik, Bd. 232, Hrsg.: Brenner, Walter; Meier, Andreas; Zarnekow, Rüdiger, Heidelberg: dpunkt 2003, S. 80.

161 Vgl. Paulus, Sacher: Risiken beim Einsatz von Informationstechnologie, in: Praxis des Risikomanagements: Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte, Hrsg.: Dörner, Dietrich; Horváth, Péter; Kagermann, Henning, Stuttgart: Schäffer-Poeschel, 2000, S. 384.

162 Vgl. Voßbein, Jörn: Organisation eines IT-Sicherheitsmanagement, in: IT-Sicherheitsmanagement in Banken, Hrsg.: Roßbach, Peter; Locareck-Junge, Hermann, Frankfurt/Main: Bankakademie-Verlag, 2002, S. 9 f.

163 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 477.

werden. Dem Subsidiaritätsprinzip des Risikomanagements folgend sind auch die Risiken der IT dezentral zu erfassen. Um die Angemessenheit und die Qualität sowohl für die Bereiche des Risikomanagements als auch für die IT-Sicherheit zu sichern, müssen sich beide Bereiche annähern. Die bisherigen Probleme in der Praxis des IT-Risikomanagements sind in Banken vor allem in der organisatorischen Trennung zwischen ISM und ORM begründet. Die in den Bereichen verankerten Organisationsphilosophien sowie die Ausstattung mit Methoden unterlagen – wie oben bereits angeführt - in der Vergangenheit unterschiedlichen Entwicklungen.[164]

Die Bedeutung von Sicherheitsaspekten wird im Risikomanagement teilweise unterschätzt. Die Wahrnehmung von Sicherheit unterscheidet sich vom normalen Verständnis des Risikos, da Sicherheitsaspekte stark von sozialen Faktoren abhängen, während leistungswirtschaftliche und finanzielle Aspekte nachgelagert sind. Sicherheitsmanagement als Abwehr von Gefahren zeichnet sich dadurch aus, dass negative Konsequenzen abgewehrt werden. Der in der Wahrnehmung des Begriffs Risiko enthaltene Chancenaspekt ist bei Sicherheitsfragen nicht gegeben. Für Bestrebungen im Bereich Sicherheit – und damit auch in der IT-Sicherheit – lässt sich festhalten, dass die Anliegen eher schutz- als chancenbezogen sind, die Art der Bedrohung gerade auf den oberen Managementebenen leicht verdrängt wird und Störungen häufig als überraschend für das Management auftreten.[165]

Sicherheit wird im IT-Bereich intensiv betrachtet. Der Fokus des ISM ist allerdings nur wenig auf das Verhältnis von Kosten und Nutzen ausgerichtet. Derzeitige Schadensmodelle in der IT-Sicherheit vernachlässigen oftmals die monetäre Komponente. Einerseits lässt sich das Ausmaß eines Schadens oftmals nicht messen, andererseits sind in der IT-Sicherheit auch Angriffe zu erfassen, die im Sinne des Angreifers nicht erfolgreich waren und somit für das angegriffene Unternehmen auch keine monetäre Auswirkung ha-

164 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 478.

165 Vgl. Haller, Matthias: <Security> und Risiko-Management – ein Widerspruch?, in: Student Business Review, Ausgabe Frühjahr 2005, St. Gallen, S. 7 f.

ben. Trotzdem müssen auch für diese Bereiche Gegenmaßnahmen geplant werden, deren qualitativer Nutzen zu bewerten ist.[166]

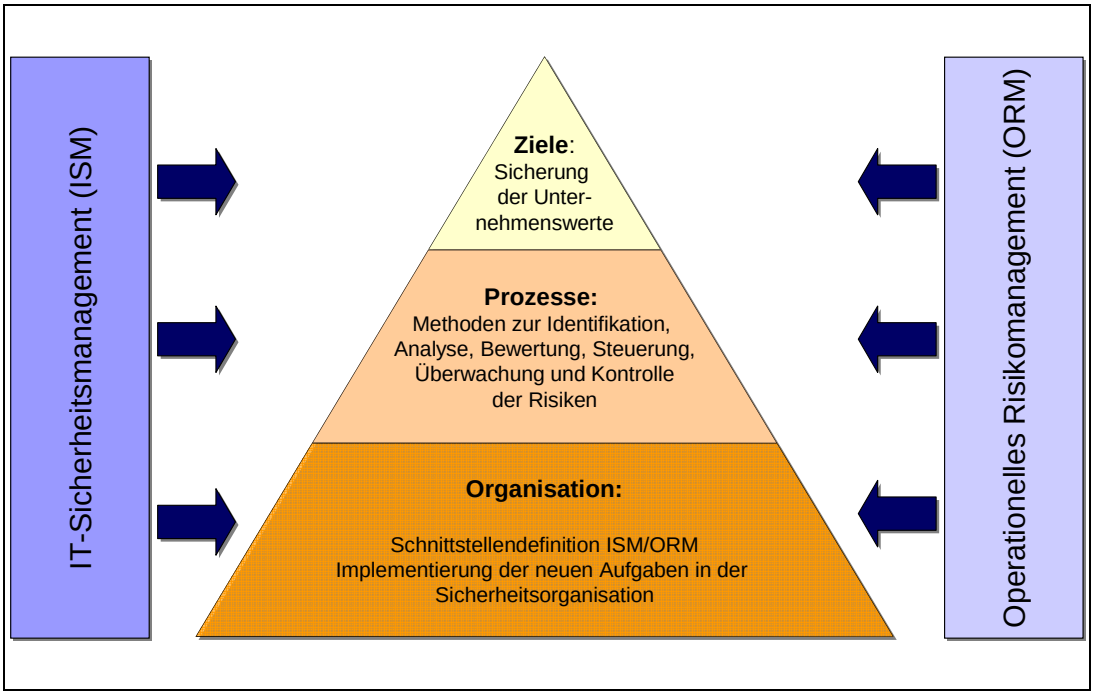

Abb. 12: Integrationsebenen zwischen ISM und ORM[167]

Zusammenfassend lässt sich feststellen: Im Bereich IT-Sicherheit sind Risiken vorhanden, die im Rahmen des ORM beachtet werden müssen. Die beiden Bereiche ISM und ORM weisen offensichtliche Schnittmengen auf. Um Doppelarbeiten im Prozess der Risikoerfassung, -bewertung, -steuerung und -kontrolle und die damit verbundenen Ineffizienzen zu vermeiden, wird in den folgenden Kapiteln ein Ansatz zur Integration entwickelt. Ziel ist die Darstellung eines effektiven und gleichzeitig effizienten Risikomanagementprozesses für Risiken aus dem Bereich IT-Sicherheit. Die Vorgehensweise orientiert sich dabei am idealtypischen Prozess des Risikomanagements, da die im Risikomanagement gesetzten Qualitätsstandards durch alle Teilbereiche des Unternehmens zu erfüllen sind. Die breite Ausrichtung des Risikomanagements – insbesondere im Management operationeller Risiken – ermöglicht eine integrative Betrachtung aller Be-

166 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 484.

167 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 486.

triebsrisiken. Die notwendigen Kompetenzen zur Durchsetzung abteilungsübergreifender Zusammenarbeit zwischen ISM und Fachabteilungen besitzt im Unternehmen das ORM. Die Konzeption eines aktiven und permanenten Risikomanagementkreislaufs erlaubt zudem eine schrittweise Integration der Bereiche ORM und ISM. Die bisherigen Verfahrensweisen des ISM sollen durch die Integration nicht vollständig ersetzt, sondern in den Bereichen sinnvoll erweitert werden, an denen ein Zusatznutzen entstehen kann.[168]

Risiken im Bereich der IT-Sicherheit müssen – wie alle Risikokategorien - systematisch identifiziert, bewertet, gesteuert und kontrolliert werden. Im Integrationsansatz werden drei Ebenen betrachtet (vgl. Abb. 12): Ziele bzw. Zielsysteme (Kapitel 4.2), Prozesse (Kapitel 4.3) und Aufbauorganisation (Kapitel 4.4).

4.2 Gemeinsame Zielsysteme

Ein gemeinsames Zielsystem ist die Voraussetzung für die erfolgreiche Integration von ISM und ORM. In Kapitel 4.1 wurde bereits darauf hingewiesen, dass Schnittmengen zwischen den beiden Bereichen existieren. Dies ist u. a. in den zueinander komplementären Zieldefinitionen begründet. Sachziel des ORM ist die „Gewährleistung des Fortbestandes des Unternehmens beim Eintreten von Schäden und die Vermeidung von inakzeptablen Schäden." Das ISM definiert sein Sachziel als „Gewährleistung der geforderten Sicherheit und Zuverlässigkeit der Systeme". Ergänzt werden die Sachziele beider Bereiche durch Formalziele wie Rechtmäßigkeit, Wirtschaftlichkeit, Angemessenheit und soziale Akzeptanz. Die Formalziele stehen teilweise in Konflikt mit den Sachzielen. Eine Bespitzelung der Mitarbeiter wäre prinzipiell geeignet, internen Betrug zu vermeiden. Sie ist arbeitsrechtlich allerdings nicht zulässig.[169]

Das Sachziel des ISM unterstützt das Sachziel des ORM und beide Zielsysteme sind miteinander vereinbar. Die Ziele beider Bereiche werden in organisatorischen Richtlinien definiert, die auf der obersten Managementebene zu verabschieden sind. Im Risi-

168 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 478.

komanagement ist eine Risikopolitik zu verabschieden, die die allgemeine Risikoeinstellung und die Grundsätze für den Umgang mit Risiken definiert. Sie ist Grundlage für die Einrichtung einer geeigneten Kontrollumgebung.[170] Der Bereich ISM erstellt in Zusammenarbeit mit dem Vorstand eine Sicherheitspolitik, die den Rahmen für den angemessenen Umgang mit der Ressource Information definiert und insbesondere den Risikofaktor „Mensch" einbezieht. Sie ist langfristig ausgerichtet und führt zur Entwicklung geeigneter Sicherheitsvorschriften für spezielle Sicherheitsaspekte.[171]

Die Formulierung und Kommunikation der Richtlinien ist Ausdruck der Unterstützung der Bereiche durch die Vorstandsebene. Der Vorstand muss auch die Basis für die Zusammenarbeit der beiden Bereiche schaffen. Nur mit der Unterstützung des Vorstandes kann die Integration von ISM und ORM durch organisatorische Verknüpfung und methodische Angleichung gelingen.

4.3 Der Prozess des IT-Risikomanagements

4.3.1 Identifikation von IT-Risiken

Die systematische Identifikation aller aktuellen und potenziellen Schadensereignisse ist Grundlage für ein effizientes Risikomangement. Verlust- oder Schadenspotenziale aus der IT entstehen in allen Bereichen, in denen das Unternehmen auf IT angewiesen ist, um seine Unternehmensziele zu erreichen. Als Teilbereich der operationellen Risiken finden IT-Risiken und damit IT-Sicherheit durch Basel II aufsichtsrechtliche Berücksichtigung. Die Integration von IT-Risiken auf Ebene der Risikokategorien ist durch Basel II allerdings nicht erfolgt. IT-Risiken werden nicht in eine eigene Risikokategorie eingeordnet, sondern sind Teilbereiche verschiedener Kategorien.[172]

---

169 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 487.

170 Vgl. dazu ausführlich Kapitel 3.3.1.

171 Eine beispielhafte Sicherheitspolitik (Information Security Policy) findet sich im Anhang A von ISO/TR 13569:2005. Vgl. International Standard Organisation (Hrsg.): ISO/TR 13569 – Financial Services – Information Security Guidelines, a. a. O., S 43.

172 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 483.

Um einen verantwortungsvollen, rationalen und wirtschaftlichen Umgang mit IT-Risiken zu ermöglichen, müssen in der Risikoidentifikation nicht nur technische Aspekte einbezogen werden. Als Ausgangspunkt für den Prozess des Risikomanagements im IT-Bereich sollten zunächst folgende Fragen gestellt werden:

- *Was* soll eigentlich geschützt werden?
- *Wovor* soll es geschützt werden?
- Was kostet Unsicherheit?[173]

Die beiden ersten Fragen sind in der Risikoidentifikation zu beantworten. Die Kosten der Unsicherheit werden im Kapitel zur Risikobewertung in die Betrachtung einbezogen.

Für eine vollständige Identifikation der IT-Risiken im Unternehmen ist eine Kategorisierung der Risiken zur systematischen Erfassung notwendige Voraussetzung. Nur eine sinnvolle Risikokategorisierung ermöglicht die Zuordnung aller Risiken in dezentralen Organisationsstrukuren in *ein* systematisches Raster. Diese Risikokategorien sind in Zusammenarbeit mit den Spezialisten des ISM durch das ORM festzulegen um eine einheitliche Risikoerfassung zu ermöglichen. Dezentrale Organisationsstrukturen und verteilte IT-Systeme führen zwangsläufig dazu, dass die Vorgabe von Kategorien bei einer zentralen Organisationseinheit (dem ORM) verankert sein muss. Die Kategorisierung muss zur Realisierung der angestrebten Effizienzsteigerungen für beide Bereiche praktikabel sein. Idealerweise lässt sich der in Zusammenarbeit von ORM und ISM entwickelte Risikokatalog in beiden Bereichen ohne Anpassungen verwenden. Damit muss das ORM die für die Eigenkapitalberechnung nach dem fortgeschrittenen Messansatz relevanten Risiken nur noch aus den Daten des ISM herausziehen. Eine Doppelerfassung wird vermieden. Es wird vereinzelt Risiken im Bereich IT-Sicherheit geben, die für das ORM unbedeutend sind. Auch diese Risiken müssen aufgenommen und ggf. nur auf Ebene des ISM weiterführend betrachtet werden.

Die eigentliche Identifikation der Risiken ist ebenfalls von ORM zu initiieren und durch dessen Methoden zu unterstützen. Die im Risikomangement üblichen Risikobewertun-

173 Vgl. Maus, Thomas: Inventarisierung und Bewertung von IT-Risiken, in: Staat & IT - Information Week Special, 11/2004, S. 25.

gen sind auch im IT-Bereich anwendbar und analysieren mögliche Schadensszenarien. Die Auswahl der Erhebungstechniken und die Ausgestaltung der im Risikomanagement weit verbreiteten Fragebögen sind eng mit dem ISM abzustimmen. Nur durch eine sinnvolle Integration des ISM in den Prozessschritt Risikoidentifikation kann eine vollständige Erfassung von IT-Risiken erfolgen. Die Vorgehensweisen des Risikomangements sind im IT-Bereich bisher eher unbedeutend. IT-Sicherheit wird nur selten mit den prozessorientierten Vorgehensweisen des ORM erfasst. Im ISM werden bisher eher periodisch wiederkehrende Sicherheitsüberprüfungen (Audits) durchgeführt.

Der *erste Schritt* zur Erfassung der Risiken ist die Inventarisierung der zu schützenden Werte. Darunter sind neben Hardware, Software und Kommunikationseinrichtungen auch Informationen als wesentliche Ressource des Unternehmens zu verstehen. Diese Darstellung der Systemlandschaft ist Aufgabe des ISM.

Im *zweiten Schritt* werden zur Erfassung der Risiken, die aus den Zusammenhängen zwischen Software (Applikationen), Hardware und Kommunikation entstehen, die Geschäftsprozesse detailliert analysiert. Daraus entsteht eine Landkarte von IT-Komponenten, die sowohl die Zusammenhänge zwischen den einzelnen Systembestandteilen, als auch die Verbindung zu den Geschäftsprozessen herstellt. Nur über die Zuordnung zu den Leistungen und Geschäftsprozessen kann die Leistung der Querschnittsfunktion IT sinnvoll quantitativ eingeordnet werden. In die Modellierung von Geschäftsprozessen sind somit IT-Komponenten aufzunehmen. Die so modellierten IT-Geschäftsprozesse (vgl. Abb. 13) bilden als horizontaler Schnitt durch die Systemlandschaft die Abhängigkeiten von den verschiedenen Teilbereichen der IT ab. Alle diese Prozesse sind vollständig zu dokumentieren und erst nach erfolgter Erfassung können die Auswirkungen der inhärenten Risiken aus einzelnen Komponenten abgeleitet werden.

Betrachtet man beispielhaft und auf abstrakter Ebene den in Abb. 13 dargestellten fiktiven Prozess einer Kreditabwicklung, so lässt sich folgendes Beispiel für den Prozessschritt Bonitätsprüfung und dessen Verbindung zu IT-Systemen beschreiben: Die Bonitätsprüfung nutzt die Applikationen A1 und A2. Beide Applikationen sind abhängig von der im vorangegangenen Prozessschritt verwendeten Applikationen A1. Die Ergebnisse werden von A1 an A3 weitergeleitet. A2 liefert an A1 sowie A3. Alle Applikationen nutzen die Systemarchitektur aus Software, Hardware und Netzen. Applikation A1

kann bspw. ein Auftragserfassungsmodul sein, das auf einem Arbeitsplatzrechner mit Anbindung an einen zentralen Server läuft. Es ist über eine bestimmte lokale Netzwerkverbindung mit A2 verbunden. Im Vertragsabschluss läuft die Applikation A6 allerdings bei einem Außendienstmitarbeiter, der über andere Kommunikationswege auf die Daten zugreift (bspw. per VPN).

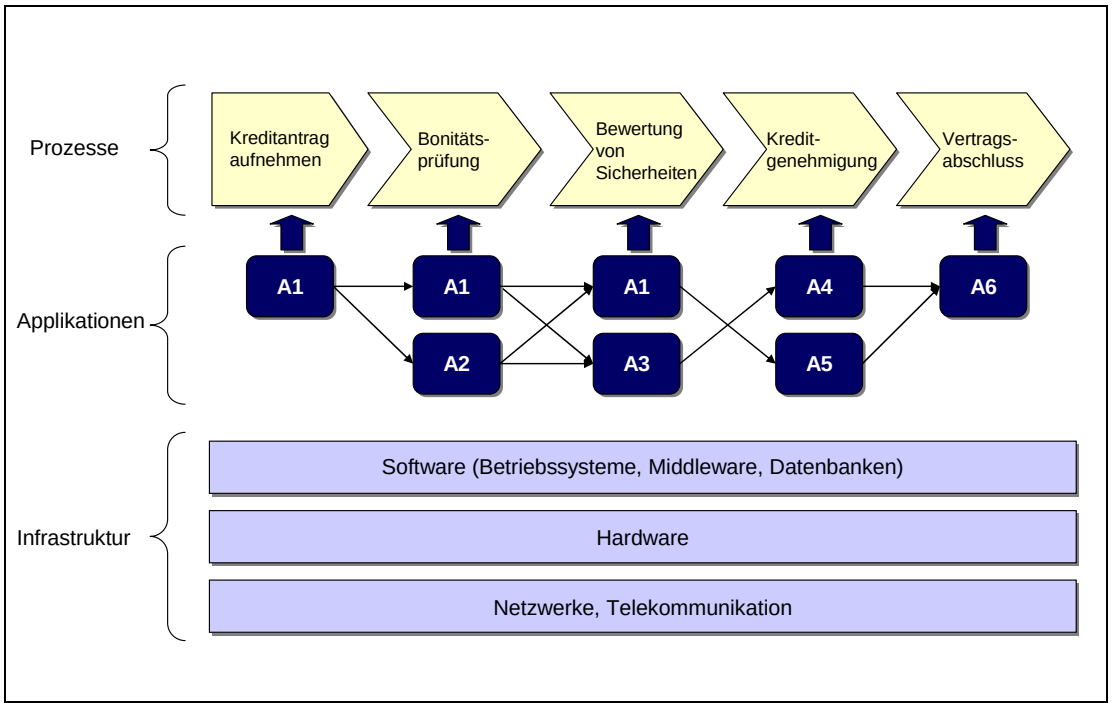

Abb. 13: Abhängigkeiten in IT-gestützten Geschäftsprozessen

In der Identifikation von Sicherheitsrisiken an der Schnittstelle von IT-Komponenten und Geschäftsprozessen ist dem Mensch die besondere Aufmerksamkeit zu widmen. Im soziotechnischen Gebilde der IT muss er als Risikofaktor besonders beachtet werden.[174]

Das Sicherheitsverhalten der Mitarbeiter und damit die Umsetzung der Sicherheitsrichtlinie muss in die Risikoidentifikation einbezogen werden. Der Umgang mit Informationen in den dezentralen Bereichen kann nur in qualitativer Form erfasst werden. Es sind Risikofaktoren aus mangelndem Sicherheitsbewusstsein der Mitarbeiter zu beachten. Diese weichen Faktoren können einerseits durch Self-Assessements aufgenommen werden, andererseits ist hier auch eine aktive Beobachtung des Mitarbeiterverhaltens im

Alltag notwendig. Dabei ist es unerlässlich, dass das Management die Wichtigkeit der Informationssicherheit durch eigenes Verhalten hervorhebt. Denn nur wenn sicherer Umgang mit Informationen von oben vorgelebt wird, kann in allen Bereichen des Unternehmens eine entsprechende Unternehmenskultur etabliert werden. Zur Identifikation von Risiken aus dem bewussten Fehlverhalten einzelner Mitarbeiter (Betrug, Überschreitung der eigenen Kompetenzen) ist das Unternehmen auf die Beobachtungen der dem Unternehmen loyal verbundenen Mitarbeiter angewiesen. Es müssen Berichtswege (ggf. anonym) eingerichtet werden, über die entsprechende Informationen kommuniziert werden können. Die aus der Vielzahl der an den Geschäftsprozessen beteiligten Faktoren resultierende Komplexität kann nur in Zusammenarbeit von ORM und ISM mit den Fachabteilungen bewältigt werden.

Vervollständigt wird die Risikoidentifikation im *dritten Schritt* durch die Beachtung von wirtschaftlichen und insbesondere rechtlichen Rahmenbedingungen. Während die wirtschaftlichen Faktoren vor allem in der generellen Risikostrategie und damit auch als Grundlage für die Bewertung und Steuerung der Risiken ihren Niederschlag finden, sind rechtliche Aspekte teilweise mit erheblichen Schadenspotenzialen verknüpft. Die in Kapitel 2,2 betrachteten gesetzlichen Vorgaben sind bei Nichtbeachtung mit teilweise erheblichen Strafen verbunden. Die Nichtbeachtung von Regelungen des BDSG kann zivilrechtliche Folgen haben. Als Allfinanzaufsichtsbehörde hat die BaFin als letzte Option bei Verstößen gegen das KWG die Option, die Zulassung zum Geschäftsbetrieb zu entziehen (§ 35 Abs. 1 KWG). In der Analyse der Risiken, die aus rechtlichen Vorgaben resultieren, müssen ISM und ORM ebenfalls zusammenarbeiten. Die Fachkompetenz für datenschutzrechtliche Fragenstellungen ist eher im ISM zu finden, während die Anforderungen aus Basel II in das Gebiet des ORM fallen.

Als Ursachen für die Risiken in der IT-Sicherheit lassen sich konzeptbedingte Schwächen der eingesetzten technischen Lösungen, Schwächen in der technischen Absicherung (Software- oder Konfigurationsfehler), Schwächen des Managements (notwendige Maßnahmen werden wissentlich oder unwissentlich nicht getroffen) oder menschliche

174 Vgl. dazu das in dieser Arbeit zugrunde gelegte Begriffsverständnis von IT (Informationstechnologie) in Kapitel 2.1.1.

Schwächen identifizieren. Letztere sind immer vorhanden und lassen sich nicht vollkommen vermeiden.[175]

Durch die Analyse der Geschäftsprozesse des Unternehmens und deren Abhängigkeit von IT lassen sich zusammenfassend drei Perspektiven identifizieren, aus denen ein vollständiges Risikoinventar abgeleitet werden kann: Werte, Prozesse und juristische Rahmenbedingungen. Die teilweise Überschneidung der Sichtweisen ist dabei akzeptiert und gewollt, da sie hilft, ein vollständiges Bild der Schadenspotenziale zu erarbeiten.[176] Diese drei Teilbereiche können durch Ausrichtung an risikoorientierten IT-Sicherheitsstandards (wie ISO 27001[177]) zu großen Teilen abgedeckt werden. Die Methoden zur Risikoanalyse und die organisatorische Durchsetzung von Risk-Assessments liegen im Verantwortungsbereich des ORM. Das ISM wird an der Schnittstelle zwischen Geschäftsprozessen und IT-Systemen in die Risikoidentifikation einbezogen. Das gemeinsam erarbeitete Risikoinventar beantwortet die Frage, *was* zu schützen ist und *wovor* es zu schützen ist. Die ersten beiden eingangs gestellten Fragen sind damit beantwortet. Das Risikoinventar dient in der Folge als Grundlage für das Risikomanagement durch ISM und ORM. Es schafft gleichzeitig eine transparente Diskussionsgrundlage für die Kommunikation zwischen ORM und ISM sowie zu den anderen Fachabteilungen und den Leitungsebenen.

4.3.2 Bewertung von IT-Risiken

Die Bewertung von Risiken der IT-Sicherheit mit Methoden des ORM ist notwendige Grundlage für den angemessenen Umgang mit diesen Risiken. Risiken, die nicht bewertet werden können, finden im Kontext der aufsichtsrechtlichen Vorgaben wenig Berücksichtigung. Insbesondere die Forderung nach einer Eigenkapitalhinterlegung operationeller Risiken aus Basel II ist ohne eine Bewertung der Risiken nicht durchführbar.

175 Vgl. Paulus, Sacher: Risiken beim Einsatz von Informationstechnologie, a. a. O., S. 397.

176 Vgl. Maus, Thomas: Inventarisierung und Bewertung von IT-Risiken, a. a. O., S. 26.

177 Vgl. Kapitel 2.4.1.

Für das ISM eröffnen sich durch eine quantitative Bewertung von Sicherheitsaspekten Wege zur wirtschaftlichen IT-Sicherheit.[178]

Für das ISM sind sowohl die quantitative Bewertung von Eintrittswahrscheinlichkeiten als auch die Ermittlung möglicher Schadenshöhen bisher relativ unbedeutend. Der Schwerpunkt des ISM lag in der Vergangenheit oft auf der Implementierung von Gegenmaßnahmen ohne intensivere Betrachtung des Risikopotenzials. Der Grundschutzansatz des BSI vernachlässigt unternehmensspezifische Risikoanalysen und schlägt Sicherheitsmaßnahmen für weit verbreitete Gefährdungen vor. Damit kann ein gewisses Schutzniveau erreicht werden. Bei dieser Vorgehensweise besteht allerdings die Gefahr einer Über- bzw. Untersicherung. Trotz dieser Kritik ist der Grundschutz ein Ansatzpunkt für eine Vielzahl von Schadensszenarien mit geringeren Schadenspotenzialen.[179] Sind höhere Schadenspotenziale zu erwarten, eigenen sich Top-Down-gerichtete Ansätze für eine detaillierte Risikoanalyse. Beispielhaft für ein solches Vorgehen wurde in Kapitel 2.4.1 der internationale Standard ISO 27001 dargestellt, der mit der Forderungen nach einer auf permanente Verbesserung ausgerichteten PDCA-Vorgehensweise eine Auseinandersetzung mit Risiken beinhaltet.

Die aus dem Risikomangement bekannten Verfahren zu Risikobewertung sind auch in der IT-Sicherheit prinzipiell anwendbar. Die Einschätzung von Risiken wird ausgedrückt in Form des Risikopotenzials, das sich aus der Multiplikation von Eintrittswahrscheinlichkeit mit dem Schadensausmaß ergibt. Die Feststellung der Schadenshöhe stellt allerdings das zentrale Problem im Bereich der IT-Sicherheit dar. IT als Querschnittsfunktion wirkt mit der Kombination aus Infrastruktur (Hardware, Kommunikation), Software (Betriebssysteme, Middleware, Datenbanken) und den darin gespeicherten Informationen auf eine Vielzahl von Geschäftsprozessen. Die Auswirkungen eines Ausfalls einer IT-Komponente können durch das ISM alleine allerdings nicht erfasst werden. Fehler und Ausfallzeiten der IT wirken sich in verschiedenen Teilbereichen des Unternehmens aus, so dass eine genaue monetäre Erfassung des Schadensausmaßes allein durch das ISM schwer möglich ist.

178 Vgl. Maus, Thomas: Inventarisierung und Bewertung von IT-Risiken, a. a. O., S. 26.

179 Vgl. Kapitel 2.4.3.

Für die Bewertung möglicher Schadensausmaße muss das Risikomanagement die Unterstützung des ISM in allen Fachabteilungen einfordern. ORM und ISM sind auf die Mitarbeit der Bereiche angewiesen, in denen die Prozesse ablaufen. Der Aufwand für die Bewertung in ggf. abteilungsübergreifenden Szenarien ist dementsprechend hoch. Trotz dieser Komplexität kann auf die Erhebung entsprechender Daten nicht verzichtet werden, wenn das ORM Nutzen aus ihnen ziehen soll. Es müssen Lösungen entwickelt werden, wie Risiken bewertet werden können. Nicht quantifizierbare Risiken müssen mit alternativen Bewertungsmodellen erfasst werden.

Als Grundlage für die Bewertung dienen die bereits im Rahmen der Risikoidentifikation modellierten IT-Geschäftsprozesse. Um den Aufwand der Risikobewertung zu minimieren, sollten in die detaillierte Einschätzung von Schadenshöhen und Eintrittswahrscheinlichkeiten allerdings nur die zentralen Prozesse des Unternehmens eingehen. Es wird das Kerngeschäft betrachtet, da hier entsprechende Schadenspotenziale erwartet werden müssen. In ihrer Relevanz untergeordnete Unterstützungsprozesse und obligatorische Maßnahmen können den hohen Aufwand der Bewertung nicht mit entsprechendem Nutzen aufwiegen und sind deshalb zu vernachlässigen. In diesen Bereichen soll das ISM auf die Methoden der Grundschutzansätze zurückgreifen.[180] Mit der Unterstützung aus den Fachabteilungen müssen Schadensszenarien von Sicherheitsvorfällen in den Prozessen erstellt werden, die eine Bewertung der Sicherheitsrisiken in den dezentralen Teilgebieten der IT-Sicherheit ermöglichen. Monetäre Bewertungen von Schadensszenarien sind zwar wünschenswert, müssen ggf. aber durch qualitative Wertmaßstäbe ersetzt werden. Sowohl Schadenshäufigkeit (z. B. auf einer Skala von extrem geringem bis extrem hohem Schadensausmaß) als auch Eintrittswahrscheinlichkeiten (sehr selten bis sehr oft) können so erfasst werden. Aus der Analyse der Prozesse wird schließlich das Schadenspotenzial gemessen oder geschätzt. Die so erarbeiteten Daten sind als qualitative Einschätzungen zu verstehen, da sie weitgehend auf Meinungen und Analysen basieren.

Für die Bewertung der auf Prozessebene nicht quantifizierbaren Risiken ist alternativ die Anwendung eines Opportunitätskostenansatzes möglich. Die Kosten für Verminde-

180 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 494.

rung des jeweiligen Risikos lassen sich in der Regel monetär messen. Dabei sind die Kosten für technische oder bauliche Maßnahmen zu bedenken. Ebenso müssen die bei Überwälzung anfallenden Versicherungskosten oder die Kosten des Outsourcings der entsprechenden IT-Leistung betrachtet werden. Der so entstehende Datenpool ist als Grundlage für die Risikobewertung im Verlustverteilungsansatz zu verwenden. Je nach individuellem Ansatz sind ggf. zusätzliche Daten, wie typischer und maximaler Schaden bzw. Eintrittswahrscheinlichkeit und die verlusttragende Organisationseinheit, mit zu erheben.[181]

Neben der Prozessanalyse und den daraus resultierenden qualitativen Schätzungen des Risikopotenzials sind interne Schadensdatenbanken aufzubauen, die aufgetretene Schäden sowie deren Auswirkungen aufnehmen und damit eine quantitative Datengrundlage für die Risikosituation des Unternehmens liefern. Es entsteht eine interne Schadensdatenbank, auf deren Basis das ORM die eigene Risikosituation einschätzen kann.

Zusätzlich zu den qualitativen Schätzungen und dem Aufbau interner Verlustdatenbanken fordert Basel II auch die Verwendung von externen Datenquellen. Zur Sammlung von Verlustdaten haben sich zahlreiche Datenkonsortien gebildet, die auf einer homogenen Basis Schadensereignisse erfassen. Die Daten werden vom Betreiber des Konsortiums anonymisiert und den angeschlossenen Instituten in aggregierter Form zur Verfügung gestellt. Als Betreiber fungieren in den meisten Fällen Dritte (bspw. Wirtschaftsprüfungsgesellschaften). Ohne Anspruch auf Vollständigkeit seien hier beispielhaft drei solcher Datenkonsortien aufgeführt: Die Operational Risk Data eXchange Association (ORX), die Global Operational Loss Database (GOLD) sowie das Datenkonsortium zu operationellem Risiko (DaKOR). Die aus externen Verlustdatenbanken bezogenen Daten können allerdings nicht ohne weiteres in die eigenen Modelle zur Risikobewertung einbezogen werden. Durch die Anonymisierung der Daten ist es schwer möglich, die Relevanz eines Datensatzes für das eigene Institut zu bewerten. Eine Skalierung der Daten muss hinsichtlich der Größe der Bank, der Tätigkeitsbereiche sowie der Komplexität der Geschäfte vorgenommen werden. Einen Teil der Schadensdaten kann man relativ einfach bestimmten Ereignissen zuordnen (bspw. Naturkatastrophen,

181 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 492.

Terroranschläge vom 11. September 2001). In der IT ist eine solche Zuordnung und damit die Anpassung der Daten auf die eigene Situation schwer möglich. Größe, Tätigkeitsfelder und die Komplexität der Geschäfte sind wenig aussagekräftige Indikatoren für vergleichende Überlegungen in der IT-Sicherheit.

Die Bewertung bleibt weiterhin eine große Herausforderung im Management von IT-Risiken. Die Frage nach den Kosten der Unsicherheit lässt sich durch die Erfassung des Schadenspotenzials prinzipiell beantworten. Allerdings sind die oben angeführten Ansätze zur Bewertung und Datenerhebung in der IT-Sicherheit aktuell noch unzureichend implementiert und sowohl interne als auch externe Schadensdatenbanken werden erst mit entsprechenden Datenmengen verlässliche Ergebnisse liefern. Somit müssen sich das ORM und das ISM in einigen Bereichen auf teilweise durch subjektive Einstellungen verzerrte Schätzungen verlassen. Mittelfristig kann durch die Prozessorientierung und die detaillierte Modellierung der Abhängigkeiten allerdings eine verlässliche Bewertungsgrundlage hergestellt werden, die den Anforderungen des ORM entspricht.

4.3.3 Steuerung von IT-Risiken

Die Steuerung der IT-Risiken muss auch nach Integration in das ORM Aufgabe der Experten auf dem Gebiet – und damit des ISM bleiben. Das ISM tritt hier allerdings nicht als alleiniger Entscheidungsträger über die zu treffenden Maßnahmen auf. Viel mehr sind die Experten aus dem ISM Berater für die Prozessverantwortlichen in den Abteilungen. Das ISM muss Kosten und Nutzen der Sicherheitsmaßnahmen aufzeigen. Die Entscheidung über die Maßnahme hat allerdings immer der für das Produkt oder die Dienstleistung Verantwortliche zu treffen.[182] Die Maßnahmenplanung muss durch eine zentrale Stelle koordiniert werden, in der auch die IT-Sicherheitsbudgets zugewiesen werden. Die bisher oftmals pauschale Bereitstellung von Mitteln für Sicherheitsinvestitionen ist für alle umfangreicheren Maßnahmen (z. B. Reorganisationen, komplexere technische Maßnahmen) durch eine systematische Planung zu ersetzen, die in das ORM

182 Vgl. Nägli, Hans-Peter: Management der Informationssicherheit – Erfahrungen eines Finanzdienstleisters, a. a. O., S. 87 f.

zu integrieren ist. Alle Maßnahmen müssen im Gesamtkontext der operationellen Risiken reflektiert werden.[183]

Um hier eine methodisch nachvollziehbare Einordnung der verschiedenen Steuerungsmöglichkeiten vorzunehmen, wird zunächst zwischen technischen und organisatorischen Maßnahmen unterschieden. Die technische Ebene beinhaltet alle Vorkehrungen und Maßnahmen technischer Art, die verwendet werden, um die identifizierten Risiken zu steuern. Organisatorische Maßnahmen sind auf Ebene des Managements einzuführen, um die informationstechnischen Risiken einzuschließen, die durch den Einsatz von Technologie nicht ausgeschlossen werden können. Die Managementebene befasst sich aber auch mit der Gesamtsicherheitskonzeption, bspw. mit der Frage, in welchen Abständen die eingesetzten Technologien zu überprüfen sind.

Auf organisatorischer und technischer Ebene werden dann die Handlungsalternativen des Risikomanagements (Vermeiden, Vermindern, Überwälzen und Akzeptieren)[184] eingeordnet. Diese Einordnung kann allerdings nicht immer trennscharf erfolgen. Gerade organisatorische Maßnahmen sind in ihrer Wirkung oft erst im Nachhinein zu bewerten. Hat eine organisatorische Maßnahme nicht den gewünschten Erfolg, kann der ursprünglich gewünschte Effekt der Risikovermeidung ggf. nur zu einer Risikoverminderung führen. Im schlimmsten Fall ist das Risiko nachträglich zu akzeptieren (vgl. Tab. 3).

Die technischen Maßnahmen zur Steuerung von IT-Risiken entwickeln sich mit den Anwendungen weiter und sollen in der vorliegenden Arbeit nicht detailliert dargestellt werden. Insbesondere betriebswirtschaftliche Standardanwendungen bringen als integrierte Lösungen bereits Sicherheitsmechanismen mit, die durch Konfiguration an die spezifischen Einsatzzwecke anzupassen sind. Tab. 3 führt beispielhaft als eine Möglichkeit zur Vermeidung von Risiken die Systemreplikation an. Eine vollständig redundante Systemumgebung (möglichst an räumlich getrennten Standorten) ist allerdings unter Kostenaspekten als unrealistisch einzustufen. Solche Redundanzen sind nur in Teilbereichen (z. B. zentrales Rechenzentrum) bzw. temporär in Umstellungsphasen sinnvoll. Die Redundanz wird deshalb neben Firewalls, Archivierung und Datensicherung sowie

183 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 493.

184 Vgl. Kapitel 3.3.4.

Verschlüsselungstechniken im Bereich der Risikoverminderung angeführt. Auf welches Niveau die Risiken durch diese Maßnahmen zu vermindern sind, muss für jedes Risiko bewertet werden. Beispielhaft sei dazu die Datensicherung angeführt. Theoretisch können stündliche Vollsicherungen aller Daten durchgeführt werden, wodurch das Risiko des Datenverlusts weitgehend minimiert wird. Der Zyklus der Datensicherung muss sich aber an den Veränderungen der Daten und deren Schutzbedarf orientieren – eine stündliche Vollsicherung historischer (und damit nicht mehr veränderlicher) Transaktionsdaten ist unangemessen. Zur technischen Administration und Überwachung komplexer Systemumgebungen sind am Markt zahlreiche Systemmanagementumgebungen (z. B. IBM Tivoli, HP OpenView) verfügbar.

	Technisch	Organisatorisch
Vermeiden	Systemreplikation	Rollenkonzepte
Vermindern	Firewall Archivierung Datensicherung Redundanz Verschlüsselung	Awareness-Kampagnen
Überwälzen		Outsourcing Versicherungen
Akzeptieren	Keine technische oder organisatorische Maßnahme.	

Tab. 3: Handlungsalternativen zur Steuerung von IT-Risiken

Das Überwälzen stellt auf technischer Ebene keine Handlungsoption dar. Unter Überwälzen wird die Übertragung des Risikos auf Dritte verstanden. Dies ist auf rein technischer Ebene nicht möglich. Mögliche Auslagerungen auf Dritte und Versicherungen der Systeme werden im Rahmen dieser Arbeit als organisatorische Maßnahmen eingeordnet.

Bestimmte Risiken sind durch technische Maßnahmen nicht zu vermeiden und müssen durch entsprechende organisatorische Maßnahmen gesteuert werden. Die Gesamtheit der Prozesse, die die Informationssicherheit im Unternehmen sicherstellen sollen, ist in einer Richtlinie als „Security Policy“ festzuhalten. Die Sicherheitsrichtlinie gilt für alle Teilbereiche des Unternehmens und kann deshalb nicht von ISM verantwortet werden.

In ihr muss unmissverständlich der zu schützende Gegenstand benannt bzw. definiert werden.[185]

Organisatorische Maßnahmen sind nicht geeignet, Risiken vollständig zu vermeiden, da durch den Faktor Mensch immer ein Restrisiko verbleibt. Menschen können sich über Organisationsrichtlinien hinwegsetzen und damit Schaden anrichten. Fordert eine Sicherheitsrichtlinie bspw. einen regelmäßigen Wechsel eines Zugangspasswortes, kann nicht verhindert werden, dass das jeweils aktuelle Passwort als Notizzettel unter der Schreibtischunterlage zu finden ist. Solche Situationen lassen sich z. B. im Rahmen von Awareness-Kampagnen[186] ansprechen, um somit das durch den Mitarbeiter verursachte Risikopotenzial zu vermindern. Für den Erfolg solcher Maßnahmen ist die nachhaltige Unterstützung aller Managementebenen notwendig. Das klare Bekenntnis zum Schutz und zur herausgehobenen Bedeutung der Ressource Information muss in Unternehmen von allen Mitarbeitern gelebt werden. Während das Überwälzen von IT-Risiken auf technischer Ebene relativ unbedeutend ist, ist es ein wesentlicher Ansatzpunkt für organisatorische Maßnahmen. Die Möglichkeit zum Outsourcing von IT-Leistungen stellt eine Handlungsoption zur Überwälzung von Risiken dar. Die Regelungen des KWG setzten der Auslagerung von zentralen IT-Funktionen allerdings enge Grenzen.[187] Neben dem Outsourcing bietet sich zur Überwälzung der Schadenswirkung die Versicherung gegen Risiken an. Die wesentlichen IT-Versicherungen sind: Sachversicherungen für Hard- und Software, Folgekostenversicherungen für Betriebsunterbrechungen, Vertrauensschadenversicherungen bei Computermissbrauch sowie Datenschutzversicherungen, die den Bereich Rechtsschutz und Haftpflicht bei Verstößen gegen das BDSG abdecken.[188]

Das Restrisiko, dass unter Beachtung der Kosten weder durch technische noch organisatorische Maßnahmen weiter reduziert werden kann, muss das Unternehmen schließlich akzeptieren. Die Entscheidung über den optimalen Einsatz von Mitteln zur Risiko-

185 Vgl. Sacher, Paulus: Risiken beim Einsatz von Informationstechnologie, a. a. O., S. 407.

186 Awareness-Kampagnen werden initiiert, um bestimmte Themen (hier: Informationssicherheit) im Bewusstsein einer Zielgruppe zu verankern und auf Problembereiche hinzuweisen.

187 Vgl. Kapitel 2.2.2.

188 Vgl. Tappert, Rainer: EDV-System-Prüfung – Bankbetriebliche Revisionsinformatik, a. a. O., S. 59.

eingrenzung hat immer durch den Verantwortlichen des mit dem IT-Risiko verbundenen Prozesses zu erfolgen. Das ISM kann dabei nur beratend zur Seite stehen.[189]

Es bleibt festzustellen, dass die Handlungsalternativen im Bereich der IT-Sicherheit durch die Kombination von technischen und organisatorischen Maßnahmen als komplex einzustufen ist. Als wesentliche Handlungsoptionen sind für die Praxis insbesondere Ausweichsysteme und Datensicherungen, organisatorische Regelungen für die Störungsbeseitigung und Schadensverhinderung sowie Sach- und Folgekostenversicherungen in Betracht zu ziehen.[190]

4.3.4 IT-Risikokontrolle

Mit der Risikokontrolle schließt sich der Risikomanagementkreislauf. Die Maßnahmen der Risikosteuerung werden darin überwacht und somit ermittelt, welche Teile der Sicherheitsrichtlinie gut umgesetzt werden konnten und in welchen Teilbereichen weiterhin Probleme bestehen. Zudem ist der Einsatz bestimmter Maßnahmen bzw. Produkte dahingehend zu bewerten, ob diese den erwarteten Sicherheitsgewinn gebracht haben oder ob die Maßnahme als fehlgeschlagen einzustufen ist.

Problematisch in der Risikokontrolle ist der Informationsfluss zwischen ORM und ISM. Aus automatisch erstellten Protokollen entstehen zahlreiche Daten, aus denen die bestehende Situation beurteilt werden kann. Diese sog. Security Audit Logs sind in vielen betriebswirtschaftlichen Anwendungen implementiert und können durch entsprechende Konfiguration sicherheitsrelevante Tätigkeiten protokollieren. Diese Protokolle müssen von den Experten im ISM regelmäßig analysiert werden. Auffällig sind bspw. mehrfache Anmeldeversuche in kurzer Zeit, bei denen zusätzlich verschiedenen Nutzerkennungen verwendet wurden. Die Schnittstellen eines Unternehmens zu dessen Geschäftspartnern und Kunden sind in einem „Intrusion Detection System“ zu überwachen und die Reports ebenfalls zu analysieren.[191] Zur technischen Überwachung der Systeme sind die

189 Vgl. Nägli, Hans-Peter: Management der Informationssicherheit – Erfahrungen eines Finanzdienstleisters, a. a. O., S. 87 f.

190 Vgl. Stickel, Eberhard; Groffmann, Hans-Dieter; Rau, Karl-Heinz (Hrsg.): Gabler Wirtschaftsinformatiklexikon, Wiesbaden: Gabler 1997, S. 646.

191 Vgl. Paulus, Sacher: Risiken beim Einsatz von Informationstechnologie, a. a. O., S. 409 f.

bereits oben angeführten Anwendungen zum Systemmanagement einzusetzen. Dadurch wird eine systemübergreifende Betrachtung von Störungen und sicherheitsrelevanten Vorfällen möglich. Die Konfiguration dieser Anwendungen ist allerdings regelmäßig auf Aktualität und Angemessenheit zu überprüfen, da nur so verwendbare Ergebnisse sichergestellt werden.

Das technische Reporting von Sicherheitsvorfällen stellt aber nur ein Bereich der Kontrolle dar. Organisatorische Schwächen sind nicht in automatisierten Protokollen zu erkennen, sondern können nur im Gespräch bzw. in Befragungen der betroffenen Mitarbeiter aufgedeckt werden. Dadurch sollen die Umsetzung der Sicherheitsrichtlinie überprüft sowie die Schwächen der Richtlinie selbst aufgezeigt werden.

Sowohl auf technischer als auch auf organisatorischer Ebene existieren Probleme in der Informationsbeschaffung. Das ISM hat relativ wenige Informationen über den Stand der IT-Sicherheit in den dezentralen Einheiten. Die vorhandenen Informationen werden vorwiegend in Form von Reviews und Audits erhoben. Es fehlt ein systematischer Prozess zur Informationsgewinnung in Form eines Informations-Push. Dies bedeutet bspw. ein automatisiertes Reporting über kritische Sicherheitsvorfälle, das analog zu den Prozessen des operationellen Risikomanagements durchgeführt wird. Entsprechende Berichtswege sind von ISM und ORM zu etablieren, um eine Grundlage für zentrale Maßnahmenentscheidungen zu erhalten. Kritische Sicherheitsvorfälle sind auf direkten Berichtswegen an das ORM zu melden. Eine Zusammenfassung der Sicherheitssituation ist in regelmäßigen Abständen von ISM zu erstellen und als Report an das ORM zu liefern. Durch die Entwicklung dieser Prozesse und die Etablierung von Berichtslinien wird das ISM und das ORM in die Lage versetzt, bessere Aussagen über den Stand der Sicherheit im Unternehmen zu treffen. Dadurch ist die Einleitung von Gegenmaßnahmen früher möglich.

Die Kontrolle der IT-Risiken ist nicht als Abschluss des Risikomanagements zu sehen. Sowohl die implementierten Maßnahmen als auch die organisatorische Verankerung der Sicherheitsziele in der Security Policy müssen regelmäßig hinterfragt werden und initieren damit den Kreislauf der Risikoidentifikation, -bewertung und -steuerung neu.

4.4 Aufbauorganisation

Der Integration des ISM in das ORM muss auch auf organisatorischer Seite durch Aufgabe der starken Dezentralisation innerhalb des ISM Rechnung getragen werden. Die bestehenden Organisationsformen, in der verschiedene Rollen und Aufgaben teilweise zentral, teilweise dezentral verteilt sind, müssen durch Reorganisation an die Anforderungen einer integrierten Vorgehensweise angepasst werden. Das ISM ist als zentrale Unterstützungsfunktion zu positionieren. Dabei ist genau festzulegen, wer welche Aufgaben innerhalb der Sicherheits- und Risikoorganisation wahrnehmen soll.[192]

Um den erhöhten Anforderungen an die Informationssicherheit gerecht zu werden und um damit die Bedeutung des ISM zu unterstreichen, ist der Chief Security Officer (CSO)[193] mit angemessenen Kompetenzen auszustatten. Er koordiniert in Abstimmung mit dem ORM die technischen, organisatorischen und ggf. baulichen Maßnahmen der Risikosteuerung und ist für die Weiterentwicklung der eingesetzten Methoden verantwortlich. In der zentralen Einheit des ISM werden die Vorgaben für die dezentralen Sicherheitsmanager erarbeitet. Für die Verankerung des ISM in der Aufbauorganisation lassen sich folgende Empfehlungen formulieren:

1) **Repräsentanz auf Unternehmensebene:** Die IT-Sicherheit als wichtiger Teil der Sicherheitsorganisation im Finanzdienstleistungssektor ist in der Unternehmensleitung bisher unterrepräsentiert. Der Sicherheitsbeauftragte sollte als CSO mit der Bedeutung der IT-Sicherheit entsprechenden Kompetenzen ausgestattet sein.

2) **Methodenfunktion einer zentralen ISM-Einheit:** Die Vorgabe von Methoden für das Management von IT-Risiken durch zentrale Einheiten ist bisher die Ausnahme. Unter der Verantwortung des CSO sind Methoden und Standards zu entwickeln, die unternehmensweit in den dezentralen Organisationseinheiten verbindlich einzusetzen sind.

---

192 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 494.

193 Die Bezeichnung Chief Security Officer (CSO) wird im Rahmen der Globalisierung genutzt, um einheitliche internationale Titel zu schaffen. Der CSO hat in Deutschland keine rechtliche Bedeutung. Er nimmt als sicherheitstechnischer Leiter eine Managementfunktion auf Vorstands- bzw. Geschäftsführungsebene ein. Vgl. o. V.: Wikipedia – Die freie Enzyklopädie, Online im Internet: http://de.wikipedia.org/wiki/ Chief_Security_Officer, 25.06.2006.

3) **Kontrollfunktion der zentralen Einheit:** Das im Risikomangement bewährte Prinzip der Eigenverantwortlichkeit und Kontrolle ist auch im ISM anzuwenden. Dabei ist auf einen dauerhaften Informations-Push zu achten, der das Sicherheitscontrolling auf Basis von Audits und Reviews ergänzt.[194]

In der Sicherheitsorganisation müssen zur Sicherung des effizienten Ablaufs klare Schnittstellen zwischen ORM und ISM definiert werden. Die Schnittstellenproblematik stellt sich in allen Bereichen, die in das Management operationeller Risiken eingebunden sind. Neben der IT-Abteilung sind das bspw. Innenrevision und Rechtsabteilung.

Die Heterogenität der operationellen Risiken bringt an den zahlreichen Schnittstellen zum ORM Reibungsverluste mit sich. Um eine Zusammenarbeit mit dem ISM erfolgreich zu gestalten, dürfen von ORM nicht nur neue Aufgaben zugewiesen werden. Die Vorteile der gemeinsamen Betrachtung müssen dem ISM aufgezeigt werden. Nur wenn der Nutzen klar erkennbar ist, kann eine aktive Mitarbeit in Risiko- und Sicherheitsfragen erwartet werden. Um die durch die integrierte Sichtweise entstehenden Reibungsverluste zu minimieren, sind alle Aufgaben und Zuständigkeiten klar zu definieren. Dadurch kann das ISM auf organisatorischer Ebene mit konsistenten Schnittstellen und Organisationsprinzipien effizient arbeiten. Zu den Schnittstellen gehören definierte Reports aus der Risikokontrolle, aber auch Gremien, in denen gemeinsame Informationsgrundlagen geschaffen werden. Das ISM arbeitet dem ORM subsidiär zu. Durch die entsprechende organisatorische Einbindung und effizienten Informationsfluss sind Konkurrenzgedanken zu minimieren, um eine Zusammenarbeit zu fördern.

4.5 Überblick zum Integrationspotenzial

In den vorangegangenen Kapiteln wurde auf Ebene von Zielsystemen, Prozessen und Organisationsstrukturen das Potenzial für Effizienzsteigerungen einer integrierten Betrachtungsweise von ORM und ISM betrachtet. Die daraus gewonnenen Erkenntnisse werden in Abb. 14 zusammenfassend dargestellt und auf zentrale Ergebnisse wird in der Folge kurz eingegangen.

194 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 494 f.

Das Sachziel des ISM unterstützt das Sachziel des ORM. Gemeinsame Aufgabe beider Bereiche ist die Sicherung der Unternehmenswerte. Dabei hat das ORM einen wesentlich weiteren Fokus als das ISM, ist in der Erreichung seiner Ziele im Rahmen der Subsidiarität auf die Zusammenarbeit mit Spezialisten der Fachabteilungen angewiesen. Die Ziele beider Bereiche werden in Richtlinien dokumentiert, die auf Ebene der Geschäftsführung zu verabschieden sind und unternehmensweite Gültigkeit besitzen. Auf Zielebene ist einer integrierten Betrachtung beider Bereiche folglich möglich. Die Zielsysteme von ORM und ISM sind miteinander vereinbar.

Auf Prozessebene liegt die Methodenverantwortung für die Risikoidentifikation beim ORM. Risikokategorien und Qualitätsstandards für die Risikoerfassung werden im ORM festgelegt, da sie vor dem Hintergrund unternehmensweiter Anwendbarkeit und Gültigkeit zu formulieren sind. Für die Identifikation der Risiken sind drei Teilbereiche zu erfassen: Die zu schützenden Werte können im ersten Schritt vom ISM bottom-up aufgenommen werden. Die Analyse der Geschäftsprozesse (Schritt 2) sowie die Einbeziehung von Risiken aus den rechtlichen Rahmenbedingungen (Schritt 3) ist gemeinsame Aufgabe beider Bereiche. Für die Analyse der Geschäftsprozesse müssen ISM und ORM gemeinsam mit den Fachabteilungen Prozessmodellierung betreiben und darin IT-Systeme aufnehmen. Die Risiken aus rechtlichen Rahmenbedingungen sind je nach Zielrichtung der Vorgaben eher im ORM (z. B. Basel II, KonTraG) bzw. ISM (z. B. BDSG) zu behandeln. Als Resultat wird im gemeinsamen Risikoinventar definiert, *was* im Rahmen des Risikomanagements zu schützen ist. Mit der Aufnahme der Bedrohungen wird zudem beantwortet, *wovor* es zu schützen ist.

In der anschließenden Risikobewertung werden auf Basis von Schadensszenarien sowie internen und externen Verlustdaten gemeinsame Bewertungsmodelle erarbeitet. Dabei beschränkt sich die detaillierte Risikoanalyse auf Bereiche, in denen mittlere bis hohe Schadenspotenziale erwartet werden müssen. Für Bereich mit geringerem Schadensausmaß können die Risiken mit Methoden des IT-Grundschutz adressiert werden. In die Bewertung sind interne und externe Verlustdatenbanken, Schadensszenarien auf Basis der Analyse der Geschäftsprozesse sowie Expertenmeinungen einzubeziehen. Wie die Modelle zur Bewertung von IT-Sicherheit genau ausgestaltet sind, kann im Rahmen dieser Arbeit nicht abschließend beantwortet werden.

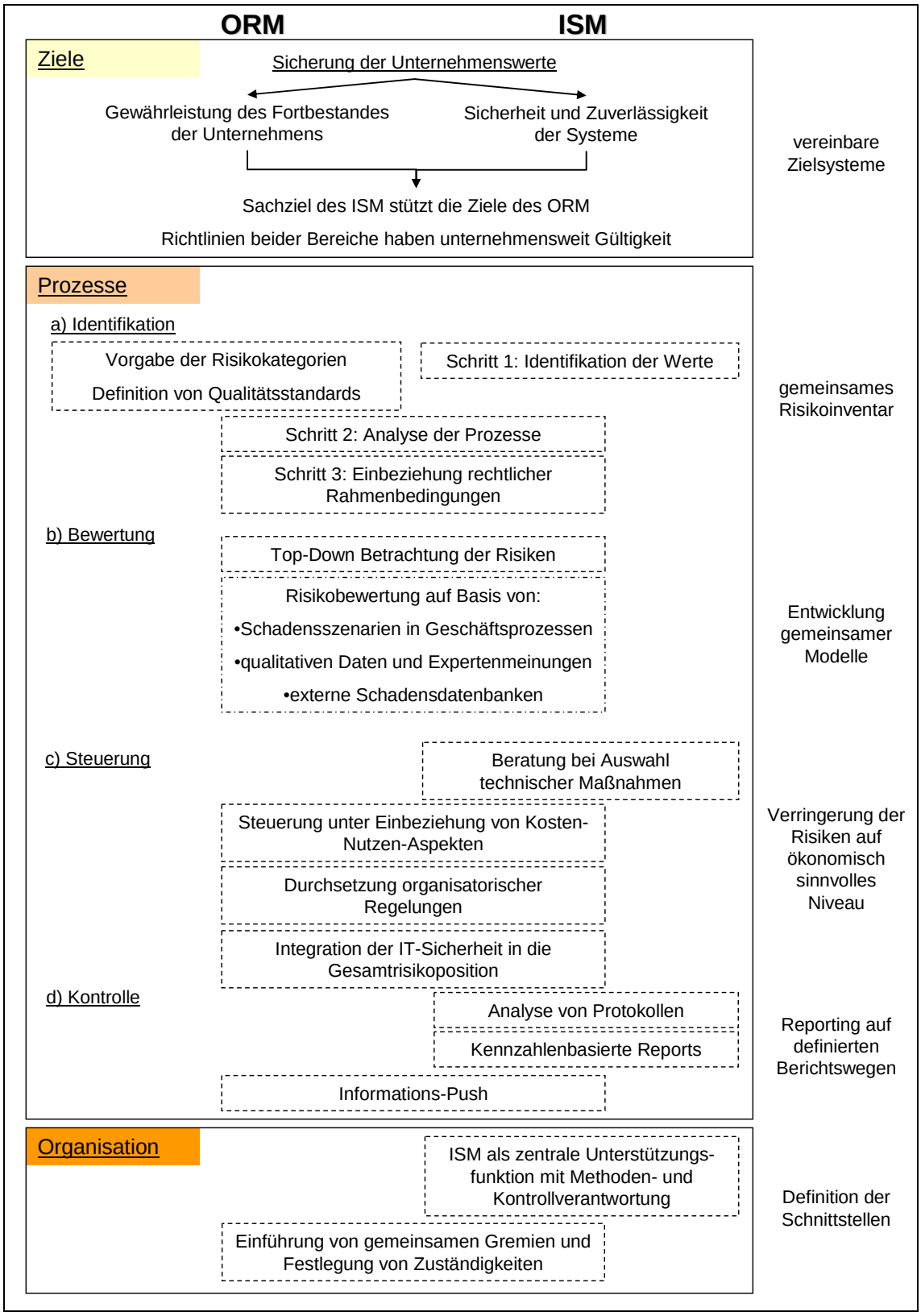

Abb. 14: Zusammenfassung des Integrationspotenzials

Bei der Steuerung der Risiken im IT-Sicherheitsbereich ist das ISM als Spezialist für die Einführung technischer Maßnahmen Ratgeber für die Prozessverantwortlichen im gesamten Unternehmen. Die Steuerung von IT-Risiken muss unter Kosten-Nutzen-Aspekten in die Gesamtrisikosituation des Unternehmens einbezogen werden. ORM und ISM konzipieren dabei gemeinsame Lösungen auf technischer und organisatorischer Ebene, die das Risikopotenzial auf ein ökonomisch sinnvolles Niveau reduzieren. Besondere Beachtung finden dabei organisatorische Regelungen, die durch Verankerung eines angemessen Sicherheitsbewusstsein und einer Risikokultur gemeinsame Aufgabe von ORM und ISM ist.

In der Risikokontrolle ist die Abkehr von periodischen Audits hin zu kennzahlenbasierten und automatisiert ablaufenden Überwachungsmechanismen sinnvoll. Informationen zur IT-Sicherheit müssen in Form eines Informations-Push in das Risikomanagement eingehen. Die im ISM generierten Reporte sind auf definierten Berichtswegen dem ORM zur Verfügung zu stellen. Zudem sind auf automatisiertem Weg Informationen über kritische IT-Sicherheitsvorfälle an den CRO zu leiten.

Auf organisatorischer Ebene ist das ISM durch Reorganisation als zentrale Unterstützungsfunktion mit entsprechenden Kompetenzen zu positionieren. Mit der Stelle des CSO werden Sicherheitsaspekte auf Vorstands- bzw. Geschäftsführungsebene institutionalisiert. Schnittstellen zwischen ORM und ISM sind klar zu definieren, um Reibungsverluste zu minimieren. Dies erfolgt durch die Einführung gemeinsamer Gremien und die Definition von Berichtswegen.

5 Zusammenfassung und Ausblick

Die steigende Abhängigkeit von IT-Systemen bringt im Finanzdienstleistungssektor einen erhöhten Sicherheitsbedarf im IT-Bereich mit sich. Erhöhte Komplexität, zunehmende Vernetzung und die gestiegen Durchdringung der Geschäftsprozesse mit IT führen dazu, dass die Schadenspotenziale der IT-Systeme zunehmend einem aktiven Management unterliegen.

Die Reduktion der Gefährdungen aus der IT ist ein zentrales Anliegen um die Glaubwürdigkeit und das Vertrauen der Kunden in die Dienstleistungen der Banken aufrecht

zu erhalten. Das Thema IT-Sicherheit wird deshalb von einer steigenden Anzahl von regulatorischen Anforderungen behandelt. Sicherheit kann dabei sowohl aus technischer Sicht als *Sicherheit der Systeme* als auch aus Sicht der Betroffenen als *Sicherheit vor dem System* verstanden werden. Die Aufteilung in diese beiden Sichtweisen wird als Konzept der dualen Sicherheit bezeichnet. Als Schutzziele ergeben sich darin: Vertraulichkeit, Verfügbarkeit, Integrität, Zurechenbarkeit und Revisionsfähigkeit bzw. Rechtsverbindlichkeit.[195] Jede Einzelne der im Rahmen dieser Arbeit betrachteten aufsichtsrechtlichen Vorgaben betrachtet IT-Sicherheit aus einer anderen Perspektive. Folglich liegt auch der Schwerpunkt der Vorgaben nicht immer auf allen fünf oben genannten Schutzzielen. Daraus ergibt sich ein komplexes Umfeld von rechtlichen Anforderungen, Verlautbarungen und Standards, die sowohl nach ihrer inhaltlichen Reichweite, als auch nach ihrer rechtlichen Verbindlichkeit zu ordnen sind.

Es zeigt sich, dass für die verschieden Kreditinstitute der deutschen Bankenlandschaft differenziert betrachtet werden muss, welche Anforderungen zu erfüllen sind. Die Regelungen des KWG, des BDSG, des WpHG sowie die Inhalte von Basel II sind von allen Kreditinstituten in Deutschland zu erfüllen. Zweigniederlassungen von ausländischen Banken sind allerdings nicht an die Regelungen des KonTraG und der MaRisk gebunden. Diese gelten für die Großbanken, den Genossenschaftssektor, die Sparkassen und Girozentralen sowie die Gruppe der Regionalbanken und sonstigen Kreditinstitute. Die erweiterten Anforderungen des SOA sind schließlich nur von einem kleinen Teil der deutschen Institute aufgrund ihres Listings an der NYSE bindend: die Dresdner Bank (als Konzerntochter der Allianz) und die Deutsche Bank.[196]

Die Stärkung der Interessen der Eigenkapitalgeber und die Unternehmenskrisen der jüngeren Vergangenheit sind Grundlage für die Forderung nach einem effizienteren Risikomanagement in den Unternehmen. Durch Basel II wird in die Eigenkapitelberechnung der Banken erstmal die Kategorie der operationellen Risiken einbezogen. Operationelle Risiken beinhalten alle von innen und außen kommenden Störungen, die das Unternehmen bei der Erbringung der Leistung behindern können. Verluste können dabei infolge von Unzulänglichkeiten oder des Versagens interner Verfahren, Menschen und

195 Vgl. Kapitel 2.1.2.

196 Vgl. Kapitel 2.5.2.

Systeme oder infolge externer Ereignisse auftreten. Während im Bankenbereich im Risikomanagement bisher auf Markt- und Kreditrisiken abgestellt wurde, müssen operationelle Risiken nun in das Risikomanagement aufgenommen werden. IT-Risiken sind dabei ein Bestandteil der operationellen Risiken und sind folglich im Risikomanagement zu beachten.

Die Ursprünge des Risikomanagements sind in der Versicherungswirtschaft zu finden. Hier war es primär Aufgabe, die Höhe der zu zahlenden Prämien optimal zu gestalten. Heute wird unter Risikomanagement der planvolle Umgang mit Risiken in einem Unternehmen verstanden. Als Risiko wird dabei die Möglichkeit eines Schadens oder Verlustes als Konsequenz eines bestimmten Verhaltens oder Geschehens verstanden; dies bezieht sich auf die Gefahrensituationen, in denen nachteilige Folgen eintreten können, aber nicht müssen.[197]

Risikomanagement wird als aktiver und iterativer Prozess verstanden.[198] Nach der Formulierung einer Risikostrategie startet ein Kreislauf von Risikoidentifikation, Risikobewertung, Risikosteuerung und Risikokontrolle. Ziel der Risikoidentifikation ist die vollständige Aufnahme aller Risiken in ein Risikoportfolio. Mit Hilfe von Kollektions- und Suchmethoden wird mit der Risikoidentifikation die Grundlage für das aktive Management der Risiken geschaffen. Im zweiten Schritt sind Risiken qualitativ zu beurteilen und quantitativ zu bewerten. Für jedes Risiko ist ein Schadenspotenzial abzuleiten, dass sich aus der Multiplikation von Eintrittswahrscheinlichkeit und Schadensausmaß ergibt. Um diese Berechnung vornehmen zu können, müssen ausreichende Datenmengen zur Bestimmung von Eintrittswahrscheinlichkeiten und Schadensausmaßen vorliegen. Bestimmte Risikokategorien mit geringen Eintrittswahrscheinlichkeiten und hohen Schadensausmaßen erfüllen diese Anforderung jedoch nicht. In Abwesenheit einer entsprechenden Datengrundlage muss die Bewertung auf Basis von internen Schätzungen und Expertenmeinungen erfolgen. In die Gesamtbewertung der Risikosituation eines Unternehmens sind Wechselwirkungen einzubeziehen, die sich durch kompensatorische Effekte nicht perfekt korrelierter Einzelrisiken ergeben können. Im Anschluss an die Bewertung erfolgt die Steuerung der Risiken. Dabei wird das unternehmerische Chan-

197 Vgl. Kapitel 3.2.

198 Vgl. Kapitel 3.3.1.

cen-Risiko-Profil optimiert, indem die risikopolitischen Handlungsalternativen des Vermeidens, Vermindern, Überwälzens und Akzeptierens unter Chancen- und Risikoaspekten abgewogen werden. Unternehmen sollten Risiken nur dann auf sich nehmen, wenn sie die entsprechenden Kompetenzen zum Management dieser Risiken besitzen. Die Risikokontrolle bildet schließlich den Abschluss des Risikomanagementkreislaufs bzw. initiiert einen neuen Durchlauf des Prozesses. Die Kontrolle ist als eine Art Risikoradar im gesamten Prozess verankert und überwacht den Erfolg der Maßnahmen durch Vergleich der tatsächlichen und der anhand risikopolitischer Grundsätze definierten Risikosituationen.[199] Auf organisatorischer Ebene ist das Risikomanagement in einer Mischform zwischen den beiden Extremen eines integrativen Risikomanagements auf der einen und eines verselbstständigten Risikomanagements auf der anderen Seite einzuordnen. Es hat sich eine subsidiäre Aufgabenverteilung zwischen dem zentralen Risikomanagement und der Unterstützung aus den Fachabteilungen etabliert.

Die Betrachtung von Risiken der IT-Sicherheit ist sowohl Bestandteil des Risikomanagements im Bereich operationeller Risiken als auch des IT-Sicherheitsmanagements. Das Management operationeller Risiken ist im Gegensatz zum ISM ein relativ neues Betätigungsfeld für Banken. Gewachsene Strukturen des ISM und bisher isoliert parallel durchgeführte Aktivitäten führen zu Ineffizienzen, die im Rahmen von Kapitel 4 dieser Arbeit betrachtet werden. Dabei werden Ansatzpunkte für die Integration der beiden Bereiche dargestellt um das Effizienzpotenzial einer integrierten Betrachtungsweise zu dokumentieren.

Für die Integration des ISM in das ORM werden die Zielsysteme beider Bereiche betrachtet. Da sich sowohl das ISM mit dem Sachziel „Sicherheit und Zuverlässigkeit der Systeme“ als auch das ORM mit dem Sachziel „Gewährleistung des Fortbestandes des Unternehmen“ dem gemeinsamen Ziel „Sicherung der Unternehmenswerte“ unterordnen, liegen komplementäre und vereinbare Zielsysteme vor. Das Sachziel des ISM stützt dabei das Sachziel des ORM.

Auf Prozessebene werden für die Integration die vier Schritte des Risikomanagementkreislaufs betrachtet. In der Risikoidentifikation sind zur Aufstellung eines vollständi-

199 Vgl. Kapitel 3.3.2 bis 3.3.5.

gen Risikoinventars drei Ebenen zu betrachten. Das ISM ist zunächst für die Identifikation der im Bereich der IT-Sicherheit zu schützenden Werte (Hard- und Software, Daten, Kommunikationsnetze) verantwortlich. Um die Komplexität und die Zusammenhänge verschiedener IT-Komponenten zu analysieren, sind im zweiten Schritt Geschäftsprozesse zu modellieren und eine Einordnung der Werte in den IT-gestützten Geschäftsprozess vorzunehmen. Diese Aufgabe ist von ORM und ISM gemeinsam mit der Unterstützung der Fachabteilungen durchzuführen. Im dritten Schritt sind Risiken aus rechtlichen Rahmenbedingungen einzubeziehen. Diese sind ebenfalls gemeinsam von ORM und ISM zu behandeln, da sich die Anforderungen verschiedener Gesetze und Verlautbarungen teilweise inhaltlich überschneiden. Die Bewertung der Risiken aus der IT-Sicherheit stellt eine große Herausforderung für ORM und ISM dar. Während im ISM monetäre Bewertungen und kennzahlenbasierte Analysen bisher eine untergeordnete Rolle spielten, ist das ORM gerade auf solche Daten angewiesen. Um eine entsprechende Bewertung zu ermöglichen müssen beide Bereiche gemeinsam geeignete Modelle entwickeln. Darin sind die Schadensszenarien auf Ebene der Geschäftsprozesse, qualitative Daten und Expertenmeinungen sowie externe Schadensdatenbanken einzubeziehen. Es muss allerdings festgestellt werden, dass dieser Bereich aufgrund fehlender Daten und Modelle noch Entwicklungspotenzial aufweist. In der Steuerung der IT-Risiken steht das ISM als Berater allen Fachabteilungen des Unternehmens zur Verfügung. Gemeinsam mit dem ORM ist die Risikosteuerung unter Kosten-Nutzen-Aspekten zu forcieren und die IT-Sicherheit in die Gesamtrisikosituation einzubeziehen. Die Entscheidung, ob ein Risiko akzeptiert wird und bzw. ob das risikopolitische Handlungsinstrumentarium zur Reduzierung der Risiken Anwendung findet, muss allerdings vom Prozessverantwortlichen und damit der ggf. verlusttragenden Einheit gefällt werden. Das ORM überwacht dabei die Risikoposition des Unternehmens und trägt gemeinsam mit dem ISM dazu bei, die Risiken aus der IT auf ein ökonomisch sinnvolles Niveau zu reduzieren. In der Risikokontrolle ist im ISM stärker auf kennzahlenbasierte und automatisierte Reports abzustellen, die die bisherigen periodischen Audits und Reviews ergänzen. Die gewonnenen Erkenntnisse über Erfolg und Misserfolg der Steuerungsmaßnahmen müssen in Form eines Informations-Push auf klar definierten Berichtswegen an das Risikomanagement geleitet werden.

Organisatorisch ist der gestiegenen Verantwortung des ISM in einer zentralen Unterstützungsfunktion durch Reorganisation Rechnung zu tragen. Sowohl die Methoden- als auch die Kontrollverantwortung für den Bereich IT-Sicherheit ist fest im ISM zu verankern. Auf Ebene der Geschäftsführung ist die gestiegene Bedeutung von Sicherheitsfragen mit der Etablierung der Funktion eines CSO zu dokumentieren. Mit der Einführung von gemeinsamen Gremien und der klaren Definition von Zuständigkeiten sind die Reibungsverluste einer integrierten Betrachtungsweise der IT-Sicherheit zu minimieren.

Die vorliegende Arbeit zeigt, dass Effizienzpotenziale einer integrierten Betrachtungsweise von ORM und ISM vorliegen. Ein umfassendes und durchgängiges Management operationeller Risiken ist allerdings in den Instituten noch lange nicht umgesetzt. Eine organisatorische Integration des ORM mit anderen Managementsystemen (wie dem hier betrachteten ISM) muss langfristig aber als Erfolgsfaktor für die Entwicklung des Unternehmens angesehen werden. Die Einführung eines operationellen Risikomanagements ist nicht als isoliertes Projekt zu sehen, sondern muss vielmehr als Beginn eines Veränderungsprozesses im Unternehmen verstanden werden. Während viele Institute momentan noch mit der Verbesserung der Datenqualität und dem Aufbau von internen und externen Schadensfalldatenbanken beschäftigt sind wird die Entwicklung eines integrativen Managementkonzepts für operationelle Risiken vernachlässigt.[200]

Die Vorteile des auf Basis des Vorgehens im Risikomanagement entwickelten Ansatzes liegen in der Möglichkeit einer kontinuierlichen Verbesserung der Zusammenarbeit zwischen ISM und ORM. Bereits durch grundlegende organisatorische Maßnahmen können erste Erfolge der Zusammenarbeit erreicht werden. Die integrierte Betrachtungsweise auf Prozessebene kann sich zunächst auf ausgewählte Risiken mit entsprechenden Schadenspotenzialen beschränken und in der Folge schrittweise ausgebaut werden. Die Integration liefert auch für das ISM Entwicklungschancen, die Verbesserungen in Organisation und Methodik mit sich bringen können. Die Integration in die gesamte Risikoorganisation stützt das ISM in den Bereichen Management Awareness, Kundenorientierung und der Umsetzung einer unternehmensweiten Sicherheitskonzep-

200 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 497 f.

tion.[201] Von einer in Integration profitieren somit sowohl das ORM als auch das ISM. Die Erfahrungen aus der Integration des ISM in das ORM lassen sich zukünftig auch für die Integration anderer Managementbereiche (Personalmanagement, Controlling) nutzen. Die Integrationsbemühungen von ISM und ORM können somit beispielhaften Charakter für die Entwicklung einer risikoorientierten Steuerung im gesamten Unternehmen haben. Die zu erwartenden Effizienzgewinne der integrierten Betrachtungsweise werden den Erfolg eines Integrationsansatzes belegen.

201 Vgl. Locher, Christian: Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, a. a. O., S. 498.

Literaturverzeichnis

1. **Anduleit, Manfred:** IT-Sicherheit ist Chefsache, in: Computerwoche, 21/2005, S. 41.

2. **Baseler Ausschuss für Bankenaufsicht (Hrsg.):** Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen – überarbeitete Rahmenvereinbarung (Juni 2004), Online im Internet: http://www.bis.org/publ/bcbs107ger.pdf, 25.06.2006.

3. **Baseler Ausschuss für Bankenaufsicht (Hrsg.):** The Basel Committee on Banking Supervision, Online im Internet: http://www.bis.org/bcbs/aboutbcbs.htm, 25.05.2006.

4. **Becker, Peter:** Prozessorientiertes Qualitätsmanagement, 4., vollständig überarbeitete Auflage, Renningen: expert 2005.

5. **Biermann, Bernd:** Modernes Risikomanagement in Banken, in: Eller, Roland; Gruber, Walter; Reif, Markus (Hrsg.): Handbuch des Risikomanagements: Analyse, Quantifizierung und Steuerung von Markt-, Kredit und operationellen Risiken, 2., überarbeitete und erweiterte Auflage, Stuttgart: Schäffer-Poeschel 2002.

6. **BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hrsg.):** Kompass der IT-Sicherheitsstandards – Ein Leitfaden für mittelständische Unternehmen, Stand März 2005, Online im Internet: http://www.bitkom.org/files/documents/BITKOM_BroschUere_Sicherheitsstandard_V1.1f.pdf, 25.06.2006.

7. **Boos, Karl-Heinz, Fischer, Reinfried, Schulte-Mattler, Hermann (Hrsg.):** Kreditwesengesetz – Kommentar zu KWG und Ausführungsvorschriften, 2. Auflage, München: C. H. Beck 2004.

8. **Braun, Ulrich:** § 25a KWG – Besondere organisatorische Pflichten von Instituten, in: Kreditwesengesetz – Kommentar zu KWG und Ausführungsvorschriften, Hrsg.: Boos, Karl-Heinz; Fischer, Reinfried; Schulte-Mattler, Hermann, 2. Auflage, München: C. H. Beck 2004.

9. **Brauner, Detlef; Raible-Besten, Robert; Weigert, Martin M.:** PC-Anwender-Lexikon, München, Wien: Oldenbourg 1999.

10. **Brehmke, Kirsten; Meyer, Ralf:** Strategisches Risikomanagement, in: Frankfurter Allgemeine Zeitung, 13.02.2006, S. 24.

11. **Buchner, Manfred:** Höchste Zeit für Basel II, in: Computerwoche, 21/2005, S. 26-27.

12. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) – Version 1.0, Online im Internet: http://www.bsi.de/literat/bsi_standard/standard_1001.pdf, 25.06.2006.

13. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** IT-Grundschutzhandbuch: Stand 2005, Online im Internet: http://www.bsi.de/gshb/deutsch/download/itgshb_2005.pdf, 25.06.2006.

14. **Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.):** Anschreiben zum Rundschreiben 18/2005: Veröffentlichung der Endfassung der MaRisk, Online im Internet: http://www.bafin.de/schreiben/89_2005/051220.htm, 20.12.2005.

15. **Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.):** Aufgaben und Ziele: Bundesanstalt für Finanzdienstleistungsaufsicht, online im Internet: http://www.bafin.de/cgi-bin/bafin.pl?verz=0201000000&sprache=0&filter=a&ntick=0, 25.06.2006.

16. **Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.):** Entwurf: Verordnung1 über die angemessene Eigenkapitalausstattung (Solvabilität) von Kreditinstituten – Solvabilitätsverordnung, Online im Internet: http://www.bafin.de/verordnungen/solvv/01_entwurf.pdf, 31.03.2006.

17. **Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.):** Rundschreiben 18/2005: Mindestanforderungen an das Risikomanagement, Online im Internet: http://www.bafin.de/rundschreiben/89_2005/051220.htm, 20.12.2005.

18. **Deutsche Bank Gruppe (Hrsg.):** Investor Relations – Konzerninformationen - Organisationsstruktur, Online im Internet: http://www.deutsche-bank.de/ir/494.shtml, 16.03.2006.

19. **Dierstein, Rüdiger:** Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, in: Informatik Spektrum, Band 27, Heft 4, S. 343-353.

20. **Foit, Mihael:** Management operationeller IT-Risiken in Banken, Regensburg: Universitäts-Verlag Regensburg 2005.

21. **Füser, Karsten; Gleißner, Werner; Meier, Günter:** Risikomanagement (KonTraG) – Erfahrungen aus der Praxis, in: Der Betrieb, 15/1999, S. 753-758.

22. **Gehrke, Wolfgang:** Das Pflichtenheft des Risikomanagements – Für eine vollständige Erfassung und Steuerung der Gesamtrisikoposition eines Unternehmens, in: Frankfurter Allgemeine Zeitung, 28.04.2003, S. 26.

23. **Gola, Peter; Schomerus, Rudolf:** Bundesdatenschutzgesetzt – Kommentar, 7. völlig neu bearbeitete Auflage, München: C. H. Beck 2002.

24. **Grill, Wolfgang; Perczynski, Hans (Hrsg.):** Wirtschaftslehre des Kreditwesens, 35., überarbeitete Auflage, Bad Homburg vor der Höhe: Gehlen 2001.

25. **Haller, Matthias:** <Security> und Risiko-Management – ein Widerspruch?, in: Student Business Review, Ausgabe Frühjahr 2005, St. Gallen, S. 6-8.

26. **Heinrich, Robert; Lang, Franz-Josef:** DV und Recht/Risikobewertung und Frühwarnsysteme – Ein neues Gesetz macht die IT-Sicherheit zur Pflicht, in: Computerwoche, 24/1999, S. 71-73.

27. **Hirschmann, Stefan; Romeike, Frank:** IT-Sicherheit als Rating-Faktor, in: RATINGaktuell, 01/2004, S. 12-18.

28. **Hofmann, Marc:** Management operationeller IT-Risiken im Kontext von Basel II, MaRisk und anderen aufsichtsrechtlichen Vorgaben, Hamburg: Dr. Kovac 2006.

29. **Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc:** Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, in: Controlling, 7/1999, S. 317-325.

30. **Huch, Burkhard; Tecklenburg, Thilo:** Risikomanagement in der Bauwirtschaft, in: Risikomanagement, Hrsg.: Götze, Uwe; Henselmann, Klaus; Mikus, Barbara, Heidelberg: Physica 2001.

31. **Institut der Wirtschaftsprüfer (Hrsg.): ** IDW-Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330), WPg 2002, Heft-Nr. 21/2002, S. 1167 ff.

32. **Institut der Wirtschaftsprüfer (Hrsg.): ** IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), WPg 2002, Heft-Nr. 21/2002, S. 1157 ff.

33. **International Standard Organisation (Hrsg.):** ISO/TR 13569 – Financial Services – Information Security Guidelines, Online im Internet (kostenpflichtig): www.iso.org, 25.05.2006.

34. **International Standard Organization (Hrsg.):** State-of-the-art information security management systems with new ISO/IEC 27001:2005 standard, Online im Internet: http://www.iso.org/iso/en/commcentre/pressreleases/archives/2005/Ref976.html, 24.05.2006.

35. **Krystek, Ulrich; Fiege, Stefanie**: Risikomanagement, in: Gabler Wirtschaftslexikon, 16. vollständig aktualisierte und überarbeitete Auflage, Wiesbaden: Gabler 2004.

36. **Kupsch, Peter**: Risikomanagement, in: Handbuch Unternehmensführung. Konzepte – Instrumente – Schnittstellen, Hrsg.: Corsten, Hans; Reiß, Michael, Wiesbaden: Gabler 1995, S. 529-543.

37. **Laudon, Kenneth C.; Laudon, Jane P.; Schoder, Detlef:** Wirtschaftsinformatik – Eine Einführung, München, Boston: Pearson Studium 2006.

38. **Loch, Friedemann; Thelen-Pischke, Hiltrud:** Basel II – Herausforderungen für die Geschäftsleitung der Institute, in: Zeitschrift für das gesamte Kreditwesen, 13/2001, S. 736-739.

39. **Locher, Christian:** Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, in: Innovationen im Retail-Banking: der Weg zum erfolgreichen Privatkundengeschäft, Hrsg.: Bartmann, Dieter, Weinheim: Wiley-VCH, 2005.

40. **Mag, Wolfgang:** Unternehmensplanung, München: Vahlen 1995.

41. **Marcharzina, Klaus; Wolf, Joachim:** Unternehmensführung - Das internationale Managementwissen: Konzepte – Methoden – Praxis, 5., grundlegend überarbeitete Auflage, Wiesbaden: Gabler 2005.

42. **Mauch, Peter:** Risikomanagement in Banken, in: Risikomanagement, Hrsg.: Götze, Uwe, Henselmann, Klaus, Mikus, Barbara, Heidelberg: Physica 2001, S. 327-350.

43. **Maus, Thomas:** Inventarisierung und Bewertung von IT-Risiken, in: Staat & IT - Information Week Special, 11/2004, S. 25-27.

44. **Mehlau, Jens Ingo:** Die Bedeutung des IT-Sicherheitsmanagement für Finanzdienstleister, in: Banking and Information Technologie (BIT), 3/2001, S. 11-18.

45. **Mikus, Barbara:** Risiken und Risikomanagement – ein Überblick, in: Risikomanagement, Hrsg.: Götze, Uwe; Henselmann, Klaus; Mikus, Barbara, Heidelberg: Physica 2001, S. 3-28.

46. **Mohr, Sonja:** Outsourcing nach Bankenart - § 25a KWG als Grundlage für sichere IT-Dienstleistungen, in: <kes> Die Zeitschrift für Informations-Sicherheit, 6/2005, S. 85-87.

47. **Münch, Isabel; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, Bonn: SecuMedia 2002.

48. **Nägli, Hans-Peter:** Management der Informationssicherheit – Erfahrungen eines Finanzdienstleisters, in: HMD – Praxis der Wirtschaftsinformatik, Bd. 232, Hrsg.: Brenner, Walter; Meier, Andreas; Zarnekow, Rüdiger, Heidelberg: dpunkt 2003, S. 79-88.

49. **O. V.:** Brockhaus Enzyklopädie, 19. Auflage, Mannheim: Brockhaus 1993, Bd. 19.

50. **O. V.:** CIOs liefern Tools für die Risikovorsorge, in: Computerwoche, 27/2005, S. 30-31.

51. **O. V.:** Gabler Wirtschaftslexikon, 16., vollständig überarbeitete und aktualisierte Auflage, Wiesbaden: Gabler 2004.

52. **O. V.:** Integriertes Risikomanagement, Online im Internet: http://www.kpmg.de/library/pdf/irm.pdf, 25.06.2006.

53. **O. V.:** US-Listing: Einbahnstraße New York, Online im Internet: http://www.manager-magazin.de/geld/artikel/0,2828,321440,00.html, 04.10.2004.

54. **O. V.:** Wikipedia – Die freie Enzyklopädie: Chief Security Officer (CSO), Online im Internet: http://de.wikipedia.org/wiki/ Chief_Security_Officer, 25.06.2006.

55. **O. V.:** Wikipedia – Die freie Enzyklopädie: Sicherheit, Online im Internet: http://de.wikipedia.org/wiki/Sicherheit, 25.06.2006.

56. **Paulus, Sacher:** Risiken beim Einsatz von Informationstechnologie, in: Praxis des Risikomanagements: Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte, Hrsg.: Dörner, Dietrich; Horváth, Péter; Kagermann, Henning, Stuttgart: Schäffer-Poeschel, 2000, S. 379-413.

57. **Pohlmann, Norbert; Blumberg, Hartmut F.:** Der IT-Sicherheitsleitfaden – Das Pflichtenheft zur Umsetzung von IT-Sicherheitsstandards im Unternehmen, Bonn: mitp 2004.

58. **Prehl, Sabine:** Outsourcing: Für Banken eine harte Nuss, in: Computerwoche, 2/2005, S. 32.

59. **Rauschen, Thomas; Disterer, Georg:** Identifikation und Analyse von Risiken im IT-Bereich, in: HMD: Praxis der Wirtschaftsinformatik, Bd. 236, Hrsg.: Mörike, Michael, Heidelberg: dpunkt 2004, S. 19-32.

60. **Romeicke, Frank:** Lexikon Risikomanagement, Köln: Wiley 2004.

61. **Romeike, Frank:** Banken unterschätzen operationelle Risiken, Online im Internet: http://www.risknet.de/RiskNET_News.29.0.html?&tx_ttnews[backPid]=1&tx_ttnews[tt_news]=328&cHash=ff9b0f2a8a&type=123, 25.06.2006.

62. **Romeike, Frank:** Die ältesten Risiken der Welt, in: RiskNews, 01/2004, S. 16-17.

63. **Romeike, Frank:** IT-Security-Ping-Pong – IT-Risk-Management muss ganzheitlich betrachtet werden, in: Risknews, 3/2004, S. 16f.

64. **Romeike, Frank:** Risiko-Management als Grundlage einer wertorientierten Unternehmenssteuerung, in: RATINGaktuell, 02/2002, S. 12-17.

65. **Roßbach, Peter; Locarek-Junge, Hermann (Hrsg.):** IT-Sicherheits-management in Banken, Frankfurt/Main: Bankakademie Verlag 2002.

66. **Schaumüller-Bichl, Ingrid:** Sicherheitsmanagement – Risikobewältigung in informationstechnologischen Systemen, Mannheim; Leipzig; Wien; Zürich: BI-Wissenschaftsverlag 1992.

67. **Staehle, Wolfgang H.; Conrad, Peter; Sydow, Jörg:** Management – Eine verhaltenswissenschaftliche Perspektive, 8. Auflage, München: Vahlen 1999.

68. **Stahlknecht, Peter; Hasenkamp, Ulrich:** Einführung in die Wirtschaftsinformatik, 10. Auflage, Berlin et al.: Springer 2001.

69. **Stickel, Eberhard; Groffmann, Hans-Dieter; Rau, Karl-Heinz (Hrsg.):** Gabler Wirtschaftsinformatiklexikon, Wiesbaden: Gabler 1997.

70. **Tappert, Rainer:** EDV-System-Prüfung – Bankbetriebliche Revisionsinformatik, Köln: Bank-Verlag 1994.

71. **Völker, Jörg:** BS 7799 – Von „Best Practice“ zum Standard – Secorvo White Paper – Informationssicherheits-Management nach BS 7799 im Überblick, Online im Internet: http://www.secorvo.de/whitepapers/secorvoo-wp10.pdf, 25.06.2006.

72. **Voßbein, Jörn:** Organisation eines IT-Sicherheitsmanagement, in: IT-Sicherheitsmanagement in Banken, Hrsg.: Roßbach, Peter; Locareck-Junge, Hermann, Frankfurt/Main: Bankakademie-Verlag, 2002, S. 9-21.

73. **Witt, Bernhard C.:** Rechtliche Anforderungen an die Informations-Sicherheit, in: <kes> Die Zeitschrift für Informations-Sicherheit, 1/2006, S. 92ff.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: Online-Bestellung unter http://wi.uni-giessen.de → Forschung

Herausgeber: Univ.-Prof. Dr. Axel C. Schwickert
Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungsarbeiten, Diplom-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr- und Vortragsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Univ. Prof. Dr. Axel C. Schwickert, Justus-Liebig-Universität Gießen.

Hinweise: Wir nehmen Ihre Anregungen und Kritik zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit dem Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe und deren Bezug erhalten Sie auf der Web Site der Professur unter der Adresse http://wi.uni-giessen.de