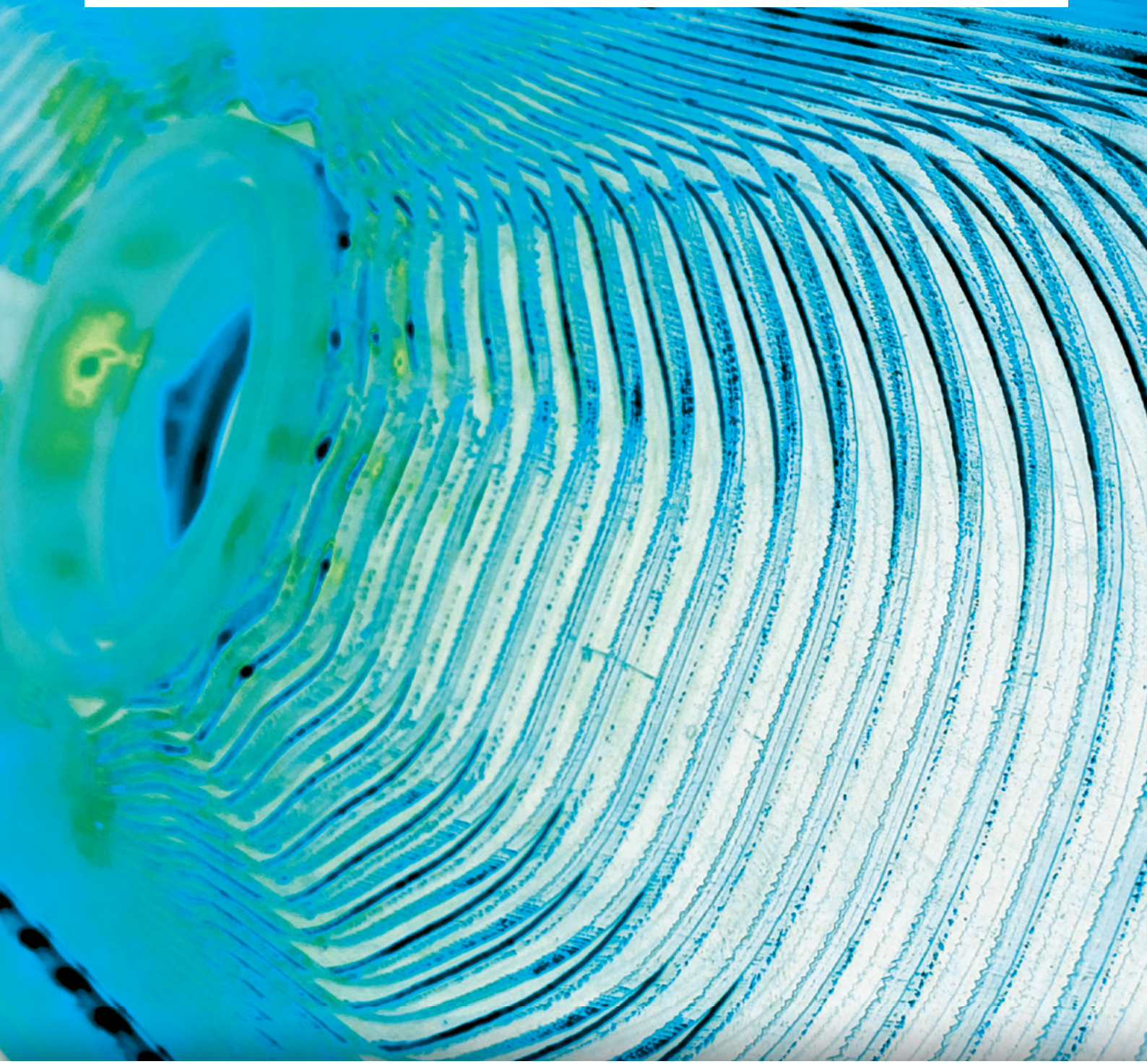
Eine Veröffentlichung des ISACA Germany Chapter e.V.
und Risk Management Association e.V.



Leitfaden ISO 31000 in der IT

mit Vergleich zu anderen Standards

ISACA
Trust in, and value from, information systems
Germany Chapter

RMA
RiskManagement
Association e.V.

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e.V.
Im Birkenfeld 1a
65779 Kelkheim
E-Mail: webmaster@isaca.de
www.isaca.de
und
Risk Management Association e.V.
Englmannstraße 2
81673 München
E-Mail: office@rma-ev.org
www.rma-ev.org

Autorenteam:
- Dipl.-Wirt.-Ing. Ines Heese, M.A.,CIA, Burda GmbH
- Christian Funk, CISA, IT-Gov.-/IT-Compl.-Manager, SCHUFA Holdig AG
- Dipl.-Wirtsch.-Inf. Knut Haufe, LL.M., CISA, CISM, CRISC, CGEIT, ISO27001-Auditteamleiter (BSI und ISO), BSI IS-Revisor, CISSP, PMP, EuroPriSe Technical and Legal Expert, PERSICON
- Dipl.-Kfm. Michael Neuy, CISA, CIA, CISM, CRISC, CP ONR49003, ISMS Auditor (IRCA), Beitragsservice von ARD, ZDF und Deutschlandradio
- Dipl.-Inf. Michael Schmid, MBA, ISMS-Auditor (ISO 27000), cand. CISM, Burda GmbH
- Dipl.-Inform. (FH) Holger Schrader, CISM, CRISC, CARMAO GmbH
- Dipl.-Ing. Dipl.-Kfm. Dirk Skicki, CISA, CRISC, E-Plus Mobilfunk GmbH & Co. KG
- Dipl.-Betriebsw. Dipl.-Wirtschaftspäd. Werner Syndikus, CISA, CGEIT, CRISC, tobaccoland Automaten GmbH & Co. KG
- Matthias Becker, CISM, Bundesamt für Sicherheit in der Informationstechnik
- Ingrid Dubois, dubois it-consulting gmbh
- Gerhard Funk, CISA, CISM, unabhängiger Berater
- Oliver Knörle, CISA, Consultant Informationssicherheit
- Dipl.-Math. Andrea Rupprich, CISA, CISM, usd AG
- Dr. Tim Sattler, CISA, CISM, CRISC, CISSP, Jungheinrich AG
- Dipl.-Kfm. Stefan Wittjen, CISA, CIA, CISM, CRISC, RBS Roever-BroennerSusat
- Dipl.-Wirt.-Inf. Karsten Wilop, CISA, CGEIT, CRISC, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft
- Andreas Teuscher MBA, CGEIT, CISA, CRISC, ISO 27001 LA, Sick AG

Der finale Entwurf des Prüfleitfadens wurde rezensiert (Review) durch:
- Dipl.-Kfm. Bernd Burfeind, CIA, CISA, CRMA, DMK Deutsches Milchkontor GmbH
- Dipl.-Oec. Nina Lissen, Senior Controller, E-Plus Gruppe

Die Worte zum Geleit schrieben freundlicherweise:
- Dipl.-Kfm. Ralf Kimpel, CIA, CRMA, Burda GmbH
- Andreas Teuscher, MBA, CGEIT, CISA, CRISC, ISO 27001 LA, Sick AG

Die Inhalte dieses Leitfadens wurden von Mitgliedern verschiedener Fachgruppen des ISACA Germany Chapter e.V. und der Risk Management Association e.V. erarbeitet und sind sorgfältig recherchiert. Trotz größtmöglicher Sorgfalt erhebt die vorliegende Publikation keinen Anspruch auf Vollständigkeit. Sie spiegelt die Auffassung des ISACA Germany Chapter und der Risk Management Association e.V. wider. ISACA Germany Chapter e.V. und die Risk Management Association e.V. übernehmen keine Haftung für den Inhalt.

Stand: Juni 2014, Version 16 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe IT-Risikomanagement)

Leitfaden ISO 31000 in der IT

mit Vergleich zu anderen Standards

ISACA®
Trust in, and value from, information systems
Germany Chapter

RMA
RiskManagement
Association e.V.

Inhaltsverzeichnis

Zum Geleit

Risikomanagement spielt angesichts der stetig steigenden Bedrohungen und der zunehmenden Komplexität der Vernetzung auch im Hinblick auf die Informationstechnologie eine immer wichtigere Rolle. In guter ISACA-Fachgruppen-Tradition wurde deshalb durch die Fachgruppe IT-Risikomanagement ein Leitfaden erstellt, der auf Basis der ISO 31000 mögliche Ansatzpunkte aufzeigen soll.

Dieser Leitfaden vermittelt eine Grundlage zum Einstieg in das Risikomanagement, in die Spezialdisziplin des IT-Risikomanagements sowie zu den Beurteilungsmethoden. Ergänzt wird dieses Dokument mit Vergleichen zu gängigen Standards aus der ISO-, COBIT- und BSI-Grundschutz-Welt.

Der Vorstand des ISACA Germany Chapter bedankt sich ausdrücklich für die vielen Stunden der ehrenamtlichen Arbeit der Mitwirkenden und freut sich sehr, dass wir mit der Risk Management Association einen professionellen Partner für das für uns so wichtige Thema gewinnen konnten. Wir hoffen, dass der Leitfaden auf eine interessierte Leserschaft trifft und zahlreich in der Praxis Anwendung finden wird.

Andreas Teuscher

Vizepräsident Facharbeit und Arbeitskreise des ISACA Germany Chapter e.V.

Standards dienen der Standardisierung, ISO-Standards der globalen Standardisierung. Sie helfen, Sprachregelungen zu finden, einen Orientierungsrahmen zu bilden, Komplexität zu reduzieren, Transparenz zu erhöhen und letztlich Vertrauen bei den Stakeholdern herzustellen. Die Wirkung von Standards liegt aber auch in der Reduktion von Kosten und der Realisierung von Skaleneffekten oder ganz allgemein darin, die Unternehmensziele zu erreichen.

Die Risk Management Association (RMA) hat sich zum Ziel gesetzt, den Standardisierungsprozess im Risikomanagement aktiv zu unterstützen und praktische Hilfestellungen dabei zu leisten, Risikomanagementstandards in die Praxis umsetzen. Auch bei der Entwicklung der ISO 31000 waren die RMA und ihre Mitglieder aktiv. Wo immer Praktiker Unterstützung bei der Umsetzung der ISO 31000 suchen, hilft die RMA und ihre Mitglieder, natürlich auch im wichtigen Bereich der IT und des IT Risk Management.

Der Vorstand der RMA freut sich sehr über die erstmalige und sehr konstruktive Zusammenarbeit mit der ISACA bei der Abfassung dieses Leitfadens für die Umsetzung der ISO 31000 in die IT-Praxis. Möge der Leitfaden vielen Risikomanagern und IT-Risikomanagern eine Hilfestellung bei den nicht zu unterschätzenden Herausforderungen in der Etablierung oder Optimierung von Risikomanagementsystemen im IT-Umfeld bieten.

Ralf Kimpel

für die Risk Management Association

Vorwort

Die ISO 31000 hat seit ihrer Herausgabe im November 2009 einen beispielhaften Erfolgsweg zurückgelegt. Man kann mit Fug und Recht behaupten, dass neben dem Rahmenwerk COSO ERM, das mit einer etwas anders gelagerten, vorwiegend aus dem Finanzsektor stammenden Intention vorangetrieben wurde, die ISO-31000-Normenfamilie der weltweit führende Standard für Risikomanagement ist. In seiner Genese wurde er von nationalen Standards beeinflusst, die ihrerseits bereits hohes Ansehen genossen, wie z.B. von dem australisch/neuseeländischen Standard AS/NZS 4360 oder der österreichischen Standardfamilie ONR 49000-2004 ff.

Es lag daher nach der Überzeugung der Autoren nahe, die Anwendbarkeit der ISO 31000 in einem der wichtigsten und in den letzten Jahren rasant entwickelten Bereiche des Risikomanagements, dem IT-Risikomanagement, darzustellen.

Dabei soll die Zusammenarbeit zwischen dem ISACA Germany Chapter als führendem Verband der IT-Auditoren, IT-Sicherheitsfachleute und IT-Governance-Fachkräfte einerseits und der Risk Management Association (RMA) als das Netzwerk der Risikomanager im deutschsprachigen Raum andererseits hierbei die notwendige fachliche Kompetenz gewährleisten, um diesen Leitfaden auf einem angemessenen Qualitätsniveau zu erstellen.

Die Autoren möchten ausdrücklich darauf hinweisen, dass dieser Leitfaden kein Ersatz und keine Übersetzung der ISO 31000 ist. Wir empfehlen ausdrücklich, diesen und andere erwähnte Standards in der Originalausgabe zu erwerben. Dies ist folgendermaßen möglich:

- In Deutschland beim Beuth Verlag, *http://www.beuth.de/*
- In Österreich bei Austrian Standards, *http://www.as-plus.at/*
- International bei der International Organization for Standardization (ISO), *http://www.iso.org/*

ISACA
Trust in, and value from, information systems
German Chapter

ISACA Germany Chapter e.V.

Das ISACA Germany Chapter e.V. ist der deutsche Zweig des weltweit führenden Berufsverbandes der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Beauftragten. Der Verein wurde 1986 gegründet und ist mit über 2.300 Mitgliedern Teil des internationalen Verbandes ISACA, dem weltweit mehr als 100.000 Know-how-Träger in über 180 Ländern der Welt angehören.

Zweck des Vereins ist es, durch Diskussion und Informationsaustausch zwischen den Mitgliedern und Interessenten das Verständnis der Probleme auf dem Gebiet der IT-Revision, IT-Sicherheit sowie der IT-Governance zu fördern und diese Erfahrungen durch Publikationen und Seminare allen Mitgliedern und Interessenten zur Kenntnis zu bringen sowie die Kontakte zwischen den Mitgliedern und Interessenten durch gesellschaftliche Veranstaltungen zu unterstützen und zu ergänzen.

ISACA fördert die Anerkennung des Berufsstandes durch die Verbreitung von Berufsstandards und Arbeitstechniken sowie durch die ständige Weiterbildung und die Zertifizierung zum Certified Information Systems Auditor (CISA), zum Certified Information Security Manager (CISM), zum IT-Governance-Experten (Certified in the Governance of Enterprise IT (CGEIT)) und zum Experten im IT-Risikomanagement und Enterprise Risk Management (Certified in Risk and Information System Control (CRISC)).

Daneben werden nationale, auf COBIT aufbauende Zertifikatsprogramme zum Cyber Security Practitioner, IT Governance & Compliance Practitioner, IT Governance Manager und IT Compliance Manager angeboten.

RMA
RiskManagement
Association e.V.

Risk Management Association e.V.

Die Risk Management Association e.V. (RMA) ist mit über 400 Mitgliedern die führende unabhängige Interessenvertretung für das Thema Risikomanagement im deutschsprachigen Raum. Als Kompetenzpartner und Impulsgeber ist die RMA erster Ansprechpartner für Informationen, den unternehmensübergreifenden Dialog sowie die Weiterentwicklung des Risikomanagements. Zu den Mitgliedern der RMA zählen u.a. internationale Konzerne, mittelständische Unternehmen sowie Privatpersonen aus Wirtschaft, Wissenschaft und dem öffentlichen Sektor.

Mithilfe eigener Fachgremien befasst sich die RMA mit den wichtigsten Risikomanagementthemen wie beispielsweise Standards im Risikomanagement, Risikomanagement & Controlling, Compliance, IT-Risiken und Enterprise Risk Management (ERM).

Die RMA bildet ein professionelles Netzwerk aus Experten und Vordenkern aus dem Risikomanagementumfeld. Damit fördert die RMA ein nachhaltiges Vorgehen und bringt sich maßgeblich in die Diskussion und Ergebnisfindung im Risikomanagement ein. Strategische Kooperationen mit weiteren Verbänden und Interessengruppen, darunter dem Internationalen Controller Verein, stärken diese Ziele.

Gemeinsam mit dem Forschungszentrum für Risikomanagement an der Hochschule Würzburg führt die RMA seit 2012 außerdem ein Weiterbildungsprogramm zur Erlangung des Zertifikats zum Enterprise Risk Manager Univ. durch und unterstützt damit die Qualifizierung der Risikomanager im deutschsprachigen Raum.

1 Grundsatz

1.1 Zielgruppe

Dieser Leitfaden ist als Hilfestellung für Fachkräfte aus dem Umfeld von Prüfung und Beratung gedacht, z.B. für folgende Berufsgruppen:

- **Interne IT-Revisoren**
  Die Interne Revision ist nach den Standards des Institute of Internal Auditors (IIA) verpflichtet, das Risikomanagement (RM) des Unternehmens zu prüfen und zu bewerten. Die IT-Revision macht hier keine Ausnahme, sodass als Gegenstand der Untersuchung das IT-Risikomanagement mit einer gewissen Berechtigung angenommen werden darf. Neben dem seit mehr als 10 Jahren bestehenden DIIR-Revisionsstandard Nr. 2 »Prüfung des Risikomanagements« ist seit dem Jahr 2010 auch ein Leitfaden des IIA als Prüfungshilfe verfügbar, der sich an die ISO 31000 anlehnt. Insofern kann der vorliegende Leitfaden als Ergänzung zum Verständnis der ISO 31000 speziell im IT-Umfeld dienen.
- **IT-Prüfer im Rahmen der Abschlussprüfung**
  Das Institut der Wirtschaftsprüfer (IDW) hat schon vor Jahren mit dem PS 340 zur Prüfung des Risikomanagements eine klare Position eingenommen. Es ist dabei zu beachten, dass der PS 340 eine Selbstbeschränkung enthält, die sich aus der Rolle des Abschlussprüfers ergibt. Es ist darin erklärt, dass es durchaus auch noch weitere Risiken für ein Unternehmen geben kann, die ein Wirtschaftsprüfer bei seiner regulären Prüfungstätigkeit nicht im Prüfungsumfang berücksichtigt. Der IT-Prüfer, der gemäß PS 330 und RS FAIT1 die abschlussrelevanten Bereiche der IT im Rahmen der Abschlussprüfung untersucht, muss nun zu den Vorgaben des PS 340 eine Brücke schlagen, um das IT-Risikomanagement zu beurteilen. Hinzu kommt, dass der PS 340, wie der Name sagt, ein Prüfungsstandard und kein Gestaltungsstandard ist. Insofern kann dieser Leitfaden dem IT-Abschlussprüfer als Erweiterung des traditionellen Ansatzes dienen, indem er eine auf die IT bezogene, allgemeingültige Interpretation der ISO 31000 ff. liefert und damit den IT-Prüfer bei der Beurteilung von IT-Risiken unterstützen kann.
- **IT-Sicherheitsfachkräfte**
  Risiken in der IT werden heute zum großen Teil mit dem Begriff »Sicherheit« in Verbindung gebracht. Viele IT-Sicherheitsfachkräfte verfügen über eine hochwertige Ausbildung, die es ihnen ermöglicht, Abwehrszenarien gegen Malware, Hacking, Identitätsdiebstahl, Datenausschleusung etc. zu entwerfen und auch in der Praxis mit Hard- und Software umzusetzen. Diese technischen Fähigkeiten können durch ein risikotheoretisches Rüstzeug sinnvoll erweitert werden. Hier kann dieser Leitfaden der Berufsgruppe der IT-Sicherheitsfachkräfte hilfreich zur Seite stehen.
- **IT-Compliance-Manager**
  Seit Inkrafttreten des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist das Risikomanagement als Einhaltung von gesetzlichen Vorschriften, also als Compliance-Thema, anzusehen. Dabei sind zwei Sichtweisen möglich: Zum einen wacht der IT-Compliance-Manager darüber, dass das gesetzlich vorgeschriebene Risikomanagement auch im IT-Bereich seinen angemessenen Platz hat. Zum anderen sind diverse Compliance-Risiken, wie Nichteinhaltung des Datenschutzes, Verstoß gegen Urheberrechte oder Nichtbeachtung des Telemediengesetzes, zu berücksichtigen. Im weiteren Sinne der Compliance ist auch der Verstoß gegen unternehmensinterne Vorschriften ein Risiko. Hierfür bedarf es eines systematischen und zielorientierten Ansatzes. Insofern kann dieser Leitfaden eine Hilfe im Bereich der IT-Compliance sein.
- **IT-Governance-Spezialisten**
  »Leitung und Überwachung« bzw. »Unternehmensführung« sind die Attribute, die mit dem Begriff Governance verbunden werden.[1] Überträgt man diese Begrifflichkeit auf die IT, so enthält sie eine Vielzahl von Aspekten, von denen die Funktion der Überwachung der IT direkt zum IT-Risikomanagement führt. So kann vorausgesetzt werden, dass ein IT-Governance-Spezialist immer auch das RM betrachten muss, da es heute mit zu den klassischen Führungsaufgaben gehört. Für diesen Spezialisten, der – sei es als externer oder als interner Berater – seinem CIO/IT-Leiter zur Seite steht, soll dieser Leitfaden eine Hilfe bei den vielen Möglichkeiten der Ausgestaltung eines Risikomanagementansatzes in der jeweiligen IT-Abteilung oder dem jeweiligen IT-Bereich sein.

1. Siehe Deutscher Corporate Governance Kodex (in der Fassung vom 13. Mai 2013), Präambel.

- **IT-Risikomanager**
  IT-Risikomanager sind – insbesondere in mittelständischen Unternehmen – auch heute noch kaum vorzufinden, zumindest nicht als ausdrücklich benannte Stelle. Dessen ungeachtet kann diese Aufgabe eine ausdrücklich gewünschte Funktion im internen Überwachungssystem eines Unternehmens sein.

1.2 Ziel des Leitfadens

Seit einigen Jahren ist das Risikomanagement in der IT zunehmend in der Diskussion. In diesen Diskussionen zeigt sich einerseits die Notwendigkeit einer Standardisierung aus dem Wunsch nach Vereinheitlichung der Begriffe und Definitionen. Andererseits geht es in der fachlichen Öffentlichkeit um den Best-Practice-Gedanken, also um ein von Experten formuliertes und in der Praxis erfolgreich erprobtes Konzept, das als Vorbild für die Einrichtung eines IT-Risikomanagements im eigenen Unternehmen dienen kann.

Bei der Einrichtung eines IT-Risikomanagements sind grundsätzlich zwei Optionen vorstellbar:

- Die Adaption eines speziellen Standards zum IT-Risikomangement, wie z.B. ISO 27005 oder standardisierter Methoden wie Octave
- Die Anwendung eines allgemeinen, auf alle Unternehmensbereiche bezogenen »ERM«-Standards im Bereich der IT

Bei Auswahl der ersten Alternative ergibt sich der Vorteil, dass der herangezogene Standard im Grundsatz auf die Belange der IT ausgerichtet ist. Möglicherweise fällt dadurch die Einführung leichter. Aber selbst dann ist darauf zu achten, ob nicht eine spezielle Sichtweise in den Vordergrund gestellt wird, wie z.B. bei der ISO 27005 (siehe hierzu Kap. 5).

Nachteile kann die Auswahl dieser ersten Alternative aber bringen, wenn man davon ausgeht, dass nicht nur die IT, sondern auch alle anderen Teile des Unternehmens, also das Unternehmen als Ganzes, einen Risikomanagementansatz braucht, der die unterschiedlichen Risikosituationen (Finanzen, Produktion, Rechtsangelegenheiten usw.) in einem einheitlich kommunizierbaren Rahmen darstellt.

Dies würde bedeuten, dass man den gewählten Best-Practice-Standard für die IT auf das ganze Unternehmen beziehen, quasi expandieren müsste. Ob er dann noch den Anspruch einer Best Practice erfüllen kann oder ob wesentliche individuelle Änderungen notwendig sind, die den Begriff »Standard« eventuell überstrapazieren, mag dahin gestellt sein. In jedem Fall müssen mit einem gewissen Aufwand Brücken gebaut und Überleitungen festgelegt werden.

Die andere Alternative vermeidet genau dieses Problem. Ein Risikomanagementstandard, der von vornherein auf alle Bereiche und Funktionen eines Unternehmens abgestellt ist – dies ist die Intention der ISO 31000 –, kann von einem zentralen Risikomanagement unternehmensweit eingeführt werden. Damit wäre auch die IT von vornherein in den funktionsübergreifenden Ansatz integriert. Unter dieser Voraussetzung ist es dann jedoch erforderlich, die speziellen Belange der unterschiedlichen Unternehmensbereiche nach den grundsätzlichen Vorgaben des Basisstandards auszurichten.

Ebenso muss das Risikomanagementsystem – unabhängig davon, ob es gemäß erster oder zweiter Vorgehensoption eingeführt wird – in die bereits bestehenden weiteren Managementsysteme des Unternehmens oder der Organisation integriert werden, wie z.B. in das interne Kontrollsystem, das Controlling, das Qualitätsmanagement.

Dieser Leitfaden wurde erstellt, um genau dort eine Hilfestellung zu bieten, wo sie aus genannten Gründen zu fehlen scheint: Er beleuchtet die Vorgaben der ISO 31000 ff. aus einem IT-bezogenen Blickwinkel stärker als bisher dokumentiert und gibt insbesondere Hinweise zur praktischen Umsetzung im Bereich der IT, die ggf. auch mit praktischen Beispielen unterlegt sind. Dazu werden die einzelnen Teile der ISO 31000 in der Originalreihenfolge angesprochen und ihr Gehalt in den Kontext der IT gestellt. Im Weiteren werden auch die zugeordneten Teile der Standardfamilie, ISO 31010 und ISO 31004, kurz unter IT-Gesichtspunkten kommentiert. Abschließend folgt noch ein Vergleich mit anderen, bekannten Standards zum IT-Risikomanagement, um dem Leser Anknüpfungspunkte für Gemeinsamkeiten und Unterschiede aufzuzeigen.

2 Die Teile der ISO 31000

2.1 Grundsätze (Principles)

2.1.1 Abstract

In diesem Abschnitt werden anhand eines kurzen Fallbeispiels die Grundsätze der Norm ISO 31000:2009 bzw. der österreichischen Umsetzung ONR 49000:2010 erläutert. Mittels kurzer Analysen zum Fallbeispiel sollen die branchenunabhängig formulierten Grundsätze in einen Bezug zur IT gebracht und insoweit in ihrer Allgemeingültigkeit IT-bezogen konkretisiert werden. Im Fallbeispiel wird ein IT-Projekt behandelt, wobei die Grundsätze ebenso für die Linienorganisation gelten.

2.1.2 Fallbeispiel: ERP-Einführung

Hintergrundinformation

Im Mittelpunkt steht ein IT-Projektleiter (im Folgenden auch »PL«) mit der Erfahrung in der Einführung von Enterprise-Resource-Planning-(ERP-)Systemen bei Herstellern von Kosmetik, Getränken und Unterhaltungselektronik. Diese Produkte werden von den Herstellern zunächst an bestimmte Großhändler ausgeliefert, die die Verteilung an die Einzelhändler vornehmen. Die Hersteller haben selbst keine Geschäftsverbindung zu den Endkunden/Einzelhändlern. Die vom PL verantworteten Projekte zeichneten sich in Hinsicht auf ihre Risiken dadurch aus, dass erst ein bis zwei Tage nach der Einführung der neuen ERP-Lösung (»Go-Live«) alle Schnittstellen funktionierten. Aus diesem Grunde wurden nicht alle Paletten bzw. Sendungen an die Großhändler vollständig geliefert. Dies war zwar nicht optimal, jedoch konnte der PL ohne weitere Analyse plausibel darstellen, dass dieses Vorgehen wirtschaftlich sei. Schließlich seien die Lagerflächen bei den Herstellern sowie die Lagerbestände bei den Großhändlern ausreichend dimensioniert.

Nach mehreren erfolgreichen ERP-Einführungen bei Lieferanten (Hersteller) eines Großhändlers wurde der PL auch von dem Großhandelsunternehmen selbst beauftragt, ein ERP-System einzuführen. Die Vorgabe war: »Mach es so gut wie bei unserem Lieferanten X«. Der PL plante und berichtete so, wie er es gewohnt war. Der Großhändler erteilte auch keine besonderen Aufträge oder besonderen Hinweise zu seiner Geschäftstätigkeit, sondern erwartete, dass der PL alles Notwendige beachten würde.

Zum Go-Live waren wieder nicht alle Schnittstellen fertig und der PL priorisierte wie üblich die »Scanner-Schnittstelle« nicht so hoch wie andere Schnittstellen. Somit würden diese »planmäßig« definitiv erst am zweiten Tag nach dem Go-Live zur Verfügung stehen.

Situation am Tag des Go-Live

- Einzelhändler (Kunden des Großhändlers) wollten die bestellten Waren abholen bzw. sollten sie geliefert bekommen, darunter nicht wie gewohnt nur Consumer Electronics, sondern auch verderbliche Lebensmittel.
- Die Scanner funktionierten nicht, daher konnten Waren nicht automatisiert herausgegeben und verbucht werden.
- Es lagen auch keine Formulare vor, die eine manuelle Herausgabe ermöglicht hätten.
- Die Bestell- bzw. Lagernummern aus den abzulösenden IT-Anwendungen konnten nicht ohne Weiteres aus dem neuen Material-/Verkaufsmodul herausgesucht werden. Die Bestellungen der Einzelhändler konnten deshalb nicht schnell recherchiert werden.

Ergebnis

Der Projektauftrag »ERP-Einführung« war zwar der gleiche, aber der PL kannte den Unterschied des Geschäfts eines Großhändlers zu dem eines Herstellers nicht ausreichend. Anders als bei den Herstellern begründete der Planungsmangel einen nicht unerheblichen Reputationsschaden beim Großhändler.

2.1.3 Gegenüberstellung der Grundsätze zum Fallbeispiel

Im nachfolgenden Abschnitt werden die in den zugrunde liegenden Normen dokumentierten Grundsätze bezüglich des Verlaufs sowie der Projektergebnisse gegenübergestellt und kurz erläutert, ob sich hieran etwas geändert hätte. Hierbei wird jeweils kurz auf die folgende Fragestellung eingegangen: Wie hätte die Berücksichtigung der Grundsätze der ISO 31000 das Ergebnis beeinflussen können?

Risk management is part of decision making

»Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.« [ISO 31000:2009, 3. c) Risk management is part of decision making]
»Risikomanagement unterstützt Risikoeigner dabei, fundierte Entscheidungen zu treffen. Risikomanagement kann dazu beitragen, Aktivitäten zu priorisieren und zwischen verschiedenen Handlungsalternativen zu unterscheiden. Letztlich kann das Risikomanagement zu Entscheidungen beitragen, ob ein Risiko akzeptierbar ist und ob die Risikobewältigung angemessen und wirksam ist.« [ONR 49000:2010, 5.2.3 Risikomanagement ist Teil der Entscheidungsfindung]

Die Frage »Was könnte schiefgehen?« ist eine wesentliche Operationalisierung dieses Grundsatzes. Hätten sich der PL oder der Großhändler im Rahmen der üblichen Planung bewusst mit den fallbezogenen Risiken auseinandergesetzt, dann wären die Besonderheiten des Auftrags rechtzeitig vor dem Go-Live festgestellt worden.

Im vorliegenden Beispiel hat der PL lediglich aufgrund seiner Erfahrung eine vergangenheitsorientierte Entscheidung getroffen. Die fallspezifischen Umstände und das Umfeld wurden nicht »risikoorientiert« analysiert. Die konkreten Prozesse und situationsspezifischen Risiken wurden nicht angemessen auf Wirksamkeit beurteilt. Insoweit wurde auch keine fundierte Entscheidung getroffen. Die Berücksichtigung des obigen Grundsatzes hätte das Ergebnis positiv beeinflussen können.

Risk management explicitly addresses uncertainty

»Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.« [ISO 31000:2009, 3. d) Risk management explicitly addresses uncertainty]
»Risikomanagement befasst sich mit denjenigen Aspekten der Entscheidung, die unsicher sind, mit den Merkmalen dieser Unsicherheit und wie mit ihr umgegangen werden kann.« [ONR 49000:2010, 5.2.4 Risikomanagement befasst sich ausdrücklich mit der Unsicherheit]

Bei diesem Grundsatz geht es um die Abgrenzung zum reaktiven »daily business«. Risikomanagement beschäftigt sich proaktiv mit der Möglichkeit von Fehlentwicklungen von Vorhaben. Im vorliegenden Fall hat der PL diesen Grundsatz nicht berücksichtigt, da er bereits davon ausging, dass bestimmte Funktionen zum Go-Live nicht fertiggestellt sein würden. Die Folgen für diesen konkreten Auftrag wären dann aufgrund einer geeigneten Entscheidungsgrundlage – es war ja eine Unsicherheit erkannt worden – zu akzeptieren gewesen.

Risk management is systematic, structured and timely

»A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.« [ISO 31000:2009, 3. e) Risk management is systematic, structured and timely]
»Ein systematischer, zeitgerechter und strukturierter Risikomanagement-Ansatz trägt zur Leistungsfähigkeit und zu beständigen, vergleichbaren und verlässlichen Ergebnissen bei.« [ONR 49000:2010, 5.2.5 Risikomanagement ist systematisch, strukturiert und zeitgerecht]

Analog zu bekannten normierten Projektmanagementsystemen wie PMBOK®[2], PRINCE2®[3] etc. wird auch in der ISO-31000-Normenfamilie zugrunde gelegt, dass durch die Systematisierung von vorher definierten Methoden eine Verlässlichkeit von Ergebnissen ermöglicht wird. Im Fallbeispiel hätte bei einer zeitgerechten Analyse der Schaden für den Großhändler vermieden oder zumindest verringert werden können.

Risk management is based on the best available information

»The Inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgment. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modeling used or the possibility of divergence among experts. Risk management is tailored. Risk management is aligned with the organization's external and internal context and risk profile.« [ISO 31000:2009, 3. f) Risk management is based on the best available information]
»Die Eingaben in den Risikomanagement-Prozess beruhen auf Informationsquellen wie Erfahrungen, Rückmeldungen, Beobachtungen, Prognosen und Expertenmeinungen. Die Entscheidungsträger sollten über die Grenzen von eingesetzten Datenreihen oder Modellen informiert sein und diese berücksichtigen. Sie müssen auch Meinungsverschiedenheiten unter Experten in Betracht ziehen.« [ONR 49001:2010, 5.2.6 Risikomanagement stützt sich auf die besten verfügbaren Informationen]

Im vorliegenden Fall hat sich der PL lediglich auf seine Erfahrungen als einzige Entscheidungsgrundlage verlassen. Es wurden keine weiteren Rückmeldungen vom Großhändler eingeholt. Außerdem hat der PL die Geschäftstätigkeit seines Auftraggebers nicht ausreichend berücksichtigt, sodass es zu der Fehleinschätzung kam. Die Berücksichtigung dieses Grundsatzes hätte einen positiven Einfluss haben können.

2. Project Management Institute (PMI)
3. AXELOS Ltd.

Risk management is tailored

»Risk management is aligned with the organization's external and internal context and risk profile.« [ISO 31000:2009, 3. g) Risk management is tailored.]
»Risikomanagement ist auf den externen und internen Zusammenhang der Organisation zugeschnitten sowie auf das Risikoprofil ausgerichtet.« [ONR 49001:2010, 5.2.7 Risikomanagement ist maßgeschneidert]

Aus dem Beispiel ergeben sich keine Hinweise, warum der PL keine Zeit für ein angemessenes Risikomanagement berücksichtigt hat. Gerade im konkreten Fallbeispiel hätte ein angemessenes, relativ knappes (auf die Bedürfnisse »zugeschnittenes«) Risikomanagement in einem günstigen Kosten-Nutzen-Verhältnis zum erlittenen Schaden gestanden. Oftmals wird in der Praxis die fehlende Zeit in der Projektplanung ins Feld geführt, um zu begründen, dass nicht einmal ein auf das Projektziel zugeschnittenes, minimales Risikomanagement eingerichtet wird. Die bewusste Beantwortung nach dem »Was könnte schiefgehen?« könnte sich aber lohnen, da zumindest die wichtigsten Risiken bedacht werden würden.

Durch diesen Grundsatz wird noch einmal klargestellt, dass der Umfang der Berücksichtigung von Risiken an das Vorhaben angepasst werden darf und muss. Selbst ein nicht formales Risikomanagement hätte im Fallbeispiel einen positiven Beitrag leisten können.

Risk management takes human and cultural factors into account

»Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.« [ISO 31000:2009, 3. h) Risk management takes human and cultural factors into account]
»Das Risikomanagement berücksichtigt die Fähigkeiten, Wahrnehmungen und Absichten externer und interner Menschen, die die Zielerreichung der Organisation fördern oder behindern können.« [ONR 49001:2010, 5.2.8 Risikomanagement berücksichtigt Human- und Kulturfaktoren]

Dieser Grundsatz ist zum einen auf die Berücksichtigung und das aktive Umgehen mit kulturellen Unterschieden gerichtet, die meist bei länderübergreifenden Risikomanagementmodellen in die Risikomanagementkonzepte eingebracht werden müssen. Im vorliegenden Fall kann man aber auch den Aspekt der Humanfaktoren im weitesten Sinne angesprochen sehen, wenn man z.B. die Reaktion auf Imageverluste des Unternehmens durch einzelne handelnde Personen innerhalb (Mitarbeiter) oder außerhalb (Lieferanten und Kunden) als Teil der fehlenden Sensibilität für Risiken auffasst.

Risk management is transparent and inclusive

»Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.« [ISO 31000:2009, 3. i) Risk management is transparent and inclusive]
»Die zweckmäßige und zeitgerechte Einbindung der Stakeholder und insbesondere der Entscheidungsträger auf allen Ebenen der Organisation stellt sicher, dass Risikomanagement wichtig und aktuell bleibt. Die Einbindung der Stakeholder macht es auch möglich, dass sie sich angemessen vertreten fühlen und ihre Ansichten bei der Festlegung der Risikokriterien berücksichtigt werden.« [ONR 49001:2010, 5.2.9 Risikomanagement ist transparent und umfassend]

Die Analyse von Risiken sollte sowohl innerhalb des Projektes als auch mit dem Lenkungsausschuss kommuniziert werden. Aus dem Fallbeispiel konnte die Berücksichtigung dieses Grundsatzes nicht festgestellt werden. Diese Transparenz wurde auch nicht vom Großhändler eingefordert. Eine Abstimmung im Team oder mit Verantwortlichen des Großhändlers hätte einen positiven Einfluss auf den Ausgang des Projektes haben können.

Risk management is dynamic, iterative and responsive to change

»Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.« [ISO 31000:2009, 3. j) Risk management is dynamic, iterative and responsive to change]
»Wenn interne oder externe Ereignisse eintreten, sich der Zusammenhang und das Wissen verändern, sind die Risiken zu überwachen und zu überprüfen, es können neue Risiken auftreten, bestehende Risiken können sich verändern oder verschwinden. Deshalb sollte die Organisation sicherstellen, dass Risikomanagement laufend die Veränderungen feststellt und auf sie reagiert.« [ONR 49001:2010, 5.2.10 Risikomanagement ist dynamisch, iterativ und reagiert auf Veränderungen]

Operationalisiert bedeutet dieser Grundsatz, dass bei jeder Planänderung oder entsprechenden Entscheidung immer auch mindestens die Frage »Was kann schiefgehen?« zur Identifizierung von (neuen) Risiken gestellt werden sollte. Zum anderen sind die bereits bewerteten Risiken dahingehend zu hinterfragen, ob der Umgang mit ihnen (Vermeidung, Verminderung, Abwälzung und Akzeptanz) immer noch angemessen ist.

Aus dem Fallbeispiel ergeben sich keine Hinweise, dass der PL diesen Grundsatz berücksichtigt hat. Vielmehr wurde eine klar geänderte Situation nicht angemessen auf neue Risiken beleuchtet. Zudem akzeptierte der PL die verspätete Fertigstellung von Schnittstellen, ohne seinen Auftraggeber (Großhändler) über mögliche Folgen zu informieren.

2.1.4 Weitere Prinzipien

Die Kurzanalyse der Grundsätze mit dem Fallbeispiel zeigt, dass die Beachtung der Grundsätze einen positiven Einfluss auf das eingetretene Ergebnis gehabt hätte. Deshalb sollen auch die beiden in den Normen zuerst genannten Grundsätze noch in einen Kontext des Fallbeispiels gestellt werden. Diese Grundsätze sind allerdings sehr allgemeingültig formuliert, sodass die Analyse durch Fallbeispiele nur ergänzt werden kann.

Risk management creates and protects value

»Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.« [ISO 31000: 2009, 3. a) Risk management creates and protects value]
»Risikomanagement trägt zur sichtbaren Erreichung der Ziele und zur Verbesserung bei, z.B. in den Bereichen menschliche Gesundheit und Sicherheit, Einhaltung von gesetzlichen und regulatorischen Vorschriften, öffentliche Akzeptanz, Schutz der Umwelt, finanzielle Leistungsfähigkeit, Produktqualität, Wirksamkeit operationeller Tätigkeiten, gute Führung (Corporate Governance) und Reputation.« [ONR 49001:2010, 5.2.1 Risikomanagement schafft Werte]

Zum Wert (creates and protects value) lässt sich für das gewählte Fallbeispiel sagen, dass es sich gelohnt hätte, den Minimalaufwand für das RM zu investieren, da damit ggf. ein Schutz von Unternehmenswerten erreicht worden wäre.

Risk management is an integral part of all organizational processes

»Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.« [ISO 31000:2009, 3. b) Risk management is an integral part of all organizational processes.]
»Risikomanagement ist Bestandteil der Verantwortung des Managements und ein integrierter Teil der organisatorischen Prozesse genauso wie aller Projekte und Veränderungsprozesse. Risikomanagement ist keine selbständige Tätigkeit, die von den Hauptaktivitäten und Kernprozessen der Organisation getrennt ist.« [ONR 49001:2010, 5.2.2 Risikomanagement ist ein integrierter Teil von Organisationsprozessen]

Es ist sehr wichtig für den Großhändler, einen angemessenen Änderungsprozess mit dem Ziel der künftigen Fehlervermeidung zu etablieren. Er muss daher in systematischer Weise dafür Sorge tragen, dass das Risikomanagement in seine eigenen betrieblichen Abläufe integriert ist.

Risk management facilitates continual improvement of the organization

»Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.« [ISO 31000:2009, 3. k) Risk management facilitates continual improvement of the organization]
»Organisationen sollten Strategien entwickeln und umsetzen, um den Reifegrad ihres Risikomanagements entlang aller Aspekte ihrer Organisation zu verbessern.« [ONR 49001:2010, 5.2.11 Risikomanagement erleichtert die kontinuierliche Verbesserung der Organisation]

In moderne Managementmethoden gehört ein Grundsatz zur kontinuierlichen Verbesserung. So wäre es in dem Fallbeispiel bereits eine Verbesserung, wenn ein Minimal-RM eingeführt würde. Dieser Grundsatz würde bedeuten, dass zu Anfang Basisstrukturen geschaffen werden, die zunächst systematisch und dann kontinuierlich (evtl. modulartig) ausgebaut werden.

Fazit

Der Abgleich der Prinzipien mit einer an den täglichen Betriebsablauf angeglichenen Fallstudie zeigt, dass die Grundsätze des Risikomanagements durchaus nicht nur

rein theoretische Lehrsätze sind, sondern bei sinngemäßer Anwendung hohe Praxisrelavanz haben.

2.2 Rahmenwerk

Die ISO 31000 spricht im englischen Original von einem »framework«, wörtlich übersetzt »Rahmenwerk«.

Ganzheitliche ERM-Ansätze, wie die ISO 31000, basieren auf einem spekulativen Risikoverständnis, nach dem unter dem Risikobegriff sowohl Chancen (positive Abweichungen) als auch Gefahren (negative Abweichungen) subsumiert werden. Entsprechende Informationen müssen von den ERM-Subsystemen, wie dem IT-RM (z.B. wesentliche Chancen und Gefahren neuer Technologien), bereitgestellt werden. Die ISO 31000 gewährleistet, dass sich das IT-Risikomanagement an den Unternehmenszielen ausrichtet, Chancen und Gefahren der IT-Nutzung auf Basis einheitlicher Kriterien beurteilt und alle relevanten Unternehmensteile einbezieht.

Das IT-Risikomanagement ist ein Teilsystem des unternehmensweiten Risikomanagements (ERM). Die IT-Risiken stellen somit eine Teilmenge der Unternehmensrisiken dar.

Der Grundaufbau lehnt sich dabei an den bekannten »PDCA«-Zyklus der Managementsystemstandards ISO 9001, ISO 14001, ISO 27001 oder OHSAS 18001 an. Im Unterschied zu den vorgenannten Standards sieht er aber das Objekt seiner Beschreibung, das Risikomanagementsystem, nicht als eigenes Managementsystem an, sondern als Querschnittsfunktion. In der Konsequenz werden auch keine zertifizierungsfähigen Anforderungen formuliert.

Das Rahmenwerk – man könnte auch den Begriff »System« verwenden[4]– stellt sich wie folgt dar (siehe Abb. 2–1).

2.2.1 Auftrag und Vereinbarung

Die Initialisierung des Risikomanagements ist eine Aufgabe der Unternehmensleitung. Von hier aus muss der Wille zur Einrichtung und zum Betrieb eines Risikomanagements kommen. Besteht die Unternehmensleitung aus mehreren Mitgliedern, so sollte über die Grundsätze des unternehmensspezifischen Risikomanagements Einigkeit herrschen.

Die Risikopolitik wird in dieser Phase durch die Unternehmensleitung definiert; dabei sollte der CIO oder der im Unternehmen für IT Verantwortliche/Leiter IT zumindest für die IT-Risiken mitwirken.

Bei der Festlegung der Risikopolitik ist die Unternehmenskultur zu berücksichtigen. Bei stark IT-orientierten Unternehmen kann diese durch die IT-Prozesse und durch die IT-Mitarbeiter geprägt sein.

4. Siehe hierzu: ONR 49000-2010, Risikomanagement für Organisationen und Systeme.

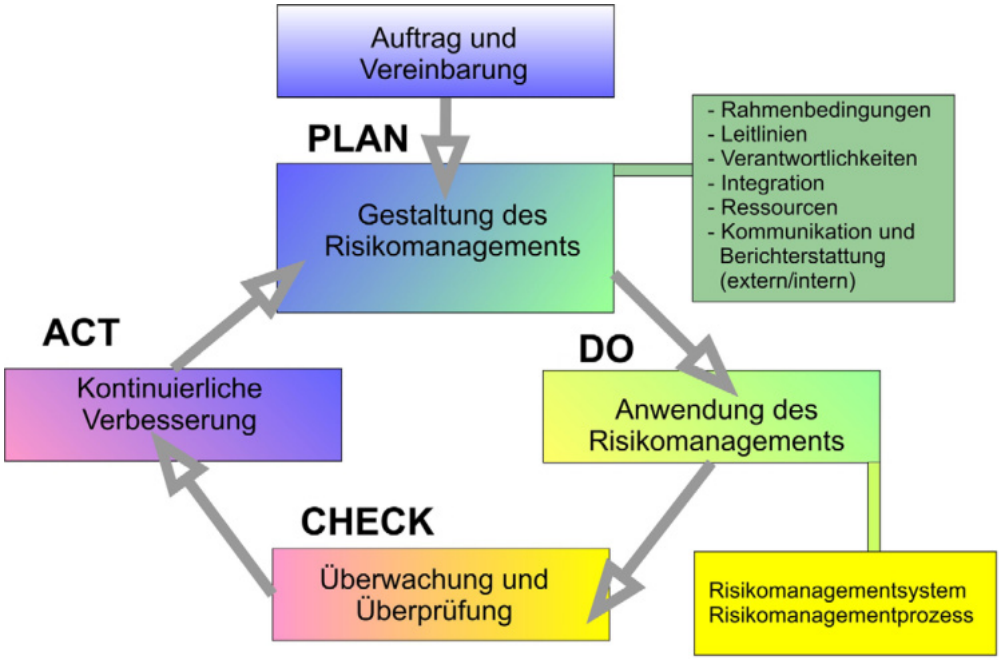


Abb. 2–1 *Rahmenwerk als PDCA-Zyklus*

Für das Risikomanagement müssen Kenngrößen beschlossen werden, die mit den Kenngrößen für die Unternehmensleitung in Einklang stehen. Die Kenngrößen des IT-Risikomanagements sollten daher aus der Unterstützungsfunktion der IT für die Geschäftsprozesse und deren korrespondierenden Kenngrößen abgeleitet werden. So kann z.B. die Anzahl der Trouble Tickets in einem Callcenter unmittelbar mit dem Risiko von ausufernden Ausfallzeiten während der Servicezeit in Verbindung gebracht werden, da hier das IT-Risiko von Betriebsstörungen in direktem Zusammenhang mit der Servicequote des Callcenters steht.

So wie die Ziele der IT in der Unterstützung der Ziele der Geschäftspolitik liegen, so muss auch sichergestellt werden, dass die durch das IT-Risikomanagement verfolgten Ziele sich im Rahmen der Ziele des Enterprise Risk Management (ERM) befinden und damit der Strategie des Unternehmens folgen.

Insbesondere in Unternehmen, deren IT sehr eng mit dem Produktionsprozess verbunden ist, wie z.B. Handels- oder Dienstleistungsunternehmen mit der Führung großer Kundendatenbanken, existieren IT-bezogene Compliance-Risiken aus den Bereichen Datenschutz, Urheberrecht, Gesundheitswesen usw. Hier ist ein hocheffizientes IT-Risikomanagement gefragt, da sich derartige Risiken im Falle ihres Eintritts zu schweren Krisen ausweiten können.

Setzt man sich mit IT-Risiken auseinander, stellen sich die zwei Kernfragen nach der Verantwortlichkeit und nach der Risikoausprägung. Im Risikomanagement sollen die Risikoeigner (Prozessverantwortliche) die Risiken identifizieren, analysieren, bewerten und angemessene Risikobehandlungsmaßnahmen abwägen und ggf. umsetzen. Damit tragen sie einen Großteil der Verantwortung für eine funktionierende Umsetzung des IT-Risikomanagements. Um IT-Risiken frühzeitig erkennen und beurteilen zu können, wird allerdings entsprechendes Fachwissen benötigt, über welches die eigentlichen Risikoeigner nicht immer verfügen. In der Praxis wird daher gerne dazu übergegangen, den Leiter der IT als Gesamtverantwortlichen der IT-Risiken zu benennen. Dieser sollte die Hauptrisiken für seinen IT-Betrieb feststellen und angemessene Maßnahmenoptionen festlegen. Dabei wird der Leiter der IT versuchen, möglichst viele standardisierte IT-Lösungen anzubieten, um das Risiko überschaubar zu halten. In diesem Falle muss er lediglich seine Einschätzung mit der des Risikoeigners abstimmen. Eine weitere Risikobewertung durch den Risikoeigner ist somit nicht mehr nötig. Bei größeren Organisationen wird dieses interne Abstimmen mithilfe von Service Level Agreements schriftlich fixiert.

Differenzierter ist der zweite Fall im Hinblick auf IT-Risiken zu sehen, wenn Teillösungen (z.B. RZ-Betrieb von Servern, die beim Betriebssystem enden) durch die IT zur Verfügung gestellt werden. Wenn dann ein Dritter den weiteren Betrieb von z.B. einer Datenbank und einer Anwendung übernimmt, sollte der Risikoeigner die IT-Risiken des Dritten bewerten. In diesem Fall wird der Leiter der IT nur für den Teil der Risiken die Verantwortung übernehmen, den er noch selbst verantworten kann. Die restlichen Risiken müssen vom Risikoeigner selbst gepflegt und übernommen werden. Dieser Mischbetrieb stellt aus IT-Risikogesichtspunkten die wohl größte Herausforderung dar, da eine Aufteilung der Verantwortlichkeiten und des damit verbundenen Risikos nicht immer exakt erfolgen kann.

Der dritte Fall der IT-Risikobetrachtung stellen das IT-Outsourcing und die Cloud-Services dar. Hier nutzt der Risikoeigner nur noch die von der IT zur Verfügung gestellte Datenkommunikation, der Rest wurde an einen externen Dienstleister ausgelagert. Eine Risikoübertragung kann auch auf einen externen IT-Anbieter erfolgen, wobei diese nur unter den Voraussetzungen von z.B. bestehenden Sicherheits- und Datenschutzrichtlinien möglich ist. Andernfalls würde für Outsourcing ein geringeres Risikoniveau gelten als für die internen IT-Risiken. Ferner liegt die Verantwortlichkeit der IT-Risiken vollständig beim Risikoeigner, der die IT-Risiken des Dritten bewerten muss.

Allen drei Fällen gemeinsam ist jedoch, dass die IT-Risiken und die Verantwortlichkeiten, die der Leiter der IT und/oder der Risikoeigner tragen, transparent und vollständig dokumentiert sein müssen. In den Fällen zwei und drei muss der Risikoeigner sich jedoch bewusst sein, dass die Risiken außerhalb des internen IT-Betriebs vollständig von ihm verantwortet werden müssen.

Damit verbunden sollte auch das gemeinsame Verständnis sein, dass Risikomanagement nicht zum »Nulltarif« erfolgen kann, sondern mit angemessenen Personal- und Sachmitteln ausgestattet werden muss.

Alle interessierten Gruppen (Aufsichts- und Verwaltungsräte, wichtige Kunden und Lieferanten, Aufsichts- und Regulierungsbehörden usw.) sollten über die Vorteile des Risikomanagements unterrichtet werden; dabei kommt dem IT-Risikomanagement stets dann herausragende Bedeutung zu, wenn die interessierten Gruppen mit oder über die IT mit dem Unternehmen in Verbindung treten.

Es muss letztlich sichergestellt werden, dass das Risikomanagementsystem angemessen für das Unternehmen ist. Die IT als innovativer Bereich muss hierzu ihren Teil beitragen.

2.2.2 Gestaltung des IT-Risikomanagements

Sind die grundsätzlichen Voraussetzungen auf der Ebene der Unternehmensleitung einschließlich des Leiters der IT geregelt und festgeschrieben, so kann mit der konkreten Ausgestaltung des IT-Risikomanagements begonnen werden.

Für das IT-Risikomanagement ist der Leiter der IT der Teil der Unternehmensleitung, der das IT-Risikomanagement in Abstimmung mit dem ERM gestaltet. In diesem Rahmen sollte er …

- … im Zusammenwirken mit dem Vorstandsvorsitzenden/Geschäftsführer die *Rahmenbedingungen des IT-Risikomanagements* klären und festschreiben.
- … in Abstimmung mit den in der Risikoleitlinie (ERM) des Unternehmens festgehaltenen Grundsätzen notwendige *spezielle Richtlinien* für den IT-Bereich erlassen.
- … einen Durchführungsverantwortlichen *für den IT-Bereich als Beauftragten* ernennen und diesem ggf. weitere Mitwirkende zuordnen. Für die so geschaffenen Rollen sollten die Aufgaben möglichst präzise beschrieben werden.
- … die *Integration der IT-Risiken* mit der Risikobeurteilung und -bewältigung der ERM-Risiken vorantreiben; dabei muss die Unterstützungsfunktion der IT für die Geschäftsprozesse stets erkennbar im Vordergrund stehen.
- … aufgrund seiner Position als Leiter IT die *notwendigen Ressourcen* sowohl an Personal – es muss ausreichend Arbeitszeit für das Risikomanagement zur Verfügung stehen – als auch an erforderlichen Sachmitteln für das Management der Risiken bereitstellen. Dies schließt Projekte zur Risikominimierung mit ein. Hierher gehört auch ein ausreichendes Budget für Schulungsaufwendungen. Dieses wird nach der Risikobewertung durch die Unternehmensführung von dem verursachenden Geschäftsbereich oder der Unternehmensführung bereitgestellt.
- … als Leiter IT weiterhin sicherstellen, dass über IT-Risiken eine angemessene und sachgerechte *Kommunikation* aufgebaut wird. Diese Forderung richtet sich zunächst für das *IT-interne Berichtswesen* an ihn selbst: Der IT-Leiter muss jederzeit über ein aktuelles und zutreffendes Bild von der Risikolage im IT-Bereich verfügen. Es muss sowohl ein regelmäßiges Risiko-Reporting als auch eine Ad-hoc-Berichtsmöglichkeit vorhanden sein. Beim *IT-externen Berichtswesen* ist der Leiter IT eventuell auch in eigener Position gefragt, da es – je nach Gesellschaftsstruktur und Rechtsform – zu seinen Aufgaben gehören kann, gegenüber dem Aufsichtsgremium über die IT-Risiken zu berichten.

Insgesamt ist es die Aufgabe des Leiters IT, die Gestaltungsphase (siehe Abb. 2–1) so einzuleiten (Plan), dass in der Folge ein erfolgreiches IT-Risikomanagement möglich ist (Do). Dies kann auch zu einem Zeitpunkt notwendig werden, wenn durch erhebliche Änderungen im Unternehmen mit entsprechenden Auswirkungen auf die IT – z.B. Outsourcing, Fusion, Technologiewechsel, Marktveränderungen (Check) – wieder ein neuer Startpunkt für das IT-Risikomanagement geboten erscheint (Act).

2.2.3 Anwendung des Risikomanagements

Bei der Umsetzung des IT-Risikomanagementsystems sollte das Unternehmen folgende Punkte beachten:

- Das Unternehmen sollte eine Risikostrategie definieren und für die Einführung passende Zeitpläne entwickeln. Dabei sollten die für die IT typischen Risiken berücksichtigt werden, z.B. Hackerangriffe, physisches und logisches Zugriffsmanagement, Systemstabilität, Business Continuity und Disaster Recovery Management, Patch-Management-Zyklen oder auch Projektphasen von IT-Projekten.
- Das Risikomanagementsystem für die IT darf nicht nur technisch orientiert sein, sondern muss auch gesetzliche, behördliche und aufsichtsrechtliche Compliance-Risiken berücksichtigen (vor allem Datenschutz und Informationssicherheit, Aufbewahrung digitaler Unterlagen usw.).
- Entscheidungen in der IT, auch Entwicklungen und Zielsetzungen, sollten grundsätzlich unter Berücksichtigung des Risikomanagements getroffen werden. Risikoreiche IT-Trends bedürfen einer angemessenen Risikobewertung!
- IT-Mitarbeiter und Führungskräfte sollten in den Grundzügen des Risikomanagements geschult werden.
- Die Kommunikation zu interessierten Parteien, wie Aufsichts- und Verwaltungsräten, sollte verdeutlichen, dass IT-Risiken angemessen und erfolgreich gesteuert werden.

2.2.3.1 Anwendung des Risikomanagementprozesses in der IT

Zur Umsetzung des Risikomanagementprozesses in den nachfolgend beschriebenen Phasen sollte ein Plan für das IT-Risikomanagement aufgestellt werden, der sicherstellt, dass alle relevanten Ebenen und Funktionen der IT als Bestandteil des Prozesses einbezogen werden. Hier sollte durch eine ganzheitliche Sicht auf die Unternehmens-IT sichergestellt werden, dass keine »weißen Flecken« in bestimmten Bereichen der IT unberücksichtigt bleiben.

Die operativen Ebenen der IT – Event-, Incident-, Problem-, Access-Management, Service-Desk etc. – müssen ihren Beitrag in den einzelnen Phasen des Risikomanagementprozesses leisten, um technisch und organisatorisch sachgerechte Bewertungen und Maßnahmen zu erstellen.

2.2.4 Überwachung und Überprüfung

Um sicherzustellen, dass das IT-Risikomanagement wirksam ist und fortlaufend den IT-Betrieb des Unternehmens unterstützt, sollte der Leiter IT …

- … Metriken zur Wirkung des Risikomanagements einsetzen und deren Angemessenheit regelmäßig überprüfen. Für Metriken im Bereich der Informationssicherheit kann auf die *ISO 27004*, »Measurement«[5] verwiesen werden, die umfangreich und detailliert auf Anforderungen und Möglichkeiten der IS-Metrik eingeht.
- … regelmäßig den Fortschritt bei Beurteilung und Behandlung der IT-Risiken und die Abweichung vom IT-Risikomanagementplan feststellen.
- … ebenfalls regelmäßig überprüfen, ob das Risikomanagementsystem in der IT und die daraus entwickelte Planung noch angemessen sind; und ob es aus Sicht der IT und ihrem Verhältnis zu den externen und internen Rahmenbedingungen Änderungsbedarf in der Risikopolitik gibt.
- … gegenüber der Unternehmensleitung über die IT-Risikosituation berichten und einen Eindruck wiedergeben, inwieweit der Risikopolitik des Unternehmens gefolgt wird.
- … sich im Rahmen seiner Verantwortung für die IT des Unternehmens bei einer Managementbewertung von der Wirksamkeit des Systems für die IT-Risiken überzeugen.

5. *www.iso.org*, ISO/IEC 27004:2009, Information technology – Security techniques – Information security management – Measurement.

Die Managementbewertung des ERM ist grundsätzlich die Aufgabe der Unternehmensleitung. Hat ein Leiter IT beispielsweise einen Platz in einem Vorstand einer Aktiengesellschaft, so ist er sowohl im Rahmen seiner Gesamtverantwortung dem ERM verpflichtet als auch als Ressortvorstand in besonderem Maße mit dem Steuern und Überwachen der IT-Risiken betraut.

Ist der Leiter IT auf der zweiten Führungsebene – z.B. im Direktorenrang in einer Familiengesellschaft – angesiedelt, so fügt sich seine Verantwortung, einschließlich der Berichtsverantwortung, als Teil in die Gesamtmanagementverantwortung der Unternehmensleitung ein.

2.2.5 Kontinuierliche Verbesserung

Basierend auf Überprüfung und Überwachung des IT-Risikomanagements sollte in angemessenen Zeitabständen und in angemessenem Rahmen entschieden werden, wie das IT-Risikomanagement bezüglich Planung und Systemkomponenten verbessert werden kann. Es sollten ggf. auch Verbesserungen, die im IT-Risikomanagement erkannt werden, in das allgemeine Risikomanagement des Unternehmens oder der Organisation (ERM) transportiert werden.

Das Resultat ist ein Prozess der ständigen Verbesserung, der die Fähigkeiten der IT – und damit eines bedeutenden Unternehmensteils – laufend darin stärkt, mit IT-Risiken umzugehen und eine erfolgreiche Risikokultur zu pflegen.

2.3 Prozess

Abbildung 2–2 zeigt den gesamten Risikomanagementprozess in einer grafischen Darstellung (siehe auch ISO 31010, Abschnitt 5.1): Er ist als »Do«-Abschnitt des PDCA-Zyklus zu verstehen. Dies bedingt, dass der gesamte Prozess – einschließlich der prozessinternen Überwachung und Datenkommunikation – ganzheitlich als ein Teil des PDCA-Zyklus angesehen wird, und die Teile »Check« und »Act« als außerhalb liegende Aktivitäten des Managements und seiner Organe verstanden werden.

2.3.1 Rahmenbedingungen – Kontext

Die Rahmenbedingungen, unter denen Risikomanagement in einem Unternehmen stattfindet, müssen in Bezug auf die Schritte des Risikomanagementprozesses geklärt sein, da sie die wichtigsten Basisgrößen liefern.

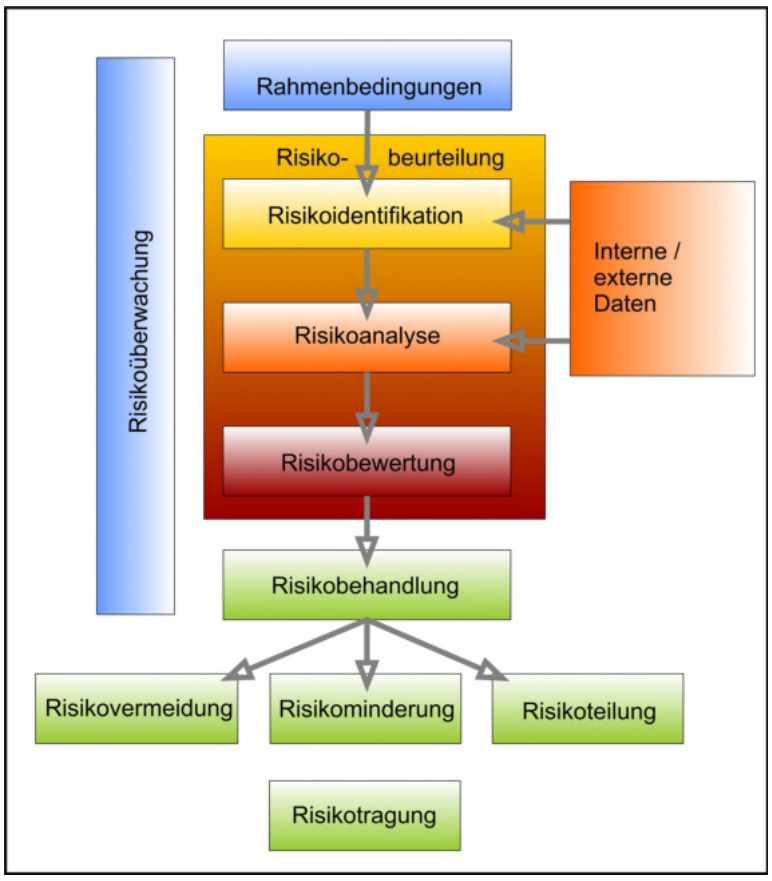


Abb. 2–2 *Grafische Darstellung des Risikomanagementprozesses*

Für das IT-Risikomanagement sind dies insbesondere die Rahmenbedingungen der IT im Unternehmen, die die Grundlage des IT-Risikomanagements bilden. Dazu zählen:

- Die Abhängigkeit der Geschäftsprozesse von der IT
- Die Kapitalbindung in der IT (ein Dienstleistungsunternehmen wird im Durchschnitt eine höhere Kapitalbindung in der IT haben als ein Fertigungsunternehmen, das über Produktionsmaschinen verfügt)
- Die Vertraulichkeits-, Verfügbarkeits- und Integritätsanforderungen an die Informationswerte (z.B. Personendaten oder Firmengeheimnisse)
- Der Grad der Außenanbindung des Unternehmens (z.B. im E-Commerce)
- Der Umfang gesetzlicher und sonstiger regulatorischer Anforderungen an die IT (SOX, MAS, GDPdU, BDSG, TKG)
- U.v.m.

Die Zusammenstellung aller relevanten Faktoren ergibt einen Gesamtkontext für das IT-Risikomanagement. Dabei kann zwischen internen (z.B. Schutzbedarf der Informationswerte) und externen (z.B. regulatorischen) Einflussgrößen unterschieden werden. Dies prägt z.B. die Flexibilität des Risikomanagements, da gesetzliche Anforderungen in der Regel nicht von Unternehmen in ihrer Existenz oder Wirkung beeinflusst werden können. Dazu gehören auch Faktoren wie die Rechtsform und die – meist dadurch bedingte – Form der Unternehmensführung. Je nachdem, ob ein Familienbetrieb mit Einzelkaufmann oder ein Konzernunternehmen mit delegierten Vorstandsmitgliedern mehrerer Mutterunternehmen vorliegt, wird sich die persönliche Risikobereitschaft der Mitglieder der Unternehmensführung unterschiedlich entwickeln.

Auf das IT-Risikomanagement wird sich dies insofern auswirken, als dass der generelle Risikoappetit der Unternehmensführung auch der Maßstab für die Kriterien des IT-Risikomanagements sein sollte. Diese Risikokriterien, bezogen auf die IT, müssen aber feststehen, um die Bewertung und Behandlung von Risiken im Sinne der Unternehmensführung steuern zu können.

2.3.2 Risikobeurteilung

2.3.2.1 Risikoidentifikation

Der erste Prozessabschnitt der Risikobeurteilung ist die Identifikation von Risiken. Bei der Identifikation IT-

bezogener Risiken wird der Aspekt der Sicherheit der Informationswerte gewöhnlicherweise im Vordergrund stehen. Hier kann dieser Schritt auch durch erhebliche Mengen an externen Quellen unterstützt werden. Es ist also nicht notwendig, alle Risiken durch Überlegung »vom grünen Tisch aus« zu identifizieren, sondern – ganz im Sinne des Standards – bereits geleistete Arbeit zu nutzen. Als Hilfe zur Identifikation können externe Quellen herangezogen werden, dazu zählen:

- Die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI), hierbei insbesondere die Kataloge zu »Gefährdungen« *http://www.bsi.bund.de/DE/Themen/weitere Themen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html*
- Die Information Security Resources des SANS-Institutes, hier z.B. die TOP 25 Most Dangerous Software Errors *http://www.sans.org/top25-software-errors/?utm_campaign=resources&utm_source=featured & utm_ medium=web&utm_content=top25*
- DsiN.de – Deutschland sicher im Netz *http://www.sicher-im-netz.de/sites/default/files/download/sicherimnetz_leitfaden_30112012_ final.pdf*

Jedoch sollte man auch die internen Quellen intensiv nutzen:

- Malware-Statistik des internen Antivirenschutzes
- Firewall- bzw. Proxyprotokolle über Eindringversuche
- IDS-Protokolle der Firewall
- Incident-Meldungen der Mitarbeiter des Helpdesks
- Auswertung des Vulnerability- und Patch-Managements
- Bedrohungen aus Blogs, Foren und sozialen Netzwerken

Die o.a. IT-Sicherheitsrisiken sollten aber nicht dazu führen, andere Risiken außer Acht zu lassen. Hierzu zählen:

- Wirtschaftliche Risiken der IT
- Compliance-Risiken der IT (z.B. bezogen auf IT-typische Gesetze wie BDSG, TKG, UrhG u.v.m.)

Auch hierzu sind ggf. externe wie interne Quellen nützlich, um ohne redundanten Aufwand und mit gemindertem Fehlerrisiko die typischen Risiken identifizieren zu können. Als externe Quelle kann hierzu z.B. COBIT 5.0 empfohlen werden.

Der Teilprozess der Risikoidentifikation hat die Aufgabe, ein unternehmensspezifisches Portfolio an Risiken zusammenzustellen, und zwar in Blickrichtung IT-Risiken. Die Risikoanalyse dient dazu, diese Risiken nach ihrem Charakter und ihrer Systematik und der Ursache-Wirkungs-Kette zu verstehen.

2.3.2.2 Risikoanalyse

In der Risikoanalyse geht es um die vertiefte Untersuchung der Ursache-Wirkungs-Mechanismen der festgestellten Risiken. Nur ein gutes Verständnis der identifizierten Risiken ermöglicht ihre sachgerechte Bewertung und Behandlung. Zur Analyse stehen eine Vielzahl von Methoden bereit. Die ISO 31010 bietet hier eine Reihe von Techniken, die auf unterschiedliche Risikosituationen angewendet werden können (siehe Kap. 3).

Risikoanalysen können dann kreative Prozesse sein, wenn bereits eine ungefähre Vorstellung des Risikos vorliegt, aber noch keine erkennbaren Wege zur Vertiefung des Verständnisses vorgezeichnet sind. In diesem Fall können verschiedene Kreativtechniken und Fachleute aus unterschiedlichen Bereichen dabei helfen, sich der spezifischen Risikosituation des Unternehmens anzunähern bzw. diese für die IT-Prozesse zu konkretisieren.

IT-Risiken erscheinen oft durch Veröffentlichungen und Diskussionen gut bekannt, sodass man fälschlicherweise annehmen könnte, auf eine eingehende Analyse verzichten zu können. Dies ist jedoch insofern ein Trugschluss, als dass sich die Einbettung einer IT-Landschaft in die Unternehmenszusammenhänge in der Regel sehr komplex darstellt und je nach Unternehmensausrichtung sehr individuell ist. Gerade in diesen Fällen bedarf es daher einer eingehenden Analyse. Grundsätzlich wird zwischen qualitativen und quantitativen Analysen unterschieden. Im Bereich der IT wird die qualitative Analyse zusätzlich noch in eher technisch bzw. organisatorisch orientierte Analysen differenziert.

Zur Optimierung der organisatorischen Analyse kann man auf den Methodenkatalog der ISO 31010 (siehe Kap. 3) zurückgreifen. Die für die eigene Situation passenden Methoden und Techniken können dann ausgewählt und angewendet werden. Insbesondere die Risiken aus IT-Projekten, der IT-Entwicklung, der IT-Wartung und dem IT-Service sollten aus organisatorischer Sicht intensiv analysiert werden.

Bei der rein technischen Risikoanalyse – diese ist im Zusammenhang mit Risiken der IT-Sicherheit unbedingt erforderlich – sollten Werkzeuge zum Einsatz kommen, die die vorhandenen Systeme analysieren und eine erste Risikoindikation vornehmen (z.B. in »Ampelfarben«). Derartige Analysen sollten für alle wichtigen Schnittstellen des IT-Systems sowie zumindest repräsentativ für sys-

temgleiche Komponenten vorliegen. Die nachfolgenden Abbildungen 2–3 bis 2–5 zeigen einige Beispiele für Werkzeuge, die einen risikoanalytischen Ansatz mit farblicher Verdeutlichung der Risikoeinstufung vornehmen.

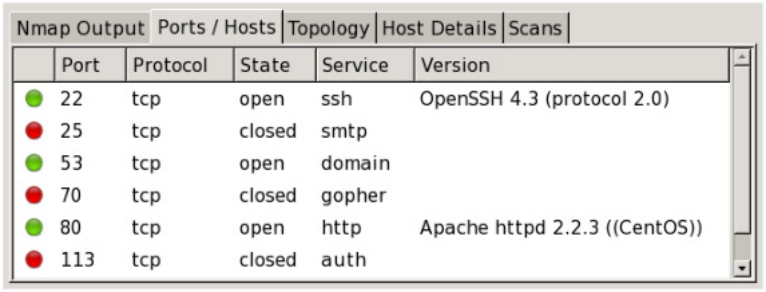


Abb. 2–3 *Beispiel aus nmap/zenmap, http://nmap.org/book/zenmap-results.html*

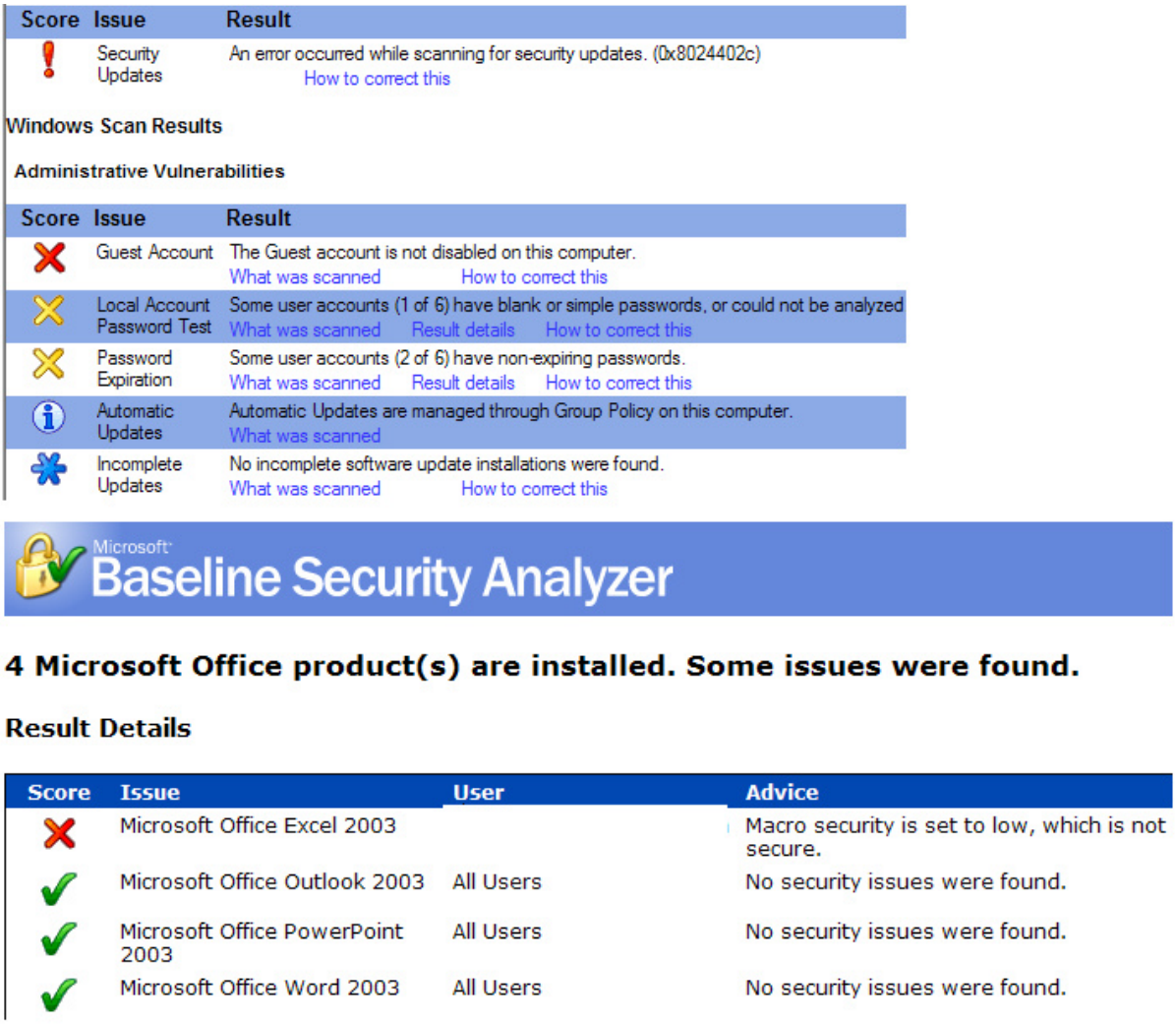


Abb. 2–4 *Beispiele aus Microsoft Baseline Security Analyzer©, http://technet.microsoft.com/de-de/security/cc184924.aspx*

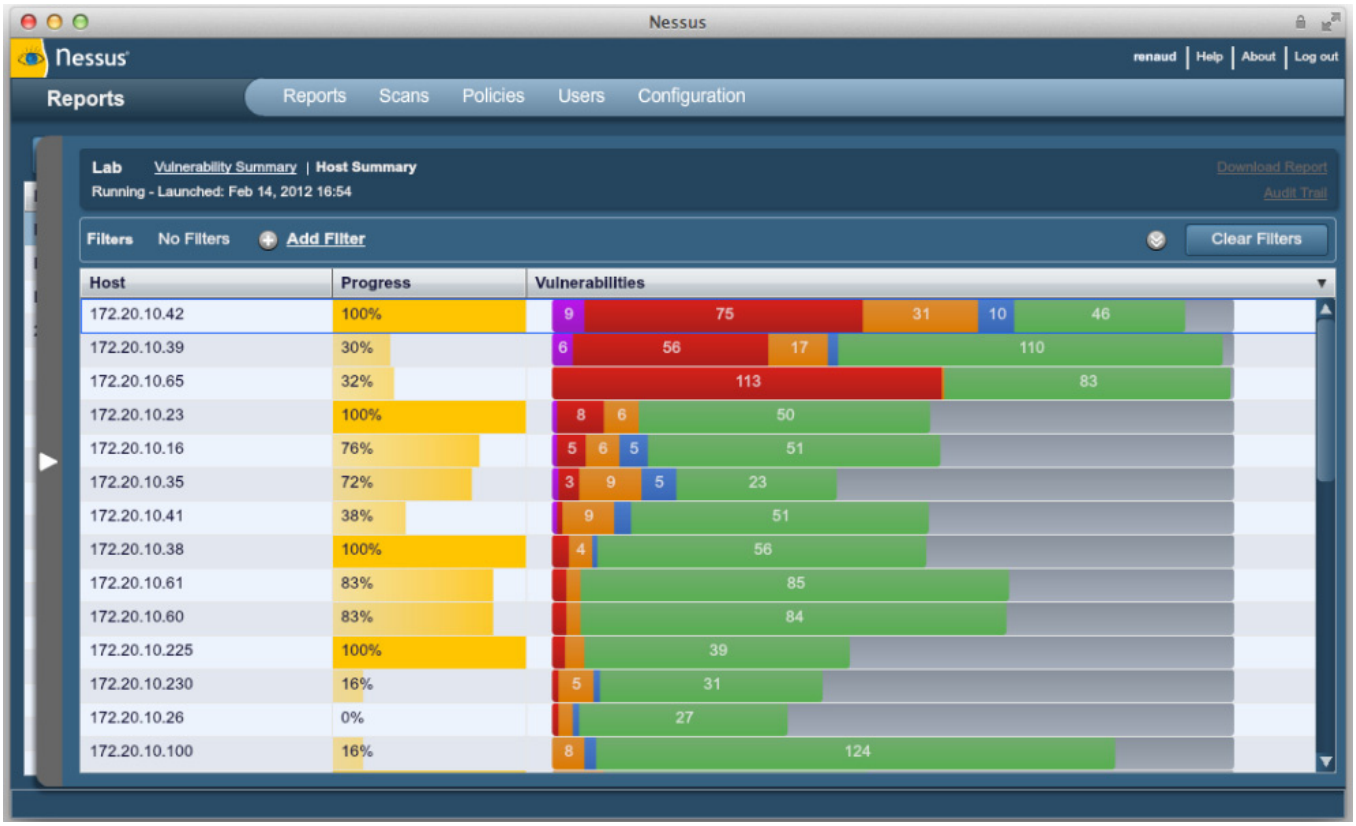


Abb. 2–5 *Beispiel NESSUS©, http://www.nessus.org/products/nessus/nessus-product-overview*

Techniken, wie sie in der grafischen Analyse von Risiken genutzt werden, sind auch Bestandteil von Programmen zur Sicherheitsanalyse.

Ziel der Risikoanalyse muss es sein, alle IT-Risiken so gut zu verstehen, dass ein für sachverständige Dritte nachvollziehbares Bild der Risikolage im IT-Bereich resultiert.

Hierbei sollten – wo möglich – interne Analyseergebnisse durch externe Daten ergänzt werden, um ein möglichst objektives Bild der Gesamtsituation zu zeichnen und der Gefahr einer »Betriebsblindheit« zu begegnen. Dazu können z.B. anerkannte Studien herangezogen werden, beispielsweise:

- Die »Schwachstellenampel« des Bundesamtes für Sicherheit in der Informationstechnik (BSI) *https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Gefaehrdungslage/Schwachstellenampel/cs_schwachstellenampel.html;jsessionid=CBD21E78C43181BC4BC62FA7743B0FC7.2_cid294*
- <kes>/Microsoft-Sicherheitsstudie 2012 *http://www.kes.info/archiv/material/studie2012/index.html*
- Die Newsletter der SANS-Organisation (beispielhaft) *http://www.sans.org/newsletters/#risk*

2.3.2.3 Risikobewertung

Nach einer sorgfältigen Risikoanalyse gilt es nun, IT-Risiken messbar zu machen. Dazu muss eine Bewertung vorgenommen werden, die unterschiedliche Risiken vergleichbar macht und die die Voraussetzung dafür schafft, dass endliche Ressourcen zur Risikobehandlung den Risiken nach ihrem Schweregrad zugeteilt werden.

Die meisten Risikobewertungen werden anhand einer Matrix vorgenommen, die die Auswirkung und Wahrscheinlichkeit auf der x- bzw. y-Achse darstellen (vgl. ISO 27005:2010, Anhang E; ONR 49001, Kap. 5; ISO 31010, B29.3, Abb. B15).

Dabei werden die Felder der Matrix meist mehrfarbig oder mit verbaler Erläuterung in Risikobereiche eingeteilt (siehe Abb. 2–6), z.B. von »grün« für ein unwahrscheinliches Risiko mit sehr geringen Auswirkungen bis »(dunkel)rot« für ein katastrophales Risiko mit sehr hoher Eintrittswahrscheinlichkeit.

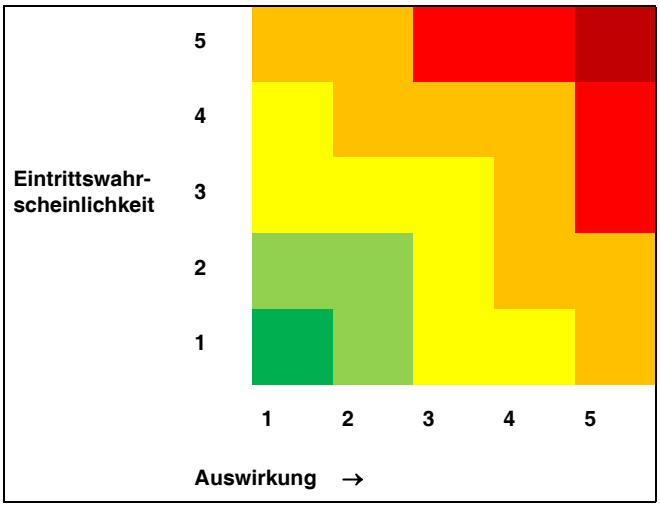


Abb. 2–6 *Risikobewertung anhand einer Matrix*

Bei den IT-Risiken besteht die Aufgabe in einer begründeten richtigen Zuweisung normierter Attribute. Aus der Risikoanalyse ist ein Verständnis für das jeweilige IT-Risiko entstanden. Dieses muss nun in einer meist auch für Nicht-IT-Risken gültigen Einstufung eingeordnet werden. Hier helfen etwas detailliertere Beschreibungen der einzelnen Einstufungen mit IT-typischen Wertungskriterien. Im Bereich der IT-Sicherheit ist es z.B. sinnvoll, die klassischen Werte der IT-Sicherheit, die auch in der ISO 27001 zugrunde gelegt werden, als Wertungsmaßstab heranzuziehen: Vertraulichkeit, Verfügbarkeit und Integrität.

Ein Beispiel, wie man die einzelnen Wertungsstufen in verbaler Form erläutern kann, zeigt Tabelle 2–1.

Grundwert → **Bewertungsziffer ↓**	**Vertraulichkeit**	**Verfügbarkeit**	**Integrität**
1 unbedeutend	Die Vertraulichkeit von Informationen, die eigentlich nicht über den vorgesehenen Kreis hinausgehen sollten, wurde nicht gewahrt. Es handelte sich aber um eine begrenzte Zahl interner Mitarbeiter, die im Nachgang relativ aufwendig zur Verschwiegenheit ausdrücklich verpflichtet werden.	Informationen von geringerer Bedeutung stehen zeitweise nicht zur Verfügung, können aber mit einem begrenzten Aufwand wieder nutzbar gemacht werden.	Informationen erfahren geringfügige Änderungen, die jedoch rasch bemerkt und mit gutem Erfolg korrigiert werden können; dies verursacht einen begrenzten Aufwand.
2 gering	Es gelangen in geringem Maße Informationen nach außen, die nicht für die Öffentlichkeit bestimmt waren. Die Informationen sind jedoch nicht personenbezogen und haben auch keinen anderen kritischen Wert.	Prozesswirksame Informationen stehen für kurze Zeit nicht zur Verfügung. Nach Wiederherstellung des Informationsstands entsteht Aufwand durch die Aufarbeitung.	Informationen sind verändert worden, die wieder korrigiert werden müssen. Dies ist mit Such-, Änderungs- und Kontrollaufwand möglich.
3 spürbar	Es gelangen vertrauliche Informationen in die Öffentlichkeit, die eine Rechtfertigung bei den Aufsichtsgremien erforderlich machen.	Es fehlen wesentliche Daten, deren Rekonstruktion aufwendig ist und eine Restunsicherheit zur Vollständigkeit beinhaltet. Der Betrieb wird durch diesen Verlust eingeschränkt.	Informationen sind so verändert worden, dass Folgefehler auftreten, die wiederum Imageverlust und Zusatzaufwand in mehreren Bereichen nach sich ziehen.
4 kritisch	Es gelangen vertrauliche Daten in solcher Menge und Sensitivität in die Öffentlichkeit, dass eine Rechtfertigung in der Presse notwendig ist. Es entstehen Zweifel an der Zuverlässigkeit der Informationssicherheit.	Es fehlen so umfangreiche Teile der Daten, dass eine vollständige Wiederherstellung nicht möglich ist. Der Umgang mit den Verlusten ist sehr aufwendig und stellt Teile des Jahresabschlusses infrage.	Informationen (Datenbestände) werden so stark verändert, dass außenwirksame Folgefehler entstehen, der Änderungsaufwand erheblich ist und haushaltswirksame finanzielle sowie grundsätzliche Ansehensverluste eintreten. Es werden Zweifel an der Qualität der Informationshaltung (Datenhaltung) geäußert.
5 katastrophal	Es gelangen massenweise Informationen (personenbezogene Daten) an die Öffentlichkeit, sodass die Stakeholder jedes Vertrauen in die Informationssicherheit des Unternehmens verlieren.	Große Mengen an Informationen (Kundendaten) gehen unwiederbringlich verloren. Die Weiterführung des Betriebs ist nicht mehr möglich.	Massive Änderungen an großen Datenbeständen stellen die Funktionsfähigkeit des Betriebs grundsätzlich infrage, das Unternehmen kann sein Kerngeschäft nicht mehr betreiben.

Tab. 2–1 *Wertungsstufen für Vertraulichkeit, Verfügbarkeit und Integrität*

Darüberhinaus sind auch andere Werte vorstellbar, z.B. Web-Trust-Kriterien wie Verbindlichkeit oder Datenschutz. Die Kriterien sollten so beschrieben sein, dass sich sowohl der Entscheidungsträger, der die Bewertung als seine Handlungsvorlage heranzieht, als auch der IT-Spezialist, der den IT-Risikobehandlungsplan sachgerecht umsetzen muss, eine möglichst gleiche Auffassung hierüber haben.

2.3.3 Risikobehandlung/Risikobewältigung

Nach abgeschlossener Risikobewertung sollte eine Risikolandschaft der IT des Unternehmens vorliegen, die eine Priorisierung von Maßnahmen zur Risikobehandlung (wird auch als Risikobewältigung bezeichnet) ermöglicht.

Maßnahmen zur Risikobehandlung sollten folgende Eigenschaften aufweisen:

- Eine Priorisierung, nach der verschiedene Maßnahmen ergriffen werden oder man ggf. von ihnen Abstand nimmt (siehe ISO 31000, Abschnitt 5.5.2).
- Einen benannten Verantwortlichen, einen oder mehrere Durchführende, einen oder mehrere Mitwirkende sowie einen oder mehrere Informierte. Das können z.B. als Verantwortlicher der Leiter eines Serverzentrums sein, als Durchführender der Directory-Administrator, als Mitwirkender der Web-Administrator und als Informierter und Budgetsponsor der Leiter IT (siehe ISO 31000, Abschnitt 5.5.3).
- Eine Terminsetzung, zu der die Maßnahme erfolgen soll; diese kann einmalig sein und in der Zukunft liegen, sie kann aber auch angeben, wie häufig die Maßnahme erfolgen soll und auf eine Frequenz wiederkehrender Aktionen hinweisen (z.B. periodisch: täglich, wöchentlich; oder ereignisbezogen: bei Rechnungsstellung etc.). Dies ist notwendig, wenn das Risiko auf wiederkehrenden Aktivitäten basiert (z.B. Datensicherung durch Back-up Tapes).
- Den Aufwand bzw. die Kosten, die mit der Maßnahme verbunden sind; auch hier können Einmalkosten (z.B. Anschaffung von Hardware/Software) oder laufende Kosten (Beschäftigung eines Administrators) anfallen.
- Die Art der Risikobehandlung (s.u.) sollte gekennzeichnet werden.

Für die Risikobehandlung oder -bewältigung stehen grundsätzlich drei aktive Varianten und eine passive zur Verfügung (siehe auch Abb. 2–7):

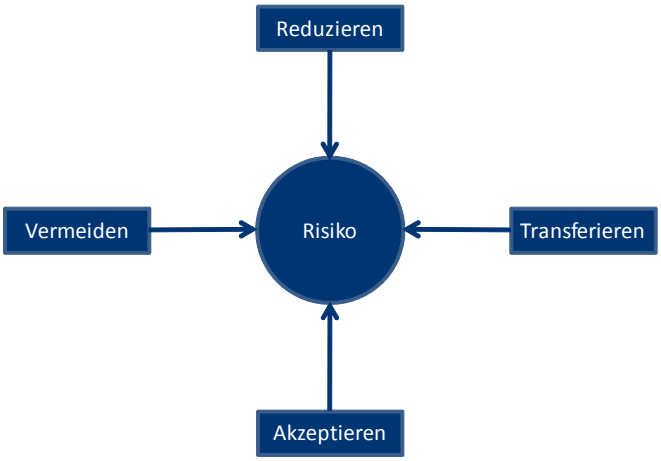


Abb. 2–7 *Maßnahmenkategorien zur Risikobehandlung bzw. -bewältigung*

- Ein Risiko wird *vermieden*, d.h., dass die Prozesse, die eine Gefährdung auslösen können, von vornherein fallengelassen werden. So können z.B. Risiken, die durch Onlineverkäufe entstehen können, vermieden werden, wenn keine B2C-Verbindung aufgebaut wird. IT-Risiken können in der Praxis häufig vermieden werden, indem z.B. ein anfälliges System abgeschaltet oder ein Prozessschritt eliminiert wird.
- Ein Risiko wird *gemindert/reduziert*, indem man auf die Wahrscheinlichkeit seines Eintritts oder auf die Auswirkungen im Fall eines Eintritts Einfluss nimmt. So ist das Auslegen von schwer entflammbarem Bodenbelag im Serverzentrum eine Maßnahme, die die Eintrittswahrscheinlichkeit eines Brandes senkt. Die Installation einer Feuerlöschanlage mit Inertgas oder Sauerstoffreduzierung ist eine Maßnahme, die den Brand, der einmal ausgebrochen ist, und damit die daraus entstehenden Schäden, mindert.
- Ein Risiko kann auch *geteilt* bzw. auf andere *transferiert (abgewälzt)* werden: Das Outsourcing von Serverleistungen mit Vereinbarung eines Service Level Agreement (SLA) ist eine Möglichkeit, mit dem Serverbetrieb verbundene Risiken an einen Dritten weiterzugeben. Ein Risikotransfer findet in der Praxis häufig auch dann statt, wenn z.B. ein Versicherungsunternehmen bei Eintritt des Risikos für eine bestimmte Schadenssumme aufkommt.
- Eine letzte Möglichkeit ist die bewusste Risikoübernahme oder Risiko*tragung* (auch mit dem Begriff *Risikoakzeptanz* verbunden). Hierbei werden die oben genannten aktiven Varianten nicht gewählt, sondern das Risiko wird bewusst übernommen. Die einzige Aktivität liegt hier in der Erklärung der Entscheider, in Kenntnis der Risikobeurteilung so zu verfahren. Ein IT-Risiko zu akzeptieren ist eventuell

dann zu empfehlen, wenn die Kosten für eine Maßnahme weitaus höher sind als die damit verbundene Risikoreduktion, oder das identifizierte IT-Risiko sehr gering ist. Diese Entscheidung sollte grundsätzlich immer durch den Vorstand bzw. die Geschäftsführung getroffen werden, es sei denn, dass es sich um sehr geringfügige Risiken handelt.

2.3.3.1 Bewertung und Auswahl der Maßnahmen zur Risikobehandlung/Risikobewältigung

Federführend bei der Identifikation angemessener Maßnahmen sollte die hierfür zuständige Fachabteilung im Zusammenspiel mit den Anwendungsverantwortlichen sein. Vor Umsetzung der Maßnahmen sollten diese auf ihre Wirksamkeit und ihre Wirtschaftlichkeit überprüft und bewertet werden.

Ein wesentlicher Faktor hierbei sind die Umsetzungskosten sowie eventuell hieraus resultierende Restrisiken bzw. Sekundärrisiken. Diese sollten je nach Risikoappetit bzw. Wirtschaftsleistung des betreffenden Unternehmens individuell bewertet werden.

Die Maßnahmen unterscheiden sich hinsichtlich der damit verbundenen Umsetzungskosten (extern wie intern), aber auch im Wirkungsgrad. Daher sollten, bevor eine Entscheidung zur Auswahl getroffen wird, die Maßnahmen anhand ihrer Fähigkeit zur Reduktion der identifizierten IT-Risiken und nach den zu erwartenden Kosten klassifiziert werden.

Hierbei könnte beispielsweise das in Tabelle 2–2 beschriebene Klassifikationsschema angewendet werden.

Die Klassifikation der Maßnahmen kann daraufhin in einer Maßnahmenmatrix (siehe Abb. 2–8) dargestellt werden.

Neben einer Einschätzung der Wirtschaftlichkeit einer Maßnahme kann die Klassifikation darüber hinaus auch zur Priorisierung (s.o.) eingesetzt werden. Maßnahmen mit geringen Kosten, die eine hohe Reduktion der identifizierten IT-Risiken bewirken (grüner Bereich der Matrix), sollten zuerst umgesetzt werden.

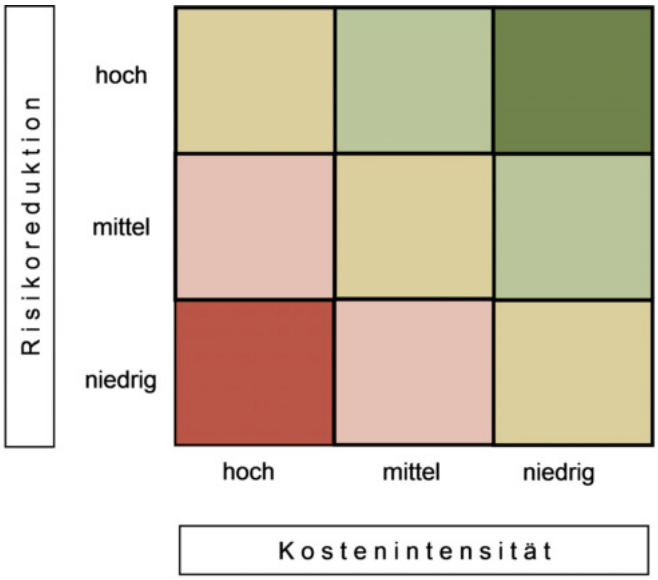


Abb. 2–8 *Maßnahmenmatrix*

Auf Grundlage der Bewertung und Priorisierung der zu treffenden Maßnahmen kann dann ein Maßnahmenplan (Risikobehandlungsplan) erstellt werden, der den zeitlichen Ablauf der Implementierung der Maßnahmen dem Verantwortlichen vorgibt und dessen Einhaltung und Kontrolle im Verantwortungsbereich des IT-Risikomanagements in der Abstimmung mit dem IT-Verantwortlichen liegt.

2.3.3.2 Sekundärrisiken

Ein Effekt, der mit der Ergreifung von Maßnahmen einhergehen kann, ist das sogenannte Sekundärrisiko. Ein plastisches Beispiel ist der Löscheinsatz der Feuerwehr, der ein Ausbreiten eines Brandes (Primärrisiko) in einem Rechenzentrum erfolgreich verhindert, aber durch den Einsatz der Löschmittel (Wasser, Schaum, Pulver) die Hardware nachhaltig schädigen kann (siehe Abb. 2–9 und ISO 31000, Abschnitt 5.5.2).

Klasse	Risikoreduktion	Kostenintensität
niedrig	Die Maßnahme trägt nur unwesentlich zur Reduktion des IT-Risikos bei einem oder mehreren Risikoszenarien bei.	Die Kosten und der Aufwand zur Umsetzung und für den Betrieb der Maßnahme sind zu vernachlässigen.
mittel	Die Maßnahme trägt zur Reduktion des IT-Risikos bei einem oder mehreren Risikoszenarien bei.	Die Kosten für Umsetzung und Betrieb der Maßnahme liegen unter xxxx € bzw. der Aufwand liegt unter xx PT.
hoch	Die Maßnahme ist signifikant für eine wesentliche Reduktion des IT-Risikos bei einem oder mehreren Risikoszenarien verantwortlich.	Die Kosten für Umsetzung und Betrieb der Maßnahme liegen über xxxxx € bzw. der Aufwand liegt über xx PT.

Tab. 2–2 *Klassifikationsschema für Maßnahmen zur Risikobehandlung*

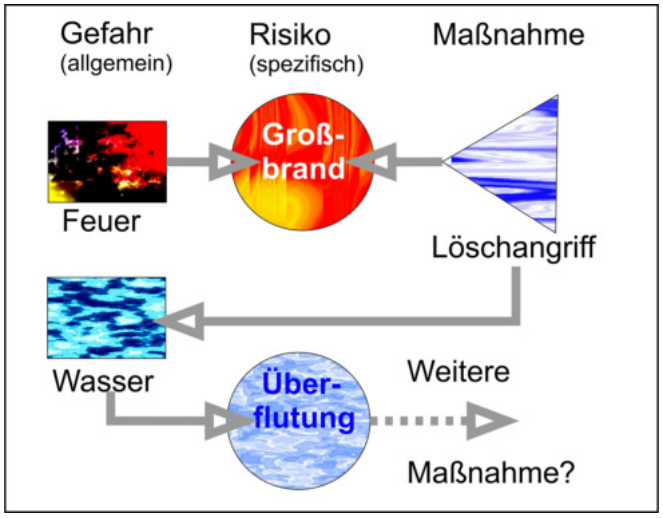


Abb. 2–9 *Sekundärrisiko durch Einsatz von Löschmittel*

2.3.4 Risikobehandlungsplan

Die Dokumentation der ausgewählten und umzusetzenden Maßnahmen sollte in Form eines Risikobehandlungsplans erfolgen. Dieser sollte folgende Informationen enthalten:

- Gründe für Festlegung der Maßnahmen, einschließlich der damit verbundenen Risikominimierung/Verbesserung
- Klare Verantwortlichkeiten für die Freigabe und Umsetzung des Plans
- Empfohlene Aktivitäten
- Benötigte Ressourcen (monetär und personell), auch für Ungeplantes
- Umsetzungsgrad der Maßnahmen und Einschränkungen
- Angemessenes Reporting und Monitoring
- Zeitplan mit entsprechenden Aktivitäten

Risikobewältigungspläne sollten in die relevanten Entscheidungsprozesse des Unternehmens implementiert werden und mit den betreffenden Stakeholdern (interessierten Parteien) abgestimmt werden.

Nachdem für alle Risiken beschlossen wurde, wie sie zu behandeln sind, und ggf. einige Maßnahmen direkt umgesetzt wurden, verbleiben als Resultat einige Risiken, die sogenannten Restrisiken. Über das Vorhandensein und den Umgang mit verbleibenden Restrisiken nach einer Risikobewältigung sollten sich alle Entscheidungsträger und andere Interessengruppen bewusst sein.

Das Restrisiko sollte im Rahmen eines Risikoakzeptanzprozesses dokumentiert, einem Monitoring bzw. einer regelmäßigen Überprüfung und falls erforderlich einer weiteren Risikobewältigung unterzogen werden. Es empfiehlt sich in der Praxis, die Restrisiken der Kategorie »bedeutendes Risiko« oder von höher eingestuften Kategorien in einem Dokument (Restrisikoanalyse) zusammenzufassen und das verbleibende IT-Risiko nach Umsetzung der Maßnahmen und deren Wirksamkeit gegenüber dem Management und Fachbereich darzustellen.

Da das Restrisiko immer auf Basis aller für den Untersuchungsgegenstand ausgewählten Maßnahmen bestimmt wird, ist es wichtig, dass die definierten Maßnahmen auch vollständig umgesetzt werden.

2.3.5 Überwachung

Zu einem effektiven Risikomanagement gehört der Prozess der Überwachung (Monitoring). Im IT-Umfeld ändern sich die Gegebenheiten, die Einfluss auf die Risikolage haben können, meist schneller als im übrigen geschäftlichen Kontext. Daher muss die Risikoüberwachung besonders zeitnah und effektiv sein.

Durch das Monitoring sollte festgestellt werden, ob die ergriffenen Maßnahmen sowohl von ihrem Prinzip (Design, Aufbau) als auch von ihrer tatsächlichen Wirksamkeit (Operational Effectiveness) zufriedenstellend sind. In der Praxis können hierzu Walkthrough Audits und Testing (Checklisten, Interview & Einsichtnahme in Maßnahmendurchführung, Ergebnismanagement/Deficiencies etc.) dienen. Für einige Überwachungsmaßnahmen im IT-Umfeld, wie z.B. Malware-Schutz und Abwehr von Hackingversuchen, ist die Wirksamkeit nur schwer anhand ausbleibender Vorfälle zu bewerten.

Das Monitoring sollte weiterhin Anhaltspunkte zur Verbesserung der Risikobewertung liefern. Hierzu können beispielsweise Statistiken wie Helpdesk-Zahlen, Change-Anforderungen oder Einhaltung der Service Level dienen.

Aus Vorfällen und risikorelevanten Ereignissen kann im Rahmen des Überwachungsprozesses gelernt werden; dabei sind insbesondere die »Beinahe-Vorfälle« von Bedeutung. Diese können z.B. am Außenperimeter abgewehrte Attacken (Hacking, Malware, Distributed Denial of Service (DDoS)) sein, aus denen man Erfahrungen für spätere, verbesserte Angriffe ableiten kann.

In diesem Zusammenhang sollten auch Änderungen in den Rahmenbedingungen bemerkt werden, einschließlich Änderungen der Risikokriterien und der Risiken selbst. Daraus kann eine Umorientierung bei der Risikobehandlung und der Prioritäten resultieren. Änderungen

von Gesetzen, z.B. Datenschutzvorschriften, können u.U. eine stärkere Beachtung der IT-Compliance-Risiken bewirken.

Letztendlich sollten auch anwachsende Risiken im Überwachungsprozess auffallen. Schleichende IT-Risiken, wie z.B. das Überaltern der Hardware-/Softwarekomponenten – z.B. aus falsch verstandener Sparsamkeit –, fallen im Tagesalltag weniger auf. Daher ist der Überwachungsprozess des IT-Risikomanagements eine Chance, diese Risiken einer Beobachtung und (Neu-)Bewertung zu unterziehen.

2.4 Attribute

Der Anhang A der ISO 31000 beschreibt 5 Attribute, die ein gut entwickeltes Risikomanagement aufweisen sollte:

- *Kontinuierliche Verbesserung (Continual improvement)*
  Der kontinuierliche Verbesserungsprozess (KVP) ist ein wesentliches Element aller Managementsysteme, die von der ISO-Organisation betreut werden, und hat auch schon in nationale Normwerke (BSI, DIN) Eingang gefunden. Auch die ISO 27001 hat den KVP zum Bestandteil, ist aber keine Risikomanagementnorm und bezieht sich auch ausdrücklich nicht nur auf die IT, sondern ist ganz dem Thema »Informationssicherheit« gewidmet. Der KVP des IT-Risikomanagements muss daher alle Risikoaspekte – z.B. auch Compliance und Efficiency – abdecken und den Risikoprozess in den Vordergrund stellen.
- *Komplette Verantwortlichkeit für Risiken (Full accountability for risks)*
  Die Ursprünge der gesetzlichen Regelung zum Risikomanagement des Kontroll- und Transparenzgesetzes (KonTraG) lagen in der Erkenntnis, dass Vorstände und Geschäftsleitungen die Verantwortung für Unternehmensinsolvenzen von sich wiesen, mit dem Argument, dass ihnen die zugrunde liegenden Risiken nicht bekannt gewesen seien. Mit Einführung des KonTraG wurden die Vorstände verpflichtet, ein System zu schaffen, das sie über Risiken rechtzeitig informiert. Dies schließt grundsätzlich auch IT-Risiken ein, insbesondere, wenn vom Einfluss der IT die Fähigkeit zur weiteren Fortführung der Geschäftstätigkeit wesentlich abhängt.
- *Anwendung des Risikomanagements in allen Entscheidungssituationen (Application of risk management in all decision making)*
  Praktisch jede unternehmerische Entscheidung kennt einen Ergebnisraum mit Chancen und Risiken. Im Bereich der IT kann das z.B. hohe Investitionen in neue Techniken bedeuten, deren Nachhaltigkeit oft nur schwer zu beurteilen ist. Daher ist die Anwendung eines guten Risikomanagements unter Umständen eine Überlebensfrage. Dies bedeutet, Werkzeuge, Einschätzungen und Analysen zielführend im Entscheidungsprozess einzusetzen.
- *Kontinuierliche Kommunikation (Continual communications)*
  Unternehmensweites Risikomanagement als Querschnittsprozess verlangt einen Kommunikationsprozess, der alle Unternehmensbereiche gleichmäßig umfasst, und nicht zulässt, dass sich »blinde Flecken« bilden, bei denen keine Kommunikation über einen längeren Zeitraum stattfindet. Die IT eines Unternehmens ist in dieser Hinsicht durchaus gefährdet, da hier viel Kommunikation auf technischem Wege erfolgt und unter Umständen weniger über schriftliche oder verbale Kanäle läuft.
- *Vollständige Integration in die Leitungs- und Überwachungsstruktur (Full integration in the organization's governance structure)*[6]
  Die IT wird in immer stärkerem Maße von Spezialisten geprägt, die bestimmte Teilgebiete beherrschen und zu denen nur eine relativ kleine Anzahl Kollegen fachlichen Zugang hat. Das kann dazu führen, dass sich in Bereichen, die sich aufgrund ihrer fachlichen Spezialisierung der regulären Leitung und Überwachung entziehen, unerkannt Risiken bilden. Das Risikomanagement in der IT muss gerade hier seinen Beitrag leisten, indem es als Werkzeug der Unternehmensführung über alle Ebenen und in allen technischen Bereichen präsent ist. Die vollständige Integration ist insofern in der IT nicht nur Herausforderung, sondern Bestandteil einer guten IT-Governance.

6. Siehe Deutscher Corporate Governance Kodex, Präambel.

3 Methoden: ISO 31010

3.1 Vorgehensweise

Die ISO 31010 (Zitat) »*provides guidance on selection and application of systematic techniques for risk assessment*«.

Sie ist also als unterstützende Richtlinie für die Risikobeurteilung anzusehen. Daher enthält sie einen prozessbeschreibenden Teil, der an die ISO 31000 anschließt, sowie einen sehr großen Teil (Appendix B) mit der Beschreibung mannigfaltiger Techniken zur Risikobeurteilung.

Im Folgenden wird zunächst kurz auf die weiteren allgemeinen Ausführungen zur Risikobeurteilung in der ISO 31010 eingegangen, um dann anschließend eine Auswahl von speziellen Techniken zu diskutieren.

3.1.1 Konzepte der Risikobeurteilung

Dieser Abschnitt spiegelt die entsprechenden Einzelabschnitte der ISO 31000 wider. Der Aufbau orientiert sich an den wesentlichen Elementen der ISO 31000:

- Zweck und Nutzen
- Risikobeurteilung und Risikomanagementsystem/ -rahmenwerk
- Risikobeurteilung und Risikomanagementprozess

3.1.2 Prozess der Risikobeurteilung

Auch dieser Abschnitt gibt exakt die Gliederung der ISO 31000 wieder, zeigt aber schon die Bezüge zu einzelnen Techniken auf. Beispielhaft werden bestimmte Methoden genannt, um den Charakter des einzelnen Prozessschrittes und die dafür geeignete Methode darzustellen. Die Schritte sind im Einzelnen:

- Überblick
- Risikoidentifikation
- Risikoanalyse
- Risikobewertung
- Dokumentation
- Überwachung und Nachschau zur Risikobeurteilung
- Anwendung der Risikobeurteilung während des Lebenszyklus

3.1.3 Auswahl der Techniken zur Risikobeurteilung

Die Auswahl geeigneter Techniken sollte sich an folgenden Maßstäben orientieren:

- Die Auswahl muss nachvollziehbar und der Situation bzw. der Organisation angemessen sein. Für das IT-Risikomanagement sind also nur solche Techniken anzuwenden, die sich auf klassische Parameter der IT wie Verfügbarkeit, Vertraulichkeit, Integrität (IT-Sicherheit) oder auch Verbindlichkeit, Effizienz und Effektivität (IT-Wirtschaftlichkeit) sowie Urheberrecht und Datenschutz (IT-Compliance) beziehen lassen.
- Das Ergebnis der Auswahl sollten eine oder mehrere Techniken sein, die das Verständnis der Natur des Risikos fördern und Wege zur Risikobewältigung aufzeigen.
- Die ausgewählte(n) Technik(en) selbst sollte(n) ebenfalls die Fähigkeit besitzen, nachvollziehbar, wiederholbar und beweisbar zu sein.

Die Verfügbarkeit der Ressourcen spielt dabei eine wichtige Rolle. Budgetmittel einerseits sowie die Erfahrung und die Kenntnisse der beteiligten Personen andererseits können die Auswahl der Methoden begrenzen. In der IT sind im besten Fall, wie in anderen Unternehmensbereichen auch, unterschiedliche Fähigkeiten zu Kreativität, Planungs- und Organisationstalent und systematischem Prozessdenken vorhanden. Diese Stärken sollten bestmöglich durch den Verantwortlichen für das IT-Risikomanagement genutzt werden.

Die Risikobeurteilung ist bestimmt durch den Grad der Unsicherheit, der dem zu beurteilenden Risikoportefeuille zugrunde liegt. In der IT können z.B. zukünftige Entwicklungstrends mit einem hohen Maß an Unsicherheit verbunden sein, da außer den technischen Gegebenheiten auch die Markteinflüsse die weitere Entwicklung beeinflussen. Es ist in diesem Zusammenhang wichtig, die interessierten Kreise (Stakeholder) angemessen und transparent über diese Unsicherheitsfaktoren zu informieren.

Bei der Auswahl der Techniken zur Beurteilung von Risiken ist sowohl die Komplexität des Risikos selbst als auch die Komplexität der Methodik zu bedenken. Es ist nicht sinnvoll, klar strukturierte Risikozusammenhänge einer aufwendigen, weil komplexen Analyse zu unterwerfen. In der IT können allerdings eher häufig kom-

plexe Risiken vorkommen, sodass die Überlegung, ein komplexes Verfahren einzusetzen, seine Berechtigung haben kann. Dies erfordert Disziplin und Engagement der Beteiligten, sodass der Verantwortliche für die Analyse die Sinnhaftigkeit eines komplexen Methodenansatzes im Vorfeld sehr gut verdeutlichen sollte.

3.2 Beurteilung der Methoden

Die ISO 31010 gibt über 30 Methoden (= Techniken) an, die man im Risikomanagementprozess als Hilfe heranziehen kann. Im Standard werden diverse Methoden einzeln beschrieben und ihre Eignung bewertet. An dieser Stelle soll die Bewertung des Standards um ein Votum in Bezug auf die IT-Eignung ergänzt werden. Hierauf bezieht sich auch der folgende kurze verbale Teil.

Legende:

- ☑ gut geeignet gemäß ISO 31010
- ☑ ☑ sehr gut geeignet gemäß ISO 31010
- ☒ nicht geeignet gemäß ISO 31000
- 💻 für die IT geeignet (Wertung der Autoren)
- 💻 💻 für die IT gut geeignet (Wertung der Autoren)

3.2.1 Brainstorming

Risikoidentifikation	☑☑
Risikoanalyse	☒
Risikobewertung	☒
IT-Eignung	💻

Brainstorming ist eine bewährte Kreativitätstechnik, die auch in der IT Anwendung findet, insbesondere in IT-Projekten und in der IT-Entwicklung. Im Bereich der Risikoidentifikation für IT-Sicherheitsrisiken ist sie nur bedingt geeignet, da hier gut Gefahrenlisten verschiedener Art eingesetzt werden können.

3.2.2 Strukturierte Interviews

Risikoidentifikation	☑ ☑
Risikoanalyse	☒
Risikobewertung	☒
IT-Eignung	💻

Hier gilt Ähnliches wie für das Brainstorming. Strukturierte Interviews bieten allerdings die Möglichkeit, die Risikoerfahrung von IT-Spezialisten aufzunehmen.

3.2.3 Delphi

Risikoidentifikation	☑ ☑
Risikoanalyse	☒
Risikobewertung	☒
IT-Eignung	💻

Die Delphi-Technik ist ebenfalls eine Kreativitätstechnik, die auf eine Expertenrunde setzt. Sie ist für die Risikoidentifikation durch IT-Fachleute durchaus geeignet, es ist jedoch darauf zu achten, dass technisches Spezialistenwissen nicht über den eigentlichen Risikoprozess dominiert.

3.2.4 Checklisten

Risikoidentifikation	☑ ☑
Risikoanalyse	☒
Risikobewertung	☒
IT-Eignung	💻 💻

Checklisten sind durch Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik und andere Einrichtungen sehr gut unterstützt. Sie können gerade im IT-Bereich ein probates Mittel sein, um systematisch an IT-Risiken heranzugehen und am Anfang einen Grundstock zu schaffen, der durch die individuelle Analyse ausgefüllt wird.

3.2.5 Vorschaden (PHA, Preliminary Hazard Analysis)

Risikoidentifikation	☑ ☑
Risikoanalyse	☒
Risikobewertung	☒
IT-Eignung	💻 -☒

Die Risikoanalyse auf Basis bisheriger Schadenserfahrungen hat den Charme, dass bekannte Zusammenhänge verwendet werden können. Die Gefahr bei der Anwendung, insbesondere in der IT, besteht darin, dass bei zügiger technologischer Weiterentwicklung bisherige Erfahrungen ohne kritische Überprüfung für zukünftige Szenarien adaptiert werden. Daher ist diese Risikoanalysetechnik nur bedingt und nur bei sorgfältiger Einschätzung der Qualität und Übertragbarkeit von bekannten Ereignissen nutzbar.

3.2.6 HAZOP (HAZard and OPerability study)

Risikoidentifikation	☑ ☑
Risikoanalyse	☑ -☑ ☑
Risikobewertung	☒
IT-Eignung	💻 💻

HAZOP ist eine strukturierte Analysemethode, die Abweichungen vom Erwarteten und Auswirkungen anhand von festgelegten Leitworten untersucht. Sie findet in der Softwareentwicklung Anwendung und wird dort auch CHAZOP (Computer HAZard and OPerability study) genannt. Eine umfassende HAZOP-Analyse erfordert die Mitwirkung von IT-Spezialisten und ist verhältnismäßig aufwendig.

3.2.7 HACCP (Hazard Analysis and Critical Control Points)

Risikoidentifikation	☑ ☑
Risikoanalyse	☒ -☑ ☑
Risikobewertung	☑ ☑
IT-Eignung	💻

Die HACCP-Methode entstammt der Lebensmittelindustrie und wird dort auch heute noch regelmäßig und mit gesetzlicher Verankerung durchgeführt. Der Grundgedanke des Verfahrens, den Prozess nicht durch eine Endkontrolle und folgende Maßnahmen abzusichern, sondern innerhalb des laufenden Prozesses kritische Punkte zu identifizieren, an denen gezielte Kontrollen bzw. Maßnahmen greifen, ist auch auf IT-Verhältnisse übertragbar. Testszenarien in der Softwareentwicklung für komplexe Systeme kommen dem nahe.

3.2.8 Toxicity Assessment

Risikoidentifikation	☑ ☑
Risikoanalyse	☒ -☑ ☑
Risikobewertung	☑ ☑
IT-Eignung	☒

Diese Technik ist für Umweltrisiken gedacht und für IT-Systeme und -Prozesse ungeeignet.

3.2.9 SWIFT (Structured »What-if« Technique)

Risikoidentifikation	☑ ☑
Risikoanalyse	☑ ☑
Risikobewertung	☑ ☑
IT-Eignung	💻

Diese Technik setzt auf bewusst aufgeworfene offene Fragen, mit denen Überlegungen zu bestimmten Szenarien angestoßen und aufgearbeitet werden. Sie hat Ähnlichkeit zur HAZOP-Methode. Sehr stark kommt es auf den Moderator an, der für eine intensive Vorbereitung Sorge tragen muss, um zu Beginn der SWIFT-Sitzungen den Kreativprozess in Gang zu bringen. Von den Teammitgliedern wird ein relativ hoher Kenntnisstand gefordert, um Risikosituationen richtig im Detail bewerten zu können. Im laufenden Verfahren muss der Moderator eine klare Struktur in der Diskussion pflegen, um kein Abschweifen zuzulassen. Daher ist die Methode grundsätzlich in der IT anwendbar, muss aber anspruchsvolle Unterstützung bei Moderator und Team finden.[7]

3.2.10 Szenario-Analyse

Risikoidentifikation	☑ ☑
Risikoanalyse	☑ -☑ ☑
Risikobewertung	☑
IT-Eignung	💻

Die Szenario-Analyse ist eine sehr variable Methode ohne feste Strukturvorgaben. Bestimmte Szenarien werden beschrieben und in Bezug auf eine Worst-Case/Best-Case-Entwicklung hin diskutiert. In der bewusst nicht festgelegten Ausführung dieser Technik liegt die Stärke der breiten und flexiblen Anwendbarkeit. Ein Nachteil – dies ist insbesondere bei der IT-Anwendung zu berücksichtigen – ist die Möglichkeit, völlig unzutreffende Szenarien zu konstruieren, deren Fortentwicklung an den falschen Stellen Aufwand verursacht, während andere relevante Risikosituationen zu wenig beachtet werden. Die Fehlbeurteilung von kommenden IT-Trends kann solche Situationen provozieren.

3.2.11 BIA (Business Impact Analysis)

Risikoidentifikation	☑
Risikoanalyse	☑ -☑ ☑
Risikobewertung	☑
IT-Eignung	💻

Die BIA ist eine anerkannte Methode der Notfallplanung bzw. des Business Continuity Management und in diesem Kontext hervorragend einzusetzen. Für technisch orientierte Risikoanalysen ohne starke Bindung an Geschäftsprozesse ist sie aber nicht immer brauchbar.

3.2.12 RCA (Root Cause Analysis)

Risikoidentifikation	☒
Risikoanalyse	☑ ☑
Risikobewertung	☑ ☑
IT-Eignung	💻

Diese Methode geht davon aus, dass die effektivste Technik der Risikobewältigung sich mit den tatsächlichen

7. Siehe auch: *http://easa.europa.eu/essi/ecast/wp-content/uploads/2011/08/ECASTSMSWG-GuidanceonHazardIdentification1.pdf*.

Ursachen von Schadensereignissen beschäftigen muss, anstatt die Symptome zu korrigieren. Voraussetzung dafür ist die möglichst präzise Kenntnis realer Schadensereignisse, einschließlich der Möglichkeit, diese tiefgehend zu ergründen. In der IT wären hier die forensischen Experten gefragt, die möglichst systemnahe Aufzeichnungen analysieren, um damit einem schadenverursachenden Incident auf die Spur zu kommen und für die Zukunft entsprechende Sicherheitsroutinen zu installieren. Hier sind auch die Grenzen erkennbar: Weder liegen in allen Fällen verwertbare Aufzeichnungen vor, noch ist die Analyse angesichts schnell wechselnder Randbedingungen längere Zeit für effektive Risikobewältigungsmaßnahmen nutzbar.

3.2.13 FMEA (Failure Mode Effect Analysis)

Risikoidentifikation	☑ ☑
Risikoanalyse	☑ ☑
Risikobewertung	☑ ☑
IT-Eignung	💻

Die FMEA-Methode – ins Deutsche gerne mit **F**ehler-**M**öglichkeits- und **E**influss-**A**nalyse übersetzt – ist eine bekannte und sehr häufig genutzte Technik an der Schnittstelle zwischen Risiko- und Qualitätsmanagement. Sie wird flächendeckend in der Automobilindustrie eingesetzt und ist daher in den Branchenstandards ausführlich dargelegt.[8]

In der IT ist sie noch relativ wenig im Einsatz, kann aber grundsätzlich, insbesondere bei der Bewertung von Prozessketten, gute Dienste leisten.

3.2.14 Fehlerbaumanalyse (FTA)

Risikoidentifikation	☑
Risikoanalyse	☒ -☑ ☑
Risikobewertung	☑
IT-Eignung	💻 💻

Die Fehlerbaumanalyse ist eine Top-down-Technik, die auch im Qualitätsmanagement verwendet wird. Für die IT eignet sich dieser Ansatz insofern gut, als dass oft komplexe Fehlersituationen vorliegen, die ein erhebliches Risiko für die Aufgabenerfüllung der IT darstellen. Daraufhin muss der betroffene Prozess erfahrungsgemäß von der erkennbaren Fehlersituation bis zu den möglichen Detailursachen durchgearbeitet werden.

8. Siehe VDA QMC, Band 4, Kapitel: Produkt- und Prozess-FMEA.

3.2.15 Ereignisbaumanalyse (ETA)

Risikoidentifikation	☑
Risikoanalyse	☑ -☑ ☑
Risikobewertung	☒
IT-Eignung	💻 💻

Die Ereignisbaumanalyse geht von einem bekannten Ereignis aus, das auf grafischem Wege – Baumstruktur – in risikorelevante Teilaspekte aufgegliedert wird. Dabei können den einzelnen Ästen der Baumstruktur auch Wahrscheinlichkeitswerte mitgegeben werden, sodass ein differenziertes Bild über die Ausprägungen eines Schadenereignisses entsteht. ETA kann für IT-Ereignisse gut verwendet werden. Abhängigkeiten und Wechselwirkungen sind allerdings so nicht darstellbar.

3.2.16 Ursache-Folge-Analyse

Risikoidentifikation	☑ ☑
Risikoanalyse	☒ -☑ ☑
Risikobewertung	☑
IT-Eignung	💻

Diese Methode kombiniert ETA mit FTA und stellt damit grundsätzlich ein mächtiges Werkzeug zur Analyse dar. Gegebenenfalls problematisch ist die Komplexität in der Handhabung. Dies kann in der IT den Einsatz erschweren, wenn die Struktur des dem Risiko zugrunde liegenden IT-Verfahrens oder -Projektes schon in sich komplex ist.

3.2.17 Ursache-Wirkungs-Analyse

Risikoidentifikation	☑ ☑
Risikoanalyse	☑ ☑
Risikobewertung	☒
IT-Eignung	💻

Die Ursache-Wirkungs-Analyse verwendet strukturierende grafische Techniken, um den Ursachen von Risiken auf die Spur zu kommen. Eine der bekanntesten Darstellungsformen ist das Ishikawa-Diagramm (»Fischgräte«). Diese Techniken sind für IT-Belange geeignet.

3.2.18 Schutzschichten-Analyse (LOPA)

Risikoidentifikation	☑
Risikoanalyse	☑ -☑ ☑
Risikobewertung	☒
IT-Eignung	💻 💻

LOPA (Layer of Protection Analysis) ist eine (semi-) quantitative Analyse zur Bewertung von Risiken mit prozessorientiertem Ansatz. Dabei wird eine Betrachtung von innen nach außen aufgesetzt, die meist mit dem Design des betroffenen Prozesses beginnt, danach folgt die Bewertung von Basismaßnahmen und anschließend von Maßnahmen bei kritischen Situationen (z.B. Alarme, Eskalationswege). Auf diese Weise werden weitere Schutzschichten bewertet. LOPA findet z.B. in der Luftsicherheit Anwendung. In der IT ist diese Methode im Einzelfall sehr gut anwendbar, z.B. bei der Beschreibung von Peripherie-Risiken oder beim kaskadierenden Malware-Schutz.

3.2.19 Entscheidungsbaum (Decision Tree)

Risikoidentifikation ☒
Risikoanalyse ☑ ☑
Risikobewertung ☑
IT-Eignung 💻 💻

Die Entscheidungsbaumanalyse ähnelt stark der Ereignisbaumtechnik, bezieht sich jedoch auf verschiedene Entscheidungsalternativen, bei denen Unsicherheitsfaktoren zugrunde liegen.

3.2.20 HRA (Human Reliability Analysis)

Risikoidentifikation ☑ ☑
Risikoanalyse ☑ ☑
Risikobewertung ☑ ☑
IT-Eignung 💻

Diese Analysemethode setzt sich mit dem »Faktor Mensch« auseinander. Kernstück der Analyse ist eine Einschätzung der menschlichen Fehlhandlungen, die zu Schadenereignissen führen können. Diese Technik ist insbesondere bei fehlertoleranten Systemen und im Bereich der IT-Sicherheit in Zusammenhang mit Social-Engineering-Angriffen verwendbar.

3.2.21 Bow Tie Analysis

Risikoidentifikation ☒
Risikoanalyse ☑ ☑
Risikobewertung ☑
IT-Eignung 💻

Der Name dieser grafischen Methodik leitet sich von der Grundform der Analysegrafik ab. Das Risiko wird in der Mitte platziert (»Knoten«), während der linke »Flügel« die Bedrohungen/Gefährdungen untereinander stellt. Auf der rechten Seite werden dann die Konsequenzen des Risikos untereinander aufgereiht, sodass eine gewisse Symetrie entsteht. Präventive und korrektive Maßnahmen auf beiden Seiten des Knotens komplettieren das Bild. Das Verfahren ist einfach anzuwenden, aber nicht sehr ausgefeilt, um Ursache-Wirkungs-Mechanismen zu verdeutlichen.

3.2.22 Zuverlässigkeitsorientierte Instandhaltung (RCM)

Risikoidentifikation ☑ ☑
Risikoanalyse ☑ ☑
Risikobewertung ☑ ☑
IT-Eignung 💻

RCM (Reliability Centered Maintenance) ist eine aus der industriellen Fertigung bekannte Methode, bei der besonderer Wert auf die Nachhaltigkeit der Wartungsmaßnahmen gelegt wird. Der Grundgedanke ist auch auf die IT übertragbar, insbesondere dann, wenn der IT-Betrieb oder die IT-Anwendung in Zusammenhang mit Prozessen steht, die Sicherheit und Gesundheit betreffen.

3.2.23 SCA (Sneak Circuit Analysis)

Risikoidentifikation ☑
Risikoanalyse ☒
Risikobewertung ☒
IT-Eignung 💻

Die Sneak-Circuit-Analyse ist eine auf das Auffinden und Bewerten von unerwarteten Zuständen gerichtete Methode. Dabei werden insbesondere solche überraschenden Ereignisse analysiert, die trotz Fehlerfreiheit ihrer einzelnen Komponenten auftreten. Sie wird beispielsweise in der Analyse von Netzwerken angewandt.

3.2.24 Markov-Analyse

Risikoidentifikation ☑
Risikoanalyse ☑ ☑ -☒
Risikobewertung ☒
IT-Eignung 💻

Die Markov-Analyse ist eine prozessorientierte Technik, die aufeinander folgende Abläufe in Schritten bewertet. Dabei können die einzelnen Prozessschritte sowohl als unabhängige Abfolge von Prozessabschnitten als auch als verketteter Gesamtprozess mit aufeinander aufbauenden Bewertungen gesehen werden. Die Markov-Analyse ist eine quantitative Methode der Risikoeinschätzung.

3.2.25 Monte-Carlo-Simulation

Risikoidentifikation	☒
Risikoanalyse	☒
Risikobewertung	☑ ☑
IT-Eignung	💻

Die Monte-Carlo-Simulation ist ebenfalls eine quantitative Methode zur Risikoeinschätzung, die als Simulation mit einer großen Menge zufällig ermittelter Ergebniswerte angelegt ist. Der Name leitet sich von den Würfen der Kugel in einem Roulette-Kessel ab, die zufällige Ergebnisse in großer Menge erzeugen.

3.2.26 Bayesian Statistics/Bayes-Netze

Risikoidentifikation	☒
Risikoanalyse	☑ ☑ -☒
Risikobewertung	☑ ☑
IT-Eignung	💻

Bayes-Netze sind statistisch-quantitative Verfahren, die oft grafische Darstellungen zur Verdeutlichung der Zusammenhänge zwischen abhängigen Ereignissen und deren Wahrscheinlichkeit benutzen.

3.2.27 FN-Kurven

Risikoidentifikation	☑
Risikoanalyse	☑ ☑
Risikobewertung	☑ ☑
IT-Eignung	💻

Diese Methode stellt Risikoeinschätzungen nicht als punktuelle Werte, sondern als Verlaufskurven dar. Dadurch ist sie besonders gut für den Vergleich von Risiken geeignet.

3.2.28 Risk Indices

Risikoidentifikation	☑
Risikoanalyse	☑ ☑
Risikobewertung	☑ ☑
IT-Eignung	💻 💻

Die Verwendung von Risikoindikatoren ist eine oft angewandte Methode, um verschiedene qualitative Einschätzungen zu kombinieren und damit IT-Risiken vergleichbar zu machen. Sie ist im IT-Risikomanagement sehr gut anwendbar, bedingt aber, dass die Daten, die als Basis der Einschätzung herangezogen werden, stichhaltig sind.

3.2.29 Wahrscheinlichkeits- und Auswirkungsmatrix (Consequence/Probability Matrix)

Risikoidentifikation	☑ ☑
Risikoanalyse	☑ ☑
Risikobewertung	☑
IT-Eignung	💻 💻

Diese Methodik kombiniert quantitative mit qualitativen Faktoren in Form einer Matrix. Wichtig hierbei ist die vorherige, einheitliche Definition der Wertstufen dieser Matrix. Dadurch wird die Vergleichbarkeit der Einschätzungen sichergestellt. Aus der Anordnung in der Matrix lassen sich sehr gut Prioritäten zur Risikobewältigung ableiten. Für das IT-Risikomanagement ist diese Methode uneingeschränkt zu empfehlen.

3.2.30 Kosten-Nutzen-Analyse (Cost/Benefit Analysis)

Risikoidentifikation	☑
Risikoanalyse	☑ ☑
Risikobewertung	☑
IT-Eignung	💻

Die Kosten-Nutzen-Analyse ist eine bekannte Methode, die auch bei Projekten und Investitionen benutzt wird. Sie ist auch im IT-Risikomanagement einsetzbar. Als schwierig erweist sich dabei meist eine vertretbare Nutzenschätzung, insbesondere wenn Reputationsrisiken mit zu beurteilen sind.

3.2.31 Multiple Criteria Decision Analysis (MCDA)

Risikoidentifikation	☑
Risikoanalyse	☑ ☑
Risikobewertung	☑
IT-Eignung	💻

Die MCDA – Multiple Criteria Decision Analysis – versucht, die Situation aufzufangen, in der mehrere und meist miteinander konkurrierende bzw. sich widersprechende Kriterien zur Entscheidungsfindung vorliegen. Die Gewichtung der Kriterien spielt dabei eine wesentliche Rolle. Erfahrungsgemäß resultiert ein Entscheidungsraum, der mögliche Optima als Ergebnis darstellt.

Dieses Verfahren ist grundsätzlich im Umfeld des IT-Risikomanagements anwendbar, u.U. aber relativ aufwendig. Das Resultat mehrerer möglicher Lösungen in einem Entscheidungsraum muss abschließend zur endgültigen Lösung zusammengeführt werden.

4 Implementierung/Anwendung: ISO 31004

Die ISO 31004 ist kein Standard im engeren Sinn, sondern ein sogenannter Technical Report. Als Guidance soll sie den Anwender der ISO 31000 bei der Implementierung unterstützen. Der Geltungsbereich entspricht dem der ISO 31000 und ist wie dieser nicht auf bestimmte Branchen und Rechtsformen beschränkt. Damit steht einer Nutzung im Bereich der IT nichts im Wege.

Die ISO 31004 legt ihren Fokus auf die Implementierung auch dann, wenn bereits Formen des Risikomanagements existieren, die noch weiter verbessert werden sollen. Eine wesentliche Rolle spielt dabei die Integration in die generellen Managementprozesse, auch in die der IT, ohne dass diese explizit erwähnt wären.

Anhang A: Underlying concepts and principles (Zugrunde liegende Konzepte und Grundsätze)

Dieser Anhang bietet vertiefende Erklärungen zu Begriffen wie Risiko, Unternehmensziele, Wahrscheinlichkeit, Unsicherheit, Risikobehandlung und Maßnahmen, Rahmenwerk für Risikomanagement, Risikokriterien sowie eine bewusste Unterscheidung zwischen Risikomanagement und dem »Managen von Risiken«.

Bei der Anwendung der ISO 31000 in der IT kann dieser Anhang hilfreich sein, um eine für alle Beteiligten gleich verstandene Sprache mit einheitlichen Begriffen und Inhalten zu finden.

Anhang B: Application of the principles (Anwendung der Grundsätze)

Wie anhand des Titels zu vermuten, geht dieser Anhang erklärend auf die 11 Grundsätze des Risikomanagements ein. Es werden – wenn auch unspezifisch – Anwendungshinweise für Unternehmen erläutert und die Sinnhaftigkeit der Grundsätze erklärt. Zu einigen Grundsätzen werden abgesetzte Kontrollfragen und Statements (practical help) angeboten. Auch die Rolle (interner) Auditoren wird erwähnt.

Für die Anwendung in der IT ist ein weiterer Transformationsprozess notwendig, um der speziellen Materie gerecht zu werden (siehe Abschnitt 2.1 dieses Leitfadens).

Anhang C: How to express mandate and commitment (Wie Auftrag und Verpflichtung ausgedrückt werden können)

Dieser Anhang ist ähnlich wie Anhang B aufgebaut. Auch hier gibt es einen abgesetzten Teil als *practical help*.

Anhang D: Monitoring and review (Überwachung und Nachschau)

Hier spielen Audits und Auditoren eine wichtige Rolle. Es wird zunächst zwischen *monitoring* (= Überwachung), *review* (= Nachschau) und *audit* (Prüfung) unterschieden. Dazu gehört, dass die Verantwortung für Überwachung und Nachschau bei der Unternehmensleitung angesiedelt und hierin ein Unterschied zum Audit gesehen wird. In der IT ist die Überwachung von Systemen eine ständige Übung und den meisten Mitarbeitern der IT gut bekannt bzw. wird aktiv genutzt. Die Nachschau unter aktiver Beteiligung des IT-Managements ist weniger klar und von der Unternehmenskultur abhängig.

Bei der Audit-Funktion wird die Unabhängigkeit vom operativen Management als entscheidend angesehen. Dies sollte durch die Trennung von IT-Leitung (CIO) und IT-Revision (CEO) gewährleistet sein; es dürfte kaum Fälle geben, in denen die Interne Revision eines Unternehmens an die Leitung der IT angebunden ist.

Der Audit-(Revisions-)Funktion werden 5 Punkte als Prüfziele nahegelegt:

- Übereinstimmung der Risikokriterien und des Risikokontextes mit den betrieblichen Zielen; hier auch im Kontext der Integration der IT-Ziele in die Unternehmensziele
- Qualität und Nachhaltigkeit des Risikomanagementprozesses; in der IT u.U. bei schnell wechselnden Gestaltungsparametern
- Angemessene Risikobehandlung bei nicht tragbaren Risiken; für die IT sind hier die klassischen Werte Verfügbarkeit, Vertraulichkeit und Integrität als Maßstab möglich
- Die Wirksamkeit der Maßnahmen, z.B. die Verhinderung von Malware, Hacking oder Spam
- Fortschritte durch die Anwendung von Risikobehandlungsplänen

Der Hinweis, dass die o.a. Aktivitäten die bestmögliche Informationsgrundlage benötigen, ist nicht überraschend, aber gerade im Umfeld der IT aufgrund ihrer Komplexität und Innovationsgeschwindigkeit herausfordernd. Berichterstattung, Korrekturmaßnahmen und kontinuierliche Verbesserung beschließen den Kreis.

Es folgt eine intensivere Darstellung der Überwachung und Nachschau mit Bezug zum Risikomanagementsystem, in dem auch tabellarisch und mithilfe von Kennzahlenvorschlägen Hinweise zur Nachschau gegeben werden. Es empfiehlt sich, die hier genannten Kenngrößen auf Verwendbarkeit in der IT zu prüfen und ggf. durch eigene Kennzahlen zu ergänzen oder zu ersetzen. Ein hervorgehobener Hinweis, unterstützt durch Beispiele und einen practical help, gilt der Veränderung im Risikokontext. Hier sind für die IT spezielle Kriterien anzuwenden.

Es schließt sich eine detailliertere Darstellung der Überwachung des Risikomanagementprozesses an. Verantwortlichkeit und Erfahrungslernen stehen am Anfang, es folgen Hinweise zur Rolle der Risikoeigner zu Kennzahlen und zur Vorgehensweise.

Abgeschlossen wird dieser relativ umfangreiche Anhang durch Hinweise zur Nachschau.

Anhang E: Integrating risk management within a management system (Integration des Risikomanagements in ein Managementsystem)

ISO 31000 pflegt das Verständnis des Risikomanagements nicht als eigenständiges System, sondern als querschnittlichen Teil anderer Managementsysteme, wie Qualitätsmanagement, Umweltmanagement, Informationssicherheitsmanagement usw. Dieser Anhang gibt Anleitung zu dieser Integration am Beispiel des Qualitätsmanagements nach ISO 9001. Für die IT verlangt dieses Beispiel noch einen Transformationsprozess, da ISO 9001 nicht unbedingt der übliche Standard in der IT ist; Methoden wie CMMI und SPICE sind hier eher bekannt.

5 Vergleich zur ISO/IEC 27005

Die Norm ISO/IEC 27005 *»Information technology – Security techniques – Information security risk management«* – nachfolgend mit ISO/IEC 27005 bezeichnet – wurde erstmalig im Jahr 2008 veröffentlicht. Sie basiert auf dem gleichen Vorgehensmodell (Prozess) und den gleichen Prinzipien wie die ein Jahr später veröffentlichte ISO 31000 *»Risk management – Principles and guidelines«*. Im Vergleich zur ISO 31000 ist die ISO/IEC 27005 eine Spezialisierung zum Thema operationales Risikomanagement in Bezug auf das Management von Informationssicherheitsrisiken.

Die Standards der ISO/IEC-270xx-Serie haben das Management der Informationssicherheit zum Inhalt. Das Risikomanagement wird in der 270xx-Familie als Werkzeug in den Prozessen der Informationssicherheit operationalisiert.

Die ISO/IEC 27001 fordert ein systematisches Informationsrisikomanagement als integralen Bestandteil des Informationssicherheitsmanagementsystems (ISMS). Als Entscheidungsgrundlage für die Risikobehandlung, insbesondere für umzusetzende Sicherheitsmaßnahmen, kommt den Risiken in der Informationsverarbeitung (Informationsrisiko) eine zentrale Rolle zu. Die durch das Risikomanagement ermittelten Informationsrisiken dienen der Unternehmensführung zur Priorisierung von Schutzmaßnahmen für Informationen, Systeme, Netze, Prozeduren etc.

So können Schutzmaßnahmen effizient eingesetzt werden, um gezielt Risiken bei der Verarbeitung und im Umgang mit Informationen zu minimieren. Aus diesem Grund wird in der ISO/IEC 27005 das operationale Risikomanagement speziell auf die Ziele der Informationssicherheit ausgerichtet, nämlich die geforderte Vertraulichkeit, Integrität und Verfügbarkeit von schützenswerten Informationen zu gewährleisten.

Maßnahmen zur Erreichung dieser Sicherheitsziele werden zielgerichtet dort etabliert, wo die Verletzung der Informationssicherheitsziele, und damit mögliche Auswirkungen/Schäden, am größten sind. Die Sicherheit von Informationen gilt als angemessen, wenn die drei vorgenannten Schutzziele in einem ausreichenden Maße erreicht sind und die verbleibenden Restrisiken von der Geschäftsleitung getragen werden, d.h. für die Organisation akzeptabel sind.

Informationsrisikomanagement ist ein kontinuierlicher Prozess, aufgebaut aus den folgenden Schritten:

- Es wird mit der Schaffung eines Kontextes für das Risikomanagement begonnen. Dazu gehört die Festlegung oder Bestätigung der Metrik für die Risikoeinschätzung, Kriterien für die Risikoakzeptanz, Bestimmung der Grenzen des Anwendungsbereiches, Einbeziehung von Geschäftszweck, Unternehmensprinzipien/Unternehmensstrategien und die Identifizierung der relevanten Verantwortlichen aus fachlicher und organisatorischer Sicht.
- Risiken in der Informationsverarbeitung werden identifiziert.
- Risiken werden von den Verantwortlichen für die Informationen bzw. zugehörigen Prozesse in Bezug auf ihre Auswirkungen auf das Geschäft und die Wahrscheinlichkeit des Eintritts eingeschätzt.
- Bedeutsame Risiken (deren Eintrittswahrscheinlichkeit und die Auswirkung) werden je nach Tragweite an die Bereichsleitung oder die Geschäftsleitung verständlich kommuniziert und Handlungsoptionen, inklusive des verbleibenden Restrisikos, nach Umsetzung der jeweiligen Handlungsoption aufgezeigt.
- Auf der Leitungsebene werden die kommunizierten Risiken und die Optionen zur Risikobehandlung bewertet, Risikoeigner benannt und Prioritäten für die Risikobehandlung festgelegt. Optionen für die Risikobehandlung können sein:
  - Vermeidung des risikobehafteten Prozesses
  - Minimierung des Risikos durch Schutzmaßnahmen
  - Verlagerung des Risikos auf andere
  - Akzeptanz des Risikos, sofern es ein akzeptables Risikoniveau hat
- Risikobehandlungen werden unter Einbeziehung der relevanten Interessengruppen geplant und von den Fachabteilungen umgesetzt.
- Es erfolgt eine Nachverfolgung der Maßnahmen zur Risikobehandlung durch den/die Verantwortlichen (Risikomanager, Risikoeigner, Verantwortliche für die Informationen/Prozesse).
- Regelmäßig – sowie nach gravierenden Änderungen und bedeutsamen Sicherheitsvorfällen – werden die Risikosituation, die Wirksamkeit von gegebenenfalls umgesetzten risikominimierenden Maßnahmen, das festgelegte Risikoakzeptanzniveau und der Risikomanagementprozess zur stetigen Hebung von Verbesserungspotenzialen überprüft und bei Bedarf angepasst.
- Führungspersonal und Mitarbeiter werden geschult/sensibilisiert, um Risiken zu erkennen, zu melden und die Risikobehandlung ernst zu nehmen.

Der erste Punkt »Identifikation der Risiken« bedarf einer standardisierten Erhebungsmethode, um Nachvollziehbarkeit und Wiederholbarkeit zu gewährleisten. Unterschiedliche Personen sollen zu gleichen Ergebnissen bei einer Risikoerhebung kommen. Die ISO/IEC 27005 gibt zu den möglichen Erhebungsmethoden keinerlei Hinweise. Hier eignet sich, wie in Abschnitt 3.2 beschrieben, die *»ISO 31010 Risk management – Risk assessment techniques«* mit ausführlichen Beschreibungen zahlreicher, unterschiedlicher Methoden.

Der zweite Punkt, die Einschätzung durch den für die Informationen bzw. zugehörigen Prozesse Verantwortlichen, kann herangezogen werden, um den Unterschied zwischen der speziellen ISO/IEC 27005 und der generischen ISO 31000 zu verdeutlichen. In der ISO-31000-Familie ist erläutert, wie Risiken professionell strukturiert behandelt werden. Es fehlen die spezifischen Beispiele für die verschiedenen Risikoarten und welcher Art die Auswirkungen sein können. Fokussiert auf Informationssicherheitsrisiken werden diese Aspekte in der ISO/IEC 27005 – insbesondere in den Anhängen – detailliert betrachtet. Unterschiedliche Auswirkungen werden aufgelistet (z.B. Störung oder Unterbrechung der Wertschöpfungskette, finanzielle Verluste, Gefahr und/oder Schaden für Leib und Leben, Reputationsschaden). Ausführlich wird in der ISO/IEC 27005 dargelegt, welche Einzelkomponenten betrachtet werden müssen, um ein Risiko in der Informationsverarbeitung abschätzen zu können.

Das Risiko setzt sich aus Bedrohung, Schwachstelle und den möglichen Auswirkungen zusammen, falls eine Bedrohung eine bestehende Schwachstelle ausnutzt. Dazu wird die Eintrittswahrscheinlichkeit für Gefährdungen ermittelt.

Eine Gefährdung resultiert aus der Kombination von

- einer bestehenden Bedrohung, der man ausgesetzt ist und die man nicht beseitigen kann, und
- einer Schwachstelle in den Schutzmaßnahmen der Organisation, die von der bestehenden Bedrohung ausgenutzt werden könnte.

Eine Bedrohung kann ein Hacker, ein Spion, jegliche Form von Schadsoftware (Viren, Würmer, Trojaner etc.), technisches Versagen, Fehlhandlungen, Angriffe oder aber auch höhere Gewalt sein. Keine dieser Bedrohungen würde die Informationen (Schutzobjekt/Wert) in einem perfekt geschützten System gefährden. Erst dadurch, dass das System oder die das System umgebenden Personen, Räumlichkeiten, technischen Schutzmaßnahmen oder organisatorischen Regelungen eine oder mehrere Schwachstellen aufweisen, besteht eine Gefährdung für das Schutzobjekt. Dies wird durch eine Grafik des Bundesamtes für Sicherheit in der Informationstechnik (BSI, *http://www.bsi. bund.de*) verdeutlicht (siehe Abb. 3–1).

Eine Liste von bekannten, typischen Bedrohungen sowie Beispiele für Schwachstellen zur besseren Einschätzung von Gefährdungen und weitere Informationen zum Risikomanagement finden sich in den informativen Anhängen der ISO/IEC 27005. Die Inhalte sind am Ende dieses Kapitels kurz dargestellt.

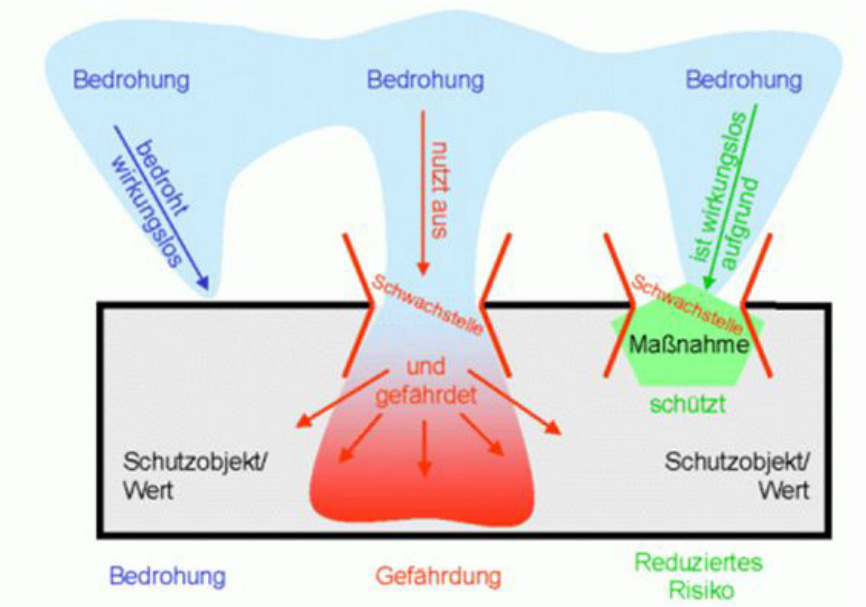


Abb. 5–1 *Bedrohung und Gefährdung eines Schutzobjekts*

Im Vergleich zur ISO 31000 sind die Optionen zur Risikobehandlung bei Informationssicherheitsrisiken reduziert. ISO 31000 definiert Risiko als eine – positive oder negative – Abweichung von dem Erwarteten. In der ISO/IEC 27005 findet sich diese Definition nicht, wohl aber eine Definition für ein Informationssicherheitsrisiko. Ein Informationssicherheitsrisiko wird immer als negative Abweichung verstanden. Sinngemäß lautet die Definition für ein Informationssicherheitsrisiko: Möglichkeit, dass eine existierende Bedrohung eine Schwachstelle ausnutzt und dabei Schaden verursacht.

Daher sind die Optionen zur Risikobehandlung in der ISO/IEC 27005 auch auf die Alternativen beschränkt, die geeignet sind, zu entscheiden, wie mit potenziellen Schäden umgegangen werden kann (Risiko vermeiden/Risiko reduzieren/Risiko übertragen/Risiko dulden).

Nachdem entschieden wurde oder gegebenenfalls noch zu entscheiden ist, wie die identifizierten Risiken behandelt werden, sind involvierte und/oder betroffene Beteiligte zu informieren. Dieser Prozessschritt findet sich in beiden Standards. In der ISO/IEC 27005 wird jedoch auf einige Besonderheiten hingewiesen, die aufgrund der schadenbehafteten Natur der erkannten Risiken besteht. Beispielhaft seien hier Vertraulichkeit (sorgsame Auswahl des Adressatenkreises), Sensibilisierung (Awareness) und Krisenkommunikation genannt.

Ein wichtiges Element des Risikomanagementprozesses ist, den Prozess und alle Prozesselemente, wie die Liste der Bedrohungen, das Risikoakzeptanzniveau, die Schutzobjekte etc., regelmäßig zu überprüfen und bei Bedarf anzupassen. Auch hier unterscheiden sich ISO 31000 und ISO/IEC 27005 nicht wesentlich. Letztere enthält allerdings mehr Hinweise, was überwacht und überprüft werden sollte. Beispielhaft seien hier genannt: gesetzliches und umgebungsbezogenes Umfeld, Wert der Schutzobjekte, Schadenskategorien, Gesamtkosten, notwendige Ressourcen.

In den Anhängen zu ISO/IEC 27005 finden sich wertvolle Hinweise zum Aufbau eines Informationssicherheitsprozesses, über Methoden und Durchführung einer Risikobewertung sowie für die Risikobehandlung.

In Anhang A ist beschrieben, wie der Anwendungsbereich, für den der Informationssicherheitsrisikoprozess gelten soll, definiert und abgegrenzt werden sollte. Berücksichtigt werden sollte z.B. der Geschäftszweck, die Unternehmensstruktur, die grundlegenden Unternehmensprinzipien und -werte sowie die Unternehmensstrategie. Außerdem sollen Rahmenbedingungen und Beschränkungen, denen das Unternehmen unterliegt, berücksichtigt werden. Die Spanne reicht von politischen, wirtschaftlichen, strategischen bis hin zu territorialen Entscheidungen. Weiterhin sollten Marktbedingungen, kulturelle, personelle, finanzielle, zeitliche Rahmenbedingungen und anderes mehr beachtet werden. Zusätzlich natürlich auch noch gesetzliche und technische Vorgaben, bestehende Gegebenheiten, Abläufe und Abhängigkeiten.

Anhang B beschreibt Beispiele und Methoden, wie Schutzobjekte (information assets) klassifiziert und identifiziert werden können. Es folgt eine Auflistung von primären und unterstützenden Schutzobjekten sowie deren unterschiedliche Typen, wie z.B. Prozesse, Information, Hardware, Software, Netzwerk, Personal, Standort und die Organisation.

Der zweite Abschnitt von Anhang B beschreibt, wie der Wert bestimmt/eingestuft werden kann, den die identifizierten Schutzobjekte für das Unternehmen haben. Als wesentliche Komponenten werden aufgeführt: das Festlegen der relevanten Kriterien, die Abstufung und der Grad der Abhängigkeit von anderen Schutzobjekten.

Der letzte Abschnitt gibt Hinweise, wie Auswirkungen auf einen Informationssicher-heitsvorfall kategorisiert und bewertet werden können.

In Anhang C findet sich eine Liste mit Beispielen für typische Bedrohungen. In einer weiteren Tabelle sind Gruppen von möglichen Angreifern, deren Motive für einen Angriff und denkbare Konsequenzen eines entsprechenden Angriffs aufgeführt.

In Anhang D findet sich eine Tabelle mit Beispielen für typische Schwachstellen. Sie sind unterschiedlichen Typen, wie z.B. Hardware, Netzwerk, Personal und einigen der im vorigen Anhang aufgeführten Bedrohungen zugeordnet.

Abschließend werden einige Methoden beschrieben, wie Schwachstellen identifiziert und bewertet werden können. Beispielhaft seien hier Penetrationstest und Codereview genannt.

In Anhang E werden verschiedene Ansätze und Methoden vorgestellt, wie Risiken bewertet und in eine verständliche und nachvollziehbare Skala eingestuft werden können. Die vorgestellten Verfahren reichen von einer ersten Grobanalyse bis hin zu detaillierten, in der Durchführung ggf. aufwendigen Methoden. Die Methoden und Verfahren werden anhand mehrerer Beispiele gut nachvollziehbar beschrieben. Der Nutzer muss jedoch selbst entscheiden, ob sich eines bzw. welches der Verfahren sich für seine Organisation am besten eignet.

In Anhang F wird die Thematik Rahmenbedingungen und Sachzwänge erneut aufgegriffen, diesmal allerdings unter dem Aspekt, dass und wie sie bei der Risikoreduktion zu berücksichtigen sind.

Ergänzung: Bezug zur ISO/IEC27001:2013

Aufgrund der geänderten Bertrachtungs- und Herangehensweise zum Umgang mit Risiken und Chancen in der ISO/IEC 27001:2013 folgt eine Ergänzung.

Ende September 2013 wurde von der Internationalen Organisation für Standardisie-rung (International Organization for Standardization, ISO) eine deutlich überarbeitete Version der ISO/IEC 27001 herausgegeben. Auch wenn hier in diesem Kapitel ein Vergleich zwischen ISO 31000 und ISO/IEC 27005 gezogen wird, soll und darf der Bezug zur ISO/IEC 27001 nicht vernachlässigt werden, denn die Bedeutung von Risikoeinschätzung und -behandlung haben in ISO/IEC 27001:2013 im Vergleich zur 2005er-Version einen deutlich anderen Stellenwert bekommen.

Die Version ISO/IEC 27001:2005 ist nach wie vor gültig und wird vermutlich erst Ende September 2015 zurückgezogen. Für ISO/IEC 27005 gibt es zum Zeitpunkt der Veröffentlichung dieses Leitfadens (Q4/2014) keine überarbeitete Version. Daher haben alle oben dargelegten Vergleiche und Bezüge Bestand.

ISO/IEC 27001:2013 nimmt direkt Bezug zur ISO 31000 und fordert, dass eine Organisation ermitteln muss, welche externen und internen Angelegenheiten für ihren Geschäftszweck relevant sind und sich auf die Ziele ihres Informationssicherheitsmanagementsystems (ISMS) auswirken können (ISO/IEC 27001:2013, Abschnitt 4.1). Weiterhin ist gefordert, dass die Organisation im Hinblick auf das ISMS interessierte Parteien und deren Anforderungen ermittelt (ISO/IEC 27001:2013, Abschnitt 4.2). Diese Angaben fließen u.a. unmittelbar in den Risikomanagementprozess ein. Bei der Planung der Maßnahmen wird nun – anders als in der 2005er-Version – explizit der Umgang mit Risiken und Chancen gefordert. Ziele des Risikoprozesses sind:

- Sicherstellung, dass das ISMS seine beabsichtigten Ergebnisse erreicht
- Verhinderung oder Reduzierung unerwünschter Auswirkungen
- Kontinuierliche Verbesserungen

Um dies erreichen zu können, sollen Maßnahmen zum Umgang mit den erkannten Risiken und Chancen geplant und diese in die ISMS-Prozesse integriert und implementiert werden.

Die Vorgehensweise zur Durchführung der Risikobewertung ist nicht mehr so streng vorgeschrieben wie bisher. Der Prozess zur Einschätzung der Informationssicherheitsrisiken und zur Risikobehandlung besteht im Wesentlichen aus den folgenden Elementen:

- Kriterien zur Durchführung von Risikobewertungen
- Risikoakzeptanzkriterien
- Identifizieren von Risiken
- Analysieren der identifizierten Risiken
- Bewerten der ermittelten Risiken (Vergleich mit den Risikoakzeptanzkriterien)
- Festlegen von Maßnahmen
- Priorisieren und Behandeln der ermittelten Risiken

Anders als in der 2005er-Version ist auch, dass der jeweilige Risikoeigentümer (und nicht das Management) den Plan zur Risikobehandlung genehmigen sowie die verbleibenden Restrisiken akzeptieren und übernehmen muss.

6 Vergleich zu COBIT

Als Modell (oder Werkzeug) soll das COBIT-Framework zur Umsetzung und Sicherstellung der IT-Governance beitragen. IT-Governance wiederum beschäftigt sich mit der Organisation, Steuerung und Kontrolle der IT eines Unternehmens und soll u.a. sicherstellen, dass die Unternehmensstrategie bzw. die Unternehmensziele unterstützt bzw. erreicht werden.

Da die Organisation, Steuerung und Kontrolle der IT selbstverständlich auch das Risikomanagement umfasst, ist COBIT zwangsläufig auch ein Framework für das IT-Risikomanagement, gleichwohl mit einem anderem strukturellen Aufbau und einem anderen Ansatz als die ISO 31000.

Nachfolgend werden die wesentlichen Unterschiede, aber auch die – sich gegenseitig – ergänzenden Funktionen beider Frameworks aufgezeigt. Grundlage der Diskussion sind die COBIT-Versionen 4.0 bzw. 4.1 (eine Erarbeitung auf Basis der Version 5.0 ist vorgesehen).

Unterschiede im strukturellen Aufbau der Frameworks bezüglich der Anforderungen an das Risikomanagement

Die ISO 31000 hat einen klaren Fokus auf das Risikomanagement mit folgenden Strukturelementen:

- Auftrag und Vereinbarung
- Gestaltung des Risikomanagements
- Anwendung des Risikomanagements
- Überwachung und Überprüfung
- Kontinuierliche Verbesserung

COBIT (Control Objectives for Information and related Technology) ist ein Prozessmodell mit 34 Prozessen. Ein Prozess dieses Frameworks – »Beurteile und manage IT-Risiken« – beschäftigt sich explizit mit dem Thema Risikomanagement.

Die o.a. wesentlichen Strukturelemente der ISO 31000 werden hier zwar auch adressiert, allerdings ohne konkrete Hinweise auf die inhaltliche Ausgestaltung. Anders ausgedrückt, gibt das COBIT-Framework Hinweise, was zu tun ist, ohne direkt darauf einzugehen, wie eine Umsetzung erfolgen könnte.

Im Einzelnen fordert COBIT:

- Abstimmung des Risikomanagements der IT und des Unternehmens
- Festlegung des Risikokontextes
- Ereignisidentifikation
- Bewertung von Risiken
- Maßnahmen zur Risikobehandlung
- Erhalt und Monitoring eines Plans zur Risikobehandlung

COBIT als Hilfskonstrukt bei der Risikoidentifikation

Im Rahmen der Risikoidentifikation kann COBIT sehr umfassende Informationen hinsichtlich potenzieller Risiken im IT-Umfeld liefern. Die in den COBIT-Prozessen definierten Kontrollziele adressieren inhärente Risikobereiche in der IT. Damit können sie (Kontrollziele) – umformuliert – auch als potenzielle IT-Schwachstellen angesehen werden (siehe auch ISACA-Leitfaden: IT-Risikomanagement – leicht gemacht mit COBIT).

Bewertung von Risiken mittels COBIT

Die den COBIT-Prozessen zugeordneten KPIs – zur Messung der Prozessqualität – können direkt herangezogen werden, um Schwachstellen und Risikoauswirkungen zu bewerten.

Risikobehandlungsmaßnahmen mit COBIT

Neben den IT-Prozessen und Kontrollzielen beinhaltet COBIT auch ein Reifegradmodell auf Prozessebene. Dieses Reifegradmodell erlaubt es, den entsprechenden Schwachstellen adäquate Risikobehandlungsmaßnahmen entgegenzusetzen.

7 Vergleich zu BSI IT-Grundschutz-Standard 100-3

Die ISO 31000 beinhaltet neben einer Beschreibung des Rahmenwerks zum Risikomanagement generische Hinweise und Empfehlungen zum Aufbau und Betrieb eines Risikomanagementsystems sowie eine generische Beschreibung eines Risikomanagementprozesses. Das Risikomanagementsystem muss individuell ausgestaltet und in die jeweilige Gesamtorganisation integriert werden.

Der Standard 100-3 des Bundesamtes für Sicherheit in der Informationstechnik (im Folgenden »BSI« genannt) fokussiert auf die Risikoanalyse als Teil des Risikomanagementprozesses. Er beinhaltet die konkrete Beschreibung einer Methodik, wie aufbauend auf den Grundschutz-Katalogen und den BSI-Standards 100-1 und 100-2 eine vereinfachte Risikoanalyse für Risiken der Informationsverarbeitung durchgeführt werden kann.

Voraussetzung für die Anwendung des BSI-Standards 100-3 ist daher ein bestehendes Sicherheitskonzept auf der Basis von BSI IT-Grundschutz. Hierzu müssen die folgenden Vorarbeiten abgeschlossen sein:

- Initiierung eines systematischen Informationssicherheitsprozesses
- Abgrenzung des Anwendungsbereiches (Informationsverbund)
- Durchführung der Strukturanalyse
- Durchführung der Schutzbedarfsfeststellung
- Durchführung der Modellierung
- Durchführung des Basis-Sicherheitschecks
- Durchführung der ergänzenden Sicherheitsanalyse (Entscheidung, für welche Assets/Unternehmenswerte eine Risikoanalyse durchgeführt werden soll)

Die Methodik gemäß BSI-Standard 100-3 besteht aus folgenden Schritten:

- Erstellung einer Gefährdungsübersicht (… aufbauend auf den Ergebnissen der Modellierung)
- Ermittlung zusätzlicher Gefährdungen
- Gefährdungsbewertung hinsichtlich
  - Vollständigkeit (… des Schutzes der bereits umgesetzten Maßnahmen gegen alle Aspekte der Gefährdung)
  - Mechanismenstärke (… der bereits umgesetzten Maßnahmen)
  - Zuverlässigkeit (… der Wirkung der bereits umgesetzten Maßnahmen)
- Risikobehandlung
- Konsolidierung des Sicherheitskonzeptes
- Rückführung in den Sicherheitsprozess

Die Methodik beinhaltet dabei lediglich eine implizite Bewertung der Wahrscheinlichkeit und Auswirkungen von Risiken im Rahmen der Ermittlung und Bewertung von Gefährdungen.

Insbesondere die Abhängigkeit des ersten Schrittes der Methodik »Erstellung einer Gefährdungsübersicht« vom Vorhandensein eines Sicherheitskonzeptes auf Basis von BSI IT-Grundschutz verhindert eine Anwendung dieser Methodik in Verbindung mit anderen Standards wie ISO 27001.

Abhilfe schafft hierbei eine Ergänzung des BSI-Standards 100-3 »Verwendung der elementaren Gefährdungen aus den IT-Grundschutz-Katalogen zur Durchführung von Risikoanalysen« des BSI. Diese Ergänzung modifiziert den ersten Schritt »Erstellung einer Gefährdungsübersicht« dahingehend, dass statt der Gefährdungen als Ergebnis der Modellierung sogenannte elementare Gefährdungen verwendet werden.

Es werden 46 produkt- und technikneutrale Gefährdungen aufgeführt und hinsichtlich der Beeinträchtigung den Grundwerten »Vertraulichkeit«, »Integrität« und »Verfügbarkeit« zugeordnet. Diese werden im Rahmen der Bearbeitung der weiteren Schritte der Methodik verwendet.

Mithilfe dieser Modifikation der Methodik des BSI-Standards 100-3 wird dessen Anwendung auch ohne ein zuvor erstelltes Sicherheitskonzept auf Basis von BSI IT-Grundschutz ermöglicht und damit einem neuen Anwenderkreis erschlossen. Ist eine explizite Bewertung der Eintrittswahrscheinlichkeit und Auswirkungen eines Risikos gefordert, ist der Einsatz des BSI-Standards 100-3 jedoch ohne weitere Modifikationen der Methodik nicht zu empfehlen.

Fazit und Ausblick

Mit der Novellierung der ISO 27001 im Jahr 2013 wurde die ISO 31000, wie bereits vorher von der ISO-Organisation angekündigt, zum Maßstab für Risikomanagement in allen ISO-geregelten Managementsystemen – hier im Informationssicherheitsmanagement – erhoben. Es bleibt abzuwarten, inwieweit dies noch in den nächsten Jahren Ausstrahlungswirkung auf weitere IT-

nahe Standards, Frameworks und Methoden haben wird.

In jedem Fall kann man gespannt sein auf die neue Fassung der ISO 31000, die für 2015 angekündigt ist und dann möglicherweise auch die für die IT relevanten Änderungen enthalten wird.

Definitionen

Dieser Leitfaden möchte keine eigenen Definitionen darstellen, sondern auf die entsprechenden Abschnitte der bereits genannten Standards verweisen.

In der ISO 31000 sind diese im Kapitel 2 »Terms and Definitions« auf Seite 1 zu finden.

Die ONR 49000 weist das Kapitel 3 »Begriffe« auf, das neben den deutschen Begriffen auch englische und französische Übersetzungen enthält.

ISO 27005 übernimmt in der gültigen Version 2011 aus Vereinheitlichungsgründen die Definitionen der ISO 31000.

Danksagung

Die erste Version des Leitfadens und Nachschlagewerks »ISO 31000 in der IT« entstand durch die enge Zusammenarbeit zwischen ISACA Germany Chapter e.V. und RMA e.V.

Unser Dank gilt allen Beteiligten am Zustandekommen des Leitfadens für das kontinuierliche Interesse am Thema sowie die zahlreichen Textbeiträge, Darstellungen und die redaktionelle bzw. Reviewarbeit, die diesen umfassenden Leitfaden erst ermöglichten.

Feedback zu den Inhalten ist seitens der Autoren erwünscht und kann über die Internetauftritte der beteiligten Verbände gerne geäußert werden.


CISA
Certified Information Systems Auditor
An ISACA Certification
CISM
Certified Information Security Manager
An ISACA Certification
CRISC
Certified in Risk and Information Systems Control
An ISACA Certification
CGEIT
Certified in the Governance of Enterprise IT
An ISACA Certification