Edition <kes>

Hans-Peter Königs

IT-Risikomanagement mit System

Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken

5. Auflage

<kes>

Springer Vieweg

Edition <kes>

Mit der allgegenwärtigen IT ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Die <kes> – Zeitschrift für Informations-Sicherheit – wird von der DATAKONTEXT GmbH im zweimonatigen Rhythmus veröffentlicht und behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz. Nähere Informationen rund um die Fachzeitschrift finden Sie unter www.kes.info.

Die Autoren der Zeitschrift und der Buchreihe Edition <kes> helfen den Anwendern in Basic- und Expert-Seminaren bei einer praxisnahen Umsetzung der Informations-Sicherheit: www.itsecuritycircles.de.

Weitere Bände in dieser Reihe
http://www.springer.com/series/12374

Hans-Peter Königs

IT-Risikomanagement mit System

Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken

5., überarbeitete und erweiterte Auflage

Springer Vieweg

Hans-Peter Königs
Olsberg, Schweiz

Edition <kes>
ISBN 978-3-658-12003-0 ISBN 978-3-658-12004-7 (eBook)
DOI 10.1007/978-3-658-12004-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Strasse 46, 65189 Wiesbaden, Germany

Geleitwort

Fast täglich vernehmen wir, wie Organisationen oder auch Einzelpersonen aus dem „Cyber Space“ angegriffen werden. Die Schäden sind zum Teil sehr hoch und haben in einzelnen Fällen das Potenzial, ein Unternehmen zu ruinieren. Wie einige im vorliegenden Buch zitierten Untersuchungen zeigen, ist das Schadensvolumen durch solche Cyber-Attacken hoch und im Steigen begriffen. Zu den aus bösartigen Absichten resultierenden Schadensereignissen gesellen sich auch unabsichtlich verursachte Schäden wie sie sich aufgrund von Unfällen, Bränden oder Stromausfällen, bei der immer höheren Abhängigkeit unserer Gesellschaft von Systemen der Informationstechnik, ergeben. So wird auch das „Internet of Things“, das zur Steuerung und Überwachung vieler Gegenstände des täglichen Lebens zunehmend Verwendung finden wird, zu Risiken führen, denen mit adäquaten Methoden begegnet werden muss.

Die vorliegende überarbeitete und erweiterte 5. Auflage des Buches trägt solchen Cyber-Risiken in einem zusätzlichen Kapitel sowie in der Überarbeitung der anderen Kapitel in hervorragender Weise Rechnung. Die im Buch durchwegs vertretene ganzheitliche Durchführung des Risikomanagements, unter Einbezug der Informationssicherheits-, IT- und Cyber-Risiken des Unternehmens ist ein Ansatz, den wir bei unseren Beratungen im öffentlichen Sektor und bei privaten Unternehmen zur Verbesserung der „Resilienz“ gern einsetzen.

An diesem Buch schätzen wir zudem die Anlehnung an wichtige nationale und internationale Normen in ihren derzeit aktuellen Versionen; zu erwähnen sind hier die ISO-Standards zum allgemeinen Risikomanagement, die vielzähligen Standards über einzelne Gebiete der Informationssicherheit und über Management-Systeme, z. B. des Informationssicherheits-Managementsystems und des Cloud-Computings (innerhalb der ISO/IEC 270xx-Reihe) sowie des Business Continuity Management. Erfreulich ist auch die Anlehnung an Standards wie denen des US-amerikanischen „National Institute of Standards and Technology“ oder der ISACA mit COBIT 5, in denen diese Institute auch zu Risikothemen Vorreiterrollen einnehmen.

Der Autor hat es dabei sehr gut verstanden, die für das Thema relevanten Quellen in das Buch einzubeziehen und die zum Teil umfangreichen und komplexen Zusammenhänge in den wesentlichen Aspekten verständlich zu behandeln und mit entsprechenden

Abbildungen zu visualisieren. Aufgrund der Mitarbeit des Autors in diversen Standardisierungsgremien der Schweizerischen Normenvereinigung, seiner Tätigkeit als Dozierender für verschiedene Fächer des Risikomanagements an der Hochschule Luzern sowie seiner Beratertätigkeit trifft er sicherlich für eine am Thema interessierte Leserschaft auch in dieser Buchauflage wiederum das richtige Mass an Theorie und Praxis.

Für diese in vielen Aspekten wie der Cyber-Risiken überarbeitete und erweiterte Buchauflage wünschen wir wiederum einen grossen Erfolg.

Zürich im Oktober 2016 Dr. Thomas Siegenthaler, Präsident CSI Consulting AG

Vorwort zur 5. Auflage

Die Risiko-Landschaft für viele Unternehmen hat sich in den letzten Jahren stark verändert, denken wir nur an die Verlagerung vieler Geschäftstätigkeiten und Informationsverarbeitungen in das Internet und die damit einhergehenden stark angewachsenen Cyber-Risiken. Auch haben die jüngst kontrovers diskutierten Ereignisse um Informationen (z. B. NSA-Belauschungen oder Hacker-Angriffe auf den deutschen Bundestag), die Informationen als hohes schützenswertes Gut vermehrt in das öffentliche Bewusstsein gerückt.

Ein Anstieg der Risiken hat sich auch aufgrund der steigenden Vernetzung und der fortschreitenden Digitalisierung von allerlei Systemen und Geräten des täglichen Lebens sowie der vielen unvermeidbaren Bedrohungen wie Hochwasser, Stürme oder Unfälle ergeben. Daher haben sich sowohl in der Standardisierung als auch in der praktischen Umsetzung des Risikomanagements von Informationssicherheits-, IT- und Cyber-Risiken in den letzten Jahren neue und vertiefte Erkenntnisse, Erfahrungen und Anpassungen ergeben; diesen Faktoren trägt die neue Buchauflage in praxisorientierter Weise Rechnung. Dabei werden in ein Gesamt-Risikomanagement integrierte Lösungsansätze vertreten, die ausgehend von der Unternehmens-Governance die fachspezifischen Risiken der Informationen, der IT mit ihren Systemen und Produkten sowie der Cyber-Systeme in systematischer Weise behandeln.

Ein solches Risikomanagement in den einzelnen Fachdisziplinen durchzuführen und in die Prozesse der Unternehmensführung zu integrieren wird nicht zuletzt durch die Unternehmensleitungen aufgrund ihrer ultimativen Verantwortung für solche Risiken gefördert wie auch durch verschiedene Gesetze und Regulative implizit verlangt. Diese Tendenz spiegelt sich auch in den jüngsten Standards der ISO wider, in denen für Managementsysteme (darunter ISO/IEC 27001) weitgehend einheitliche Anforderungs-Strukturen, z. B. bezüglich Unternehmens-Kontext, Einbindung der Führungspersonen, Ressourcenbereitstellung, Dokumentation und Kontrolle, gefordert werden. Solche wichtigen Anforderungen an die Führungsprozesse, die bei der Integration des Managements von Informationssicherheits-, IT- und Cyber-Risiken eine wichtige Rolle spielen, werden im Teil II dieses Buches behandelt.

Die derzeit laufenden Standardisierungen, an denen ich in den relevanten Normen-Komitees der Schweizerischen Normenvereinigung aktiv mitarbeite, tragen solchen aktuellen Aspekten Rechnung. Trotz der starken Anlehnung an solche Standards, ist es nicht Zweck des Buches, diese Standards zu interpretieren, zu erläutern oder die möglichen Neuerungen aus den zurzeit laufenden Reviews der Standards (z. B. ISO 31000, ISO-Guide 73, ISO/IEC 27003 oder ISO/IEC 27005) vorwegzunehmen. Vielmehr sollen für den Leser die wesentlichen praktischen Aspekte eines Risikomanagements aus der Sicht des Unternehmens und aus allgemeingültigen Grundlagen herausgearbeitet werden. Somit versteht sich das Buch als Alternative und Ergänzung zu den heute vielfältig vorhandenen und in den Literaturhinweisen erwähnten Rahmenwerken und Standardisierungs-Dokumenten.

Wie im erweiterten Titel des Buches erkennbar ist, beschränkt sich das Buch weder alleine auf die Risiken der Informationssicherheit[1] noch ausschliesslich auf die Risiken der IT, sondern behandelt im Rahmen eines Unternehmens-Risikomanagements die Risiko-Felder der Informationssicherheit, der Unternehmens-IT und der Cyber-Risiken als operationelle Unternehmens-Risiken. Deshalb sind die Buchteile I, II und IV aus der Top-down-Perspektive eines Unternehmens-Risikomanagements verfasst. Somit verfolgt das Buch das Ziel, den derzeitigen Stand des Risikomanagements von Informationssicherheits-, IT- und Cyber-Risiken, eingebettet in die Unternehmensperspektive, in einer für die praktische Anwendung notwendigen Übersicht und Ausführlichkeit zu behandeln.

Um der Sicht eines Unternehmens-Risikomanagements dienen zu können, wurde das Buch wiederum in die vier folgenden Teile gegliedert:

Teil I: Grundlagen erarbeiten
Teil II: Anforderungen aus Unternehmenssicht berücksichtigen
Teil III: Informations-Risiken erkennen und behandeln
Teil IV: Unternehmensprozesse meistern

Damit erklärt sich, dass in den ersten beiden Buchteilen die Grundlagen und die Anforderungen in einer für das Unternehmen allgemeinen Weise behandelt werden. Hingegen werden die für die IT- und Informations-Risiken spezifischen Inhalte im dritten Teil des Buches und die Umsetzung und die Integration des Informationssicherheits- und IT-Risikomanagements in die Unternehmensprozesse im vierten und letzten Teil des Buches behandelt.

Am Ende eines jeden Kapitels finden sich einige Kontrollfragen und Aufgaben. Die Musterlösungen für die Kontrollfragen und Aufgaben können über einen Online-Service im Internet abgerufen werden. Die URL dafür ist:

http://www.koenigs-media.ch/IT-Risikomanagement/

Fragen, fachliche Hinweise oder gar einen über den Online-Service möglichen Dialog sind mir herzlich willkommen.

[1] Sicherheit der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen.

Dank

Einen wesentlichen Impuls zur Aktualisierung des vorliegenden Buches erhalte ich jeweils durch meine Tätigkeit als externer Dozierender an der Hochschule Luzern in meinen Vorlesungen über Informationssicherheit und Risikomanagement. Für die Unterstützung beim Einsatz dieses Buches in verschiedenen Ausbildungsveranstaltungen über „Information Security“ im Department „Informatik“ der Hochschule Luzern danke ich der Hochschule. Besonders danke ich dem Kurs- und Studienleiter Prof. Armand Portmann für sein Interesse, für die gemeinsamen Diskussionen sowie für die Abstimmungen über die dem Buch entnommenen Vorlesungsinhalte.

Für ihr stetes Interesse und Bereitschaft, einzelne Themen und ihre Praxistauglichkeit mit mir zu diskutieren danke ich meinen Kollegen: PD Dr. Karsten Decker, CEO Decker Consulting GmbH; Marcus Griesser, Dozentenkollege und CISO bei der SBB; Dr. Thomas Siegenthaler, Präsident CSI Consulting AG; und Janos Vrbata, CEO Vrbata Consulting.

Mein Dank gilt auch dem Lektorat des Springer Vieweg Verlags und vorab Frau Dr. Sabine Kathke für die sehr gute Betreuung und die wertvollen Hinweise.

Mein besonderer Dank geht vor allem an meine Frau Dr. Diemuth Königs, Historikerin und Autorin historischer Bücher, die mir mit Rat und Tat in allen Belangen zur Seite steht.

Olsberg im Oktober 2016 Hans-Peter Königs

Abkürzungsverzeichnis

AktG	Aktiengesetz
ASL®	Application Services Library (ASL® ist eine eingetragene Marke der ASL BiSL Foundation.
BiSL®	Business Information Services Library (BiSL® ist eine eingetragene Marke der ASL BiSL Foundation)
BS	British Standard
BSC	Balanced Scorecard
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
BSI	British Standards Institution (UK)
CC	Common Criteria
CEO	Chief Executive Officer
CERT®	Computer Emergency Response Team (Carnegie Melon University)
CERT®/CC	Computer Emergency Response Team/Coordination Center (Carnegie Melon University)
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CISO	Chief Information Security Officer
CLO	Chief Legal Officer
COBIT®	Control Objectives for Information and related Technology (COBIT® ist eine eingetragene Marke der Information Systems Audit and Control Association)
COO	Chief Operation Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRAMM	Centre for Information Systems Risk Analysis und Management Method
CRO	Chief Risk Officer
CSF	Critical Success Factor
CSO	Chief Security Officer
EBK	Eidgenössische Bankenkommission (Schweiz)
ETA	Event Tree Analysis (Ereignisbaum-Analyse)

FINMA	Eidg. Finanzmarktaufsicht
FMEA	Failure Modes and Effects Analysis (Fehler-Effekt- und Ausfall-Analyse)
FMECA	Failure Modes, Effects and Criticality Analysis
FTA	Failure Tree Analysis (Fehlerbaum-Analyse)
GL	Geschäftsleitung
HGB	Handelsgesetzbuch (Deutschland)
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISACA®	Information Systems Audit and Control Association®
ISMS	Informationssicherheits-Management-System
ISO	International Standards Organisation
IT	Informations-Technologie (Information Technology)
ITGI	IT Governance Institute®
ITIL®	IT Infrastructure Library (ITIL® ist eine eingetragene Marke der AXELOS, einem Joint Venture zwischen CAPITA und Cabinet Office UK)
ITSEC	Information Technology Security Evaluation Criteria
KCI	Key Control Indicator
KGI	Key Goal Indicator
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MAO	Maximum Acceptable Outage
MTPD	Maximum Tolerable Period of Disruption
Mil Std	Military Standards (USA)
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failures
MTTR	Mean Time To Repair
NIST	National Institute of Standards and Technology
OR	Schweizerisches Obligationenrecht
PDCA	Plan Do Check Act
PCCIP	President's Commission on Critical Infrastructure Protection
RM	Risikomanagement
ROSI	Return on Security Investments
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SOX	Sarbanes-Oxley Act (USA)
SWOT	Strength, Weaknesses, Opportunities, and Threats
SSL	Secure Socket Layer
VR	Verwaltungsrat

Inhaltsverzeichnis

Einführung

1

Überblick

„Wer nicht an die Zukunft denkt, wird bald Sorgen haben." Dieses Zitat von Konfuzius[1] bewahrheitet sich in unseren tagtäglichen Erfahrungen. Von solchen zukünftigen Sorgen soll uns das in diesem Buch behandelte Risikomanagement möglichst entlasten. Es stellt sich also die Frage: „Warum beschäftigen sich Unternehmen mit Risiken?" Die Antwort auf diese Frage und wie mit Risiken im Allgemeinen und mit den Risiken der Informationssicherheit, der IT und dem Cyberspace im Besonderen umgegangen werden soll, wird in diesem einführenden Buchkapitel grob behandelt. Dabei werden die vier Teile, in die das Buch gegliedert ist, kurz vorgestellt. Jedoch spätestens nach dem Lesen des ganzen Buches sollte der Leser mit den Vorgehensweisen zum Management solcher Risiken aus der Sicht einer Organisation[2] vertraut sein.

1.1 Warum beschäftigen sich Unternehmen mit Risiken?

Risiken sind eine Selbstverständlichkeit des Alltags. Der ehemalige deutsche Bundespräsident Walter Scheel[3] definierte dies treffend so: „Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts". Die Frage dabei ist nur, wie den unerwünschten Risiken begegnet werden kann. Die Erfahrungen zeigen doch, dass mit geeigneten Vorkehrungen und Massnahmen das Eintreten der unerwünschten Ereignisse weitgehend verhindert oder

[1] Konfuzius: Chinesischer Philosoph (551 v.Chr. - 479 v.Chr.)

[2] In diesem Buch werden die Begriffe „Unternehmen" und „Organisation" synonym angewandt, obwohl die Standardisierungsliteratur unter dem Begriff Organisation auch nicht gewinnsuchende soziale Strukturen (z. B. Stiftungen, Kirchen oder andere Gemeinschaften) einbezieht.

[3] Deutscher Bundespräsident von 1974 bis 1979.

H.-P. Königs, *IT-Risikomanagement mit System*, Edition <kes>,
DOI 10.1007/978-3-658-12004-7_1

die negativen Konsequenzen bei einem Eintritt zumindest vermindert werden können. Wem es je passiert ist, dass kurz vor der Fertigstellung einer umfangreichen Schreibarbeit am PC die Informationen unwiederbringlich gelöscht waren, wird die Nützlichkeit einer regelmässigen Informationssicherung auf ein anderes Speicher-Medium kaum in Frage stellen. Werden hingegen nur ein paar wenige aus dem Gedächtnis leicht zu reproduzierende Zeilen geschrieben, dann wird sich der Aufwand für ein zusätzliches Abspeichern auf ein zweites Speicher-Medium wohl kaum lohnen. Dieses simple Beispiel zeigt, wie ein den Risiken angemessenes Handeln gerade beim Umgang mit Informationen gewinnbringend sein kann. Dabei ist es auch eine allgemein bekannte Weisheit, dass negative Ereignisse (z. B. Unfälle), auch mit noch so weiser Voraussicht, nie gänzlich vermieden werden können; meist können jedoch mit entsprechenden Vorkehrungen entweder die Häufigkeit des Eintritts reduziert oder die negativen Konsequenzen unerwünschter Ereignisse gemildert werden. So hat das am 11. März 2011 stattgefundene Erdbeben in Japan und die nachfolgende Tsunami- und Atomreaktor-Katastrophe in eklatanter Weise gezeigt, wie den Verhältnissen angemessene vorsorgliche Massnahmen den Tsunami zwar nicht verhindern, aber dessen Schadens-Auswirkungen – vor allem die nachfolgende Reaktorkatastrophe – hätten wesentlich reduzieren können. So kam auch der am 5. Juli 2012 veröffentlichte Bericht einer eingesetzten parlamentarischen Untersuchungskommission zum Schluss, dass die „von Menschen verursachte Katastrophe“ der Kernschmelze „vermeidbar“ gewesen wäre. Betroffen von den Auswirkungen oder involviert in die Handlungen vor und nach Schadensereignis waren eine Vielzahl von Personen und Firmen wie beispielsweise der Kraftwerkbetreiber TEPCO und die japanischen Behörden.

Wie IT-Risiken Firmenpleiten verursachen können, kann am Beispiel des Unterwäsche-Herstellers Schiesser AG ersehen werden. Über die 2009 insolvent gewordene Firma am Standort Radolfzell mit 2300 Mitarbeiter war beispielsweise im Internet zu lesen: „Die Lieferschwierigkeiten der Schiesser AG waren in der Branche bekannt. Dafür verantwortlich: die Betriebssoftware. Sie stellt die Lieferbarkeit sicher. Bei Schiesser tat sie das eben nicht (…).“

Auch zeigt die inzwischen fast endlose Liste von Cyber-Attacken, wie Unternehmen und deren Anspruchsgruppen (Kunden, Lieferanten etc.) durch solche Angriffe zu Schaden kommen können, weil es offensichtlich an den angemessenen Sicherheitsmassnahmen fehlt. So wurde „Target Corporation“, eines der grössten Einzelhandels-Unternehmen in den USA, im Jahr 2013 Opfer eines Hackerangriffs. Die Datendiebe erbeuteten 70 Millionen Datensätze mit persönlichen Informationen der Kundschaft, darunter von 40 Millionen Kredit- und Debit-Kartenbesitzer die Datensätze mit Kontodaten, einschliesslich der Sicherheitsdaten wie Kreditkartennummer, Gültigkeitsdatum, CVV-Sicherheitscode und PIN-Code. Für außergerichtliche Einigungen mit betroffenen Kunden musste Target rund zehn Millionen Dollar investieren. Der damalige CEO Gregg Steinhafel musste ein halbes Jahr nach dem Datendiebstahl die Firma verlassen. Angeblich könnte Target bis zu einem Betrag von 3.6 Milliarden Dollar haftbar sein. Das Vertrauen der Kunden in die Sicherheitsmassnahmen von Target wurde durch das Ereignis beschädigt, was sich u. a. auch in einem Umsatzrückgang zeigte [Pere14].

Ähnliches, aber in umgekehrter Richtung, gilt für positive Ereignisse, die mit möglichst positiven Effekten herbeigewünscht werden. Solche ebenfalls ungewissen, jedoch wünschbaren positiven Ereignisse werden als Chancen bezeichnet. Um die positiven Effekte mit grösstmöglicher Wahrscheinlichkeit oder mit möglichst günstigen Ergebnissen herbeizuführen, werden auch entsprechende Massnahmen ergriffen. So soll beispielsweise die Werbung für ein Produkt die Chancen vergrössern, dass ein Produkt möglichst häufig gekauft und dabei allenfalls auch noch ein hoher Kaufpreis erzielt wird. Unterbleiben die Massnahmen, dann wird das Produkt allenfalls nicht mehr gekauft und der gewünschte Erfolg wird zu einem Misserfolg, was umgangssprachlich wiederum als „Risiko“[4] bezeichnet wird. So ist es ein zentraler Aspekt beim Umgang mit Risiken, unter Berücksichtigung der vorhandenen Bedingungen und der in Zukunft möglichen Entwicklungen, die optimalen Massnahmen zum Erreichen wünschenswerter Ergebnisse herauszufinden und zu realisieren. Diese eben skizzierte Beschäftigung mit Risiken ist grob vereinfacht das, was die Unternehmen allgemein unter „Risikomanagement“ verstehen.

Systematik beim „Risikomanagement“
Um mit allen und zum Teil abstrakten Aspekten zu den gewünschten optimalen Ergebnissen zu kommen, braucht es in der Regel ein grosses Mass an Systematik. Gerade, wenn es um hohe Risiken und hohe Massnahmenkosten geht, die den Unternehmen rund um die Risiken der Informationssicherheit, der IT und der Cyber-Sicherheit entstehen, ist es wichtig, die Risiken ganzheitlich, systematisch und transparent zu behandeln.

„Risikomanagement“ mit systemischen Modellen
Die für das Risikomanagement in diesem Buch verwendeten Modelle werden als „systemische“ Modelle verstanden. Dabei kann eine Risiko-Ursache zu verschiedenen Auswirkungen führen und eine Auswirkung das Resultat verschiedener Ursachen sowie Ursache neuer Auswirkungen sein. Um die meist „komplexe“ Wirklichkeit möglichst gut zu modellieren, enthalten die Problemlösungs-Prozesse des Risikomanagements mit ihren Sub-Prozessen entsprechende Rückkopplungen und Iterationen ([Ulri91], S. 36–50, 114–136). Mit diesem „systemischen“ Ansatz findet auch der gewählte Titel dieses Buches „IT-Risikomanagement mit System“ seine Erklärung.

1.2 Risiken und Chancen bei unternehmerischen Tätigkeiten

Risiken und Chancen sind in jedem Unternehmen – wenn auch nicht immer offensichtlich – vorhanden. Es gilt der Grundsatz, dass mit dem Ergreifen von Chancen auch immer Risiken einhergehen. Dabei ist es eine normale menschliche Eigenschaft, die Risiken aus

[4] Der im Abschn. 2.2 erwähnte „Erweiterte Risikobegriff“ enthält sowohl die negativen als auch die positiven Ungewissheiten, dabei wird als Antonym zu „Chance“ (Opportunity) nicht der Begriff „Risiko“, sondern der Begriff „Gefahr“ respektive „Bedrohung“ (Threat) verwendet (vgl. [Cott13], S. 2; [Glei05], S. 27).

dem Bewusstsein möglichst zu verdrängen. Dennoch ist der sorgfältige Umgang mit Risiken, gleichermassen wie das Wahrnehmen von Chancen, eine der wichtigsten unternehmerischen Verantwortlichkeiten und muss in der Unternehmens-Politik, in der Unternehmens-Strategie sowie in allen unternehmerischen Handlungen gepflegt werden; ist doch das Wohl des Unternehmens und gar sein Überleben vom richtigen Umgang mit den Risiken abhängig.

Die Leidtragenden der Risiken sind auch nicht nur die Eigentümer eines Unternehmens, sondern alle am Unternehmen beteiligten sogenannten Anspruchsgruppen (Stakeholder), wie Beschäftigte, Kapitalgeber, Verbände, Partner, Lieferanten, Behörden, Kommunen und der Staat. So haben die in den letzten Jahren aufgetretenen Schadensereignisse bewirkt, dass das Risikomanagement in den meisten Industriestaaten zu einer von Gesetzgebern und Regulatoren verordneten „Muss-Disziplin" der Unternehmensführung geworden ist.

1.3 Inhalt und Aufbau dieses Buchs

Die unterschiedlichen Risiken in einem Unternehmen sind in ihrer Art und Entstehung stark voneinander abhängig und tragen letztlich zum Erfolg oder Misserfolg eines Unternehmens in entscheidendem Masse bei. Deshalb muss die Steuerung und Überwachung der Risiken bereits auf der obersten Ebene der Unternehmensführung erfolgen. Das Buch behandelt zwar speziell die Informationssicherheits-, IT- und Cyber-Risiken, dennoch müssen die Bedrohungen, Massnahmen und Prozesse zum Management dieser Risiken in einem ganzheitlichen Zusammenhang aus Unternehmenssicht und dessen Zielen, Anforderungen und Management-Prozessen gesehen werden. Demzufolge wird vor der spezifischen Behandlung der auf Informationen bezogenen Risiken in den Teilen III und IV des Buches, in den Teilen I und II die dazu notwendigen Grundlagen und Voraussetzungen behandelt.

Teil I: Grundlagen erarbeiten

Gemäss diesem Buchaufbau werden in **Teil I** des Buches die für ein ganzheitliches Risikomanagement in einem Unternehmen notwendigen allgemeinen Grundlagen und Instrumente erarbeitet. Dabei werden die in der Praxis oft vereinfacht und pragmatisch verwendeten Risikobegriffe und Vorgehensweisen in ihrer Grundsätzlichkeit erläutert. Da das Buch die Informations- und IT- und Cyber-Risiken wo möglich aus Unternehmenssicht und aus der Sicht des Unternehmensmanagements behandelt, werden in diesem Teil des Buches viele Grundlagen allgemein und nicht „nur" spezifisch für die Informations-Risiken[5] aufgezeigt. Im Kap. 3 erfolgt sodann die Verknüpfung der im Kap. 2 bereits dargestellten Methoden und Werkzeuge in einem, an den Standard ISO 31000:2009

[5] Die drei Risiko-Arten „Informationssicherheits-Risiken", „IT-Risiken" und „Cyber-Risiken" überlappen sich stark (s. Abb. 17.1). Daher wird, wenn mehrere dieser Risiken gemeint sind, vereinfacht

angelehnten allgemeinen Risikomanagement-Prozess, der ein möglichst effizientes und effektives Risikomanagement ermöglichen soll. Die fachspezifischen Details für das Informations-Risikomanagement können leicht aus diesem allgemeinen Prozess abgeleitet werden.

Teil II: Anforderungen aus Unternehmenssicht berücksichtigen
Im Sinne eines von den Anforderungen her getriebenen Unternehmens-Risikomanagements, werden im **Teil II** die an das Unternehmen gestellten aktuellen Anforderungen an ein Risikomanagement sowohl aus „Compliance-Sicht" als auch aus Sicht der Governance und der verschiedenen Management-Prozesse behandelt. Die dazu zusammengestellten Konzepte, Methoden und Instrumente haben zum Ziel, im Sinne eines „Integrierten Risikomanagements", ein möglichst effektives Risikomanagement, unter Einbezug der wichtigen Risiken und Anforderungen bezogen auf die IT und die Informations-Risiken aufzubauen und zu betreiben.

Teil III: Informations-Risiken erkennen und bewältigen
Der Teil III widmet sich ausschliesslich dem Risikomanagement der Informationssicherheit und der Informationstechnologie (IT). Resultierend aus den im Teil II beschriebenen Unternehmensanforderungen werden mit entsprechenden Methoden und Verfahren die Risiken der Informationssicherheit und der IT detailliert behandelt. Der gebräuchliche, aber unscharfe Begriff der „Informations-Risiken" schliesst dabei die Informationssicherheits-Risiken wie auch die Risiken im Zusammenhang mit der Leistungserbringung der IT ein.

Teil IV: Unternehmensprozesse meistern
Im Teil IV wird sodann gezeigt, wie sich die verschiedenen Risiken, darunter die operationellen Risiken der Informationssicherheit und der Informations-Technologie, in einen gesamten Risikomanagement-Prozess des Unternehmens einfügen lassen. Dazu gehört vor allem die Integration der fachspezifischen Risikomanagement-Prozesse der Informationssicherheit, der IT und der Cyber-Sicherheit in den gesamten Risikomanagement-Prozess und in den Strategieprozess des Unternehmens. Behandelt werden auch unternehmenswichtige Management-Systeme und -Prozesse wie die des Geschäftskontinuitäts-Managements (BCM) und deren Verankerung im Gesamt-Risikomanagement-Prozess des Unternehmens. Letztlich werden in diesem Buchteil auch einige für die Unternehmen wichtige Risiko-Themen, wie Lifecycle von Informationen und Systemen, IT-Sourcing, Cloud-Computing sowie die immer wichtiger werdenden Vorgehensweisen bezüglich der „Cyber-Bedrohungen" behandelt.

---

von „Informations-Risiken" gesprochen, da alle drei Risiko-Arten ja ihren Ursprung bei „Informationen" haben.

Literatur

[Cott13] Cottin, Claudia und Sebastian Döhler: Risikoanalyse. Wiesbaden, Springer Spektrum, 2013.

[Glei05] Gleissner, Werner und Frank Romeike: Risikomanagement. München: Haufe, 2005.

[Pere14] Perez, Sarah: Target's Data Breach Gets Worse: 70 Million Customers Had Info Stolen, Including Names, Emails And Phones. Tech Crunch: Jan 10, 2014. URL: https://techcrunch.com/2014/01/10/targets-data-breach-gets-worse-70-million-customers-had-info-stolen-including-names-emails-and-phones/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29&utm_content=Netvibes, abgerufen 11.9.2016.

[Ulri91] Ulrich, Hans und Gilbert J. B. Probst: Anleitung zum ganzheitlichen Denken und Handeln. 3. erw. Auflage, Bern: Haupt, 1991.

Teil I

Grundlagen erarbeiten

Beschäftigung mit Risiken und Risikomanagement

2

Überblick

Ein grosser und in den Grundlagen des Risikomanagements anspruchsvoller Teil liegt in der methodischen Erkennung, Analyse, Verwaltung und der Kommunikation der Risiken. Auf der Basis einer qualitativen oder quantitativen Einstufung der Risiken sowie einiger weiterer Kriterien sollen möglichst optimale Massnahmen-Lösungen gefunden und umgesetzt werden; in einer prozessorientierten, nachvollziehbaren Abwicklung des Risikomanagements ist es auch wichtig, inwiefern die nach der Risiko-Behandlung verbleibenden Restrisiken in einem Risiko-Portfolio toleriert und ohne weitere Behandlung bewusst getragen werden können. In diesem Kapitel werden, ausgehend von Eigenschaften und den möglichen Darstellungsweisen eines Risikos, einige grundlegenden Vorgehensweisen und Instrumente für das Risikomanagement in einem Unternehmen behandelt.

2.1 Vernetzte Aktivitäten und Stellenwert Risikomanagement

Die hauptsächlichen Aktivitäten eines Risikomanagements werden vorteilhaft in einer prozessorientierten Weise durchgeführt (s. Abb. 2.1). Die Abb. 2.1 zeigt auch, dass die Aktivitäten eines Risikomanagement-Prozesses in hohem Masse untereinander vernetzt sind, d. h. dass alle Subprozesse voneinander abhängig sind und zur Verbesserung der Ergebnisse aufeinander einwirken sollen. Demzufolge werden auch alle Aktivitäten im Rahmen des Risikomanagements mittels Kommunikationsaktivitäten untereinander verbunden. Eine detaillierte Behandlung des Risikomanagement-Prozesses mit seinen Subprozessen erfolgt im Kap. 3 dieses Buches.

H.-P. Königs, *IT-Risikomanagement mit System*, Edition <kes>,
DOI 10.1007/978-3-658-12004-7_2

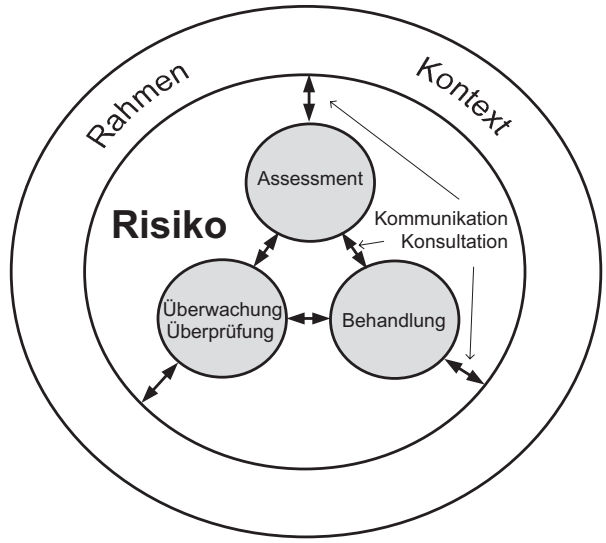

Abb. 2.1 Vernetzte Aktivitäten im Risikomanagement (vgl. [Niir11], S. 8)

Bedeutung des Risikomanagements für die Unternehmensführung
Das „Risikomanagement", wie es in diesem Buch sowohl generell aus der Unternehmenssicht als auch spezifisch für die Gebiete der Informationssicherheit, der Informationstechnologie und der Cyber-Sicherheit behandelt wird, ist eine bedeutende Disziplin der Unternehmensführung; soll doch der Einsatz der Disziplin „Risikomanagement" den Führungspersonen erlauben, die negativen Entwicklungen und Ereignisse abzuwenden und die Geschicke des Unternehmens in positive Bahnen zu lenken.

Interdisziplinäre Vernetzungen beim Risikomanagement
Das Risikomanagement und seine Durchführung hat auch einen hohen interdisziplinären Stellenwert, können doch beispielsweise die „Informationssicherheits-Risiken" oder „Cyber-Risiken" grosse andere Risiken in der Volkswirtschaft, in öffentlichen Verwaltungen, im Gesundheitswesen, im Kommunikations-, Energie-, Verkehrs-, Finanz- und Transportwesen sowie ganz allgemein in der Gesellschaft nach sich ziehen. Zu den kriminellen Ursachen kommen die Risiken aufgrund menschlichen Versagens, höherer Gewalt und des Versagens von Technik oder Prozessen, die zu Schäden an Leib und Leben, zu hohen Abschreibungen oder zum Ruin ganzer Unternehmen führen können. Einige solcher Risiken sind: Flops oder Mängel bei grossen IT-Projekten, Ausfälle wichtiger IT-Systeme (z. B. in Banken oder öffentlichen Verwaltungen), Datendiebstähle (Namen, Passwörter und Kreditkartennummern), undurchschaubare Funktionen mit Manipulation und Datenabfluss bei der Benutzung sozialer Netzwerke. Immer stärkere Bedeutung erlangen auch die Cyber-Attacken, bei denen Kriminelle, mittels „Social Engineering" und „Trojanern", die Computer von Privatpersonen, Unternehmen und Behörden zu Betrugszwecken ausspionieren und Daten manipulieren. Solche Angriffe dienen beispielsweise der Erpressung von Personen bis hin zur Staats- und Wirtschaftsspionage und dem heute zur Realität gewordenen „Cyber-Krieg".