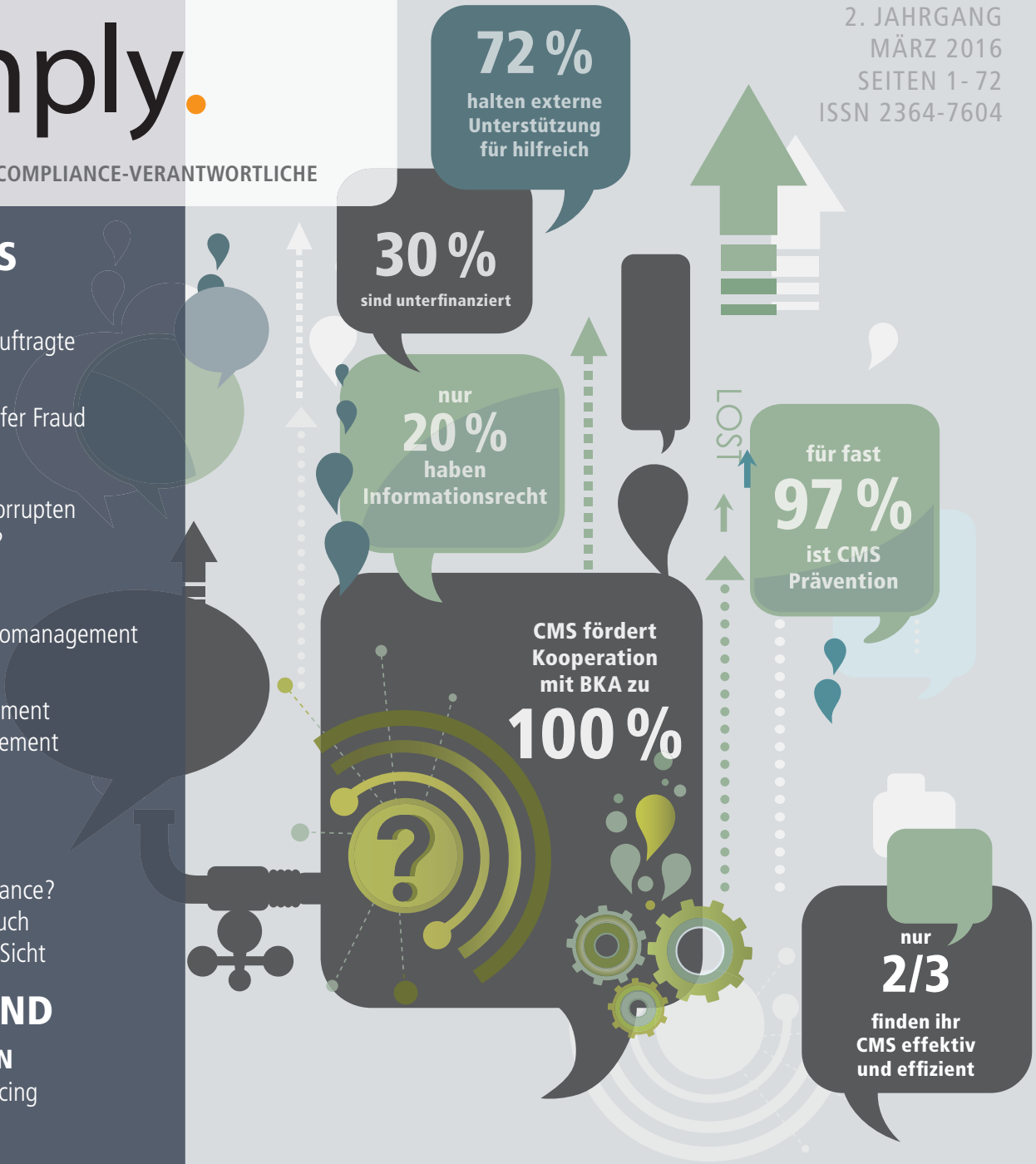
Best Practice für Compliance und Sicherheit

01/2016

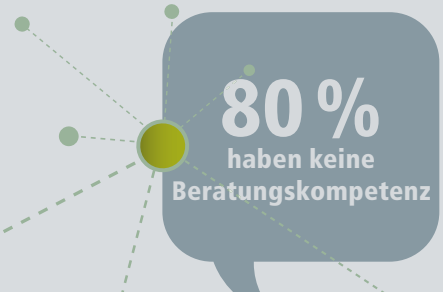
www.comply-online.de
2. JAHRGANG
MÄRZ 2016
SEITEN 1- 72
ISSN 2364-7604

comply.

FACHMAGAZIN FÜR COMPLIANCE-VERANTWORTLICHE



Compliance in Zahlen



Bundesanzeiger Verlag

COMPLIANCE ACADEMY

IN KOOPERATION MIT:

Viadrina Compliance Center

Der risikobasierte Ansatz der ISO 19600 und Risikomanagement nach ISO 31000

Wie sich Compliance-Risiken im Rahmen eines Risk Management Systems nach ISO 31000 steuern lassen

Einer der Vorwürfe, die der Norm „ISO 19600 Compliance Management Systems (CMS)“ entgegengebracht werden, geht dahin, dass die Norm zwar einen risikobasierten Ansatz verfolge, zum Riskmanagement selbst aber wenige Empfehlungen enthalte. Der Vorwurf erweist sich jedoch schnell als falsch, wenn der Verweis der Norm auf „ISO 31000 Risikomanagement – Grundsätze und Leitlinien“ beachtet wird. Der Autor beleuchtet anhand von konkreten Beispielen, wie sich Compliance-Risiken im Rahmen eines integrierten Riskmanagementsystems nach ISO 31000 steuern lassen und welche konkreten Prozessschritte es dabei zu beachten gilt.

Prae ISO 19600

In der Vergangenheit stand die Frage im Raum, ob Compliance nur ein neuer Begriff oder eine neue Aufgabe sei. Nr. 4.1.3 des DCGK (Deutscher Corporate Governance Kodex) definierte Compliance als Absicherung der Einhaltung gesetzlicher Bestimmungen und der unternehmensinternen Richtlinien.[1] Mit dem Hinweis, dass in der komplexen Welt inzwischen eine systematische Herangehensweise erforderlich sei, wurde die Entwicklung, Implementierung, Anwendung und Weiterentwicklung eines Compliance-Programms gefordert, z.B. in einem Drei-Säulen-Modell, bei dem Compliance von den Säulen Commitment, Organisation und Leadership getragen wird.[2] Dabei wurde für die dritte Säule die Verzahnung mit der Internen Revision und dem Risikomanagement dargestellt; der Anglizismus sollte verdeutlichen, dass es dabei um mehr als direkte Mitarbeiterführung geht.

Abbildung 1: Drei-Säulen-Modell eines Compliance-Programms

ISO 19600 als Managementsystemnorm

Mit der ISO 19600 wurden 2014 auf der Basis eines globalen Konsenses Empfehlungen zur Einführung, Entwicklung, Implementierung, Bewertung, Erhaltung und Verbesserung eines effektiven, bedarfsgerechten Compliance Management Systems (CMS) veröffentlicht. Die Norm ist im Aufbau und zum Teil im Wortlaut identisch mit dem Aufbau anderer neuer Managementsystemnormen der ISO (MSS) – z.B. der ISO 9001:2015 zum Qualitätsmanagement. Das erleichtert dem Anwender die Integration seines Compliance Managements zusammen mit den anderen Bausteinen (z.B. seinem Qualitätsmanagement) in ein einheitliches/holistisches Managementsystem. Ein Eckpfeiler der MSS-Struktur der ISO ist der sogenannte risikobasierte Ansatz aller neuen MSS, der sich insbesondere in den Abschnitten 6 und 8 der ISO 19600 wiederfindet.

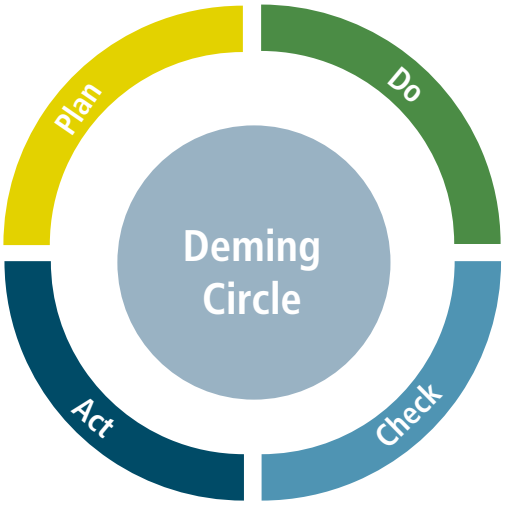


Abbildung 2: Das PDCA-Modell

Alle MSS folgen dem PDCA-Modell.[3] Ein CMS soll nach ISO 19600 die Grundsätze Verhältnismäßigkeit und Flexibilität, Transparenz sowie Nachhaltige Compliance-Kultur einhalten. Im operativen Bereich legen folgende Grundschritte nahe, wie das CMS kostengünstig in jedem Organisationstyp eingeführt und gepflegt werden kann: Aufgaben der Unternehmensleitung, Informationsbeschaffung, Compliance-Programm, Rollenzuweisung, Operative Compliance, Aufklärung und Verbesserung sowie Berichterstattung und Dokumentation.[4]

Risikobasierter Ansatz und Bedeutung der ISO 31000 im Rahmen eines CMS nach ISO 19600

Die Unternehmensleitung muss sich aktiv zum CMS bekennen, es ermöglichen, indem sie ausreichende Ressourcen bereitstellt, sowie es aktiv unterstützen und überprüfen. Wenn Grundstrukturen und Plan feststehen, müssen ausreichende Informationen über das Unternehmen und sein Umfeld gesammelt werden.

Neben der Ermittlung und Dokumentation der Compliance-Pflichten (Abschnitt 4.5) sind Identifikation, Analyse und Bewertung der Compliance-Risiken (Abschnitt 4.6) hier die zentrale Aufgabe. In diesem Zusammenhang stellt es die ISO 19600 dem Anwender frei, ob eine formale Risikobeurteilung durchgeführt oder ein anderer Ansatz gewählt wird, verweist aber in der NOTE 3 auf die ISO 31000 für detaillierte Empfehlungen zur Risikobeurteilung.

Compliance-Risiken sind zu ermitteln, indem die Compliance-Pflichten in Beziehung zu allen relevanten Betriebsaspekten gesetzt werden, um die Situationen zu identifizieren, in denen Compliance-Verstöße vorkommen können. Das bedeutet, dass ISO 19600 tatsächlich nur negative Abweichungen für das Compliance-Risiko kennt, obwohl die weite Bedeutung der ISO 31000 (positive oder negative Abweichungen) in den Definitionen 3.11 und (nach ihrem Wortlaut) 3.12 übernommen wurde. Die Compliance-Risiken müssen nach den Vorgaben des Abschnittes 4.6 regelmäßig und darüber hinaus in bestimmten Situationen neu eingeschätzt werden.

Dr. Frank Herdmann

Der Autor ist Leiter der DIN-Delegation zum ISO/TC 262 Risikomanagement. Der Jurist und langjährige Geschäftsführer mittelgroßer Unternehmen berät selbst Unternehmensführungen in Managementfragen einschließlich Compliance und Risikomanagement.

www.herdmann.de

Für den Umgang mit den Compliance-Risiken sind die notwendigen Maßnahmen nach Abschnitt 6.1 zu planen und ihre Effektivität zu überwachen und zu dokumentieren. Die Empfehlung in Abschnitt 8.1 lautet, dafür entsprechende Geschäftsprozesse zu implementieren. Nach Abschnitt 8.2 sind dazu Kontrollmechanismen einzurichten, die möglichst in die allgemeinen Organisationsprozesse einzubetten sind.

Struktur und Ansätze der ISO 31000

In der ISO 31000 wird ein etwas anderer Ansatz verfolgt. Zum einen wird betont, dass es sich nicht um ein MSS handele sondern nur um generische Empfehlungen. Die Struktur unterscheidet sich fundamental von den Vorgaben der ISO für die MSS. Trotzdem haben die Regeln über die Schaffung eines angemessenen Rahmens für das Risikomanagement in Abschnitt[4] einen breiten Umfang. Im Abschnitt 5 finden sich detaillierte (und hilfreiche) Vorgaben für den Risikomanagementprozess, im Abschnitt 1 zum Anwendungsbereich findet sich der Harmonisierungsauftrag unter dem Primat der Norm. Im DIN (Deutsches Institut für Normung e.V.) wurde daraus der Rückschluss gezogen, dass die Norm dennoch ein Managementsystem abbilde und einen unerwünschten Zertifizierungsdruck erzeugen könne.[5]

Die »ISO 31000 Risikomanagement – Grundsätze und Leitlinien« ist in fünf Abschnitte und einen informativen Anhang mit drei Abschnitten gegliedert. Im Abschnitt 1 wird der Anwendungsbereich sehr weit (für alle Unternehmen, Vereinigungen und sonstigen Organisationen oder Einzelpersonen in allen Wirtschaftszweigen und Sektoren zu allen Zeiten und für alle Risiken) gefasst.

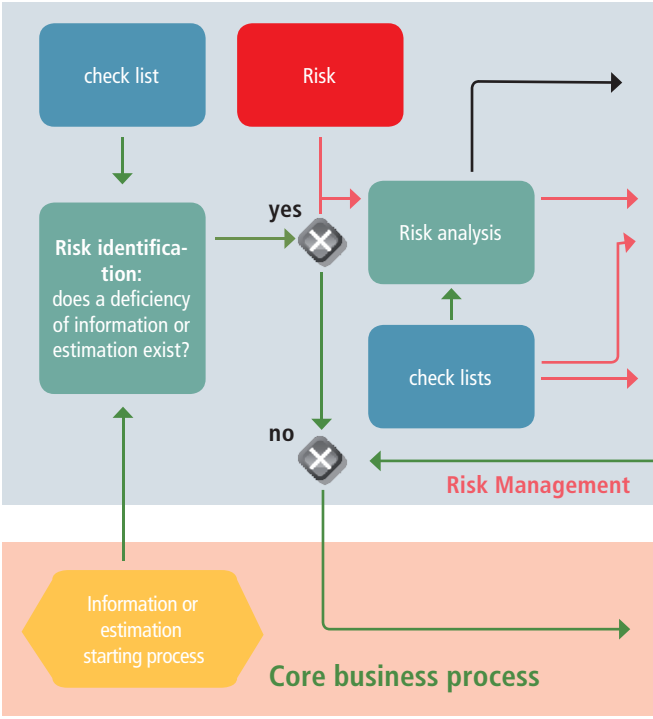


Abbildung 5: Der Core Business Process

Abschnitt 2 enthält die wesentlichen Definitionen, wobei die Definition 2.1 das Risiko mit Auswirkung von Unsicherheit auf Ziele ebenso weit fasst und dazu erläutert, dass mit der Auswirkung eine Abweichung von den Erwartungen gemeint sei – in positiver und/oder negativer Hinsicht. Auch diese Definition ist im DIN kritisiert worden, weil es bei der menschlichen Sicherheit, im Gesundheitsschutz und im Umweltschutz keine Risiken mit „positiven Auswirkungen" gebe.[6] Die Abschnitte 3 bis 5 werden in der Einleitung in einem Schaubild zusammengefasst. Abschnitt 3 behandelt die im Schaubild aufgeführten elf Grundsätze, die ein wirkungsvolles Risikomanagement erfüllen solle. Von den Grundsätzen in

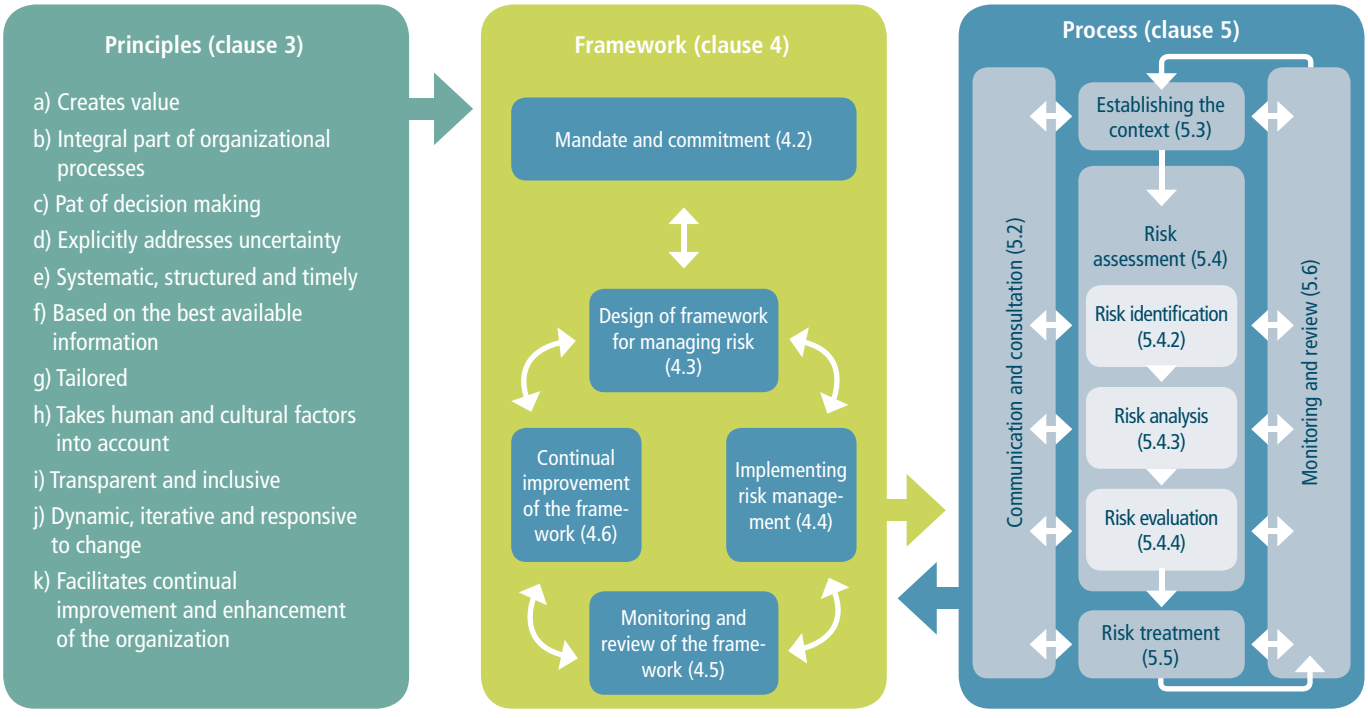
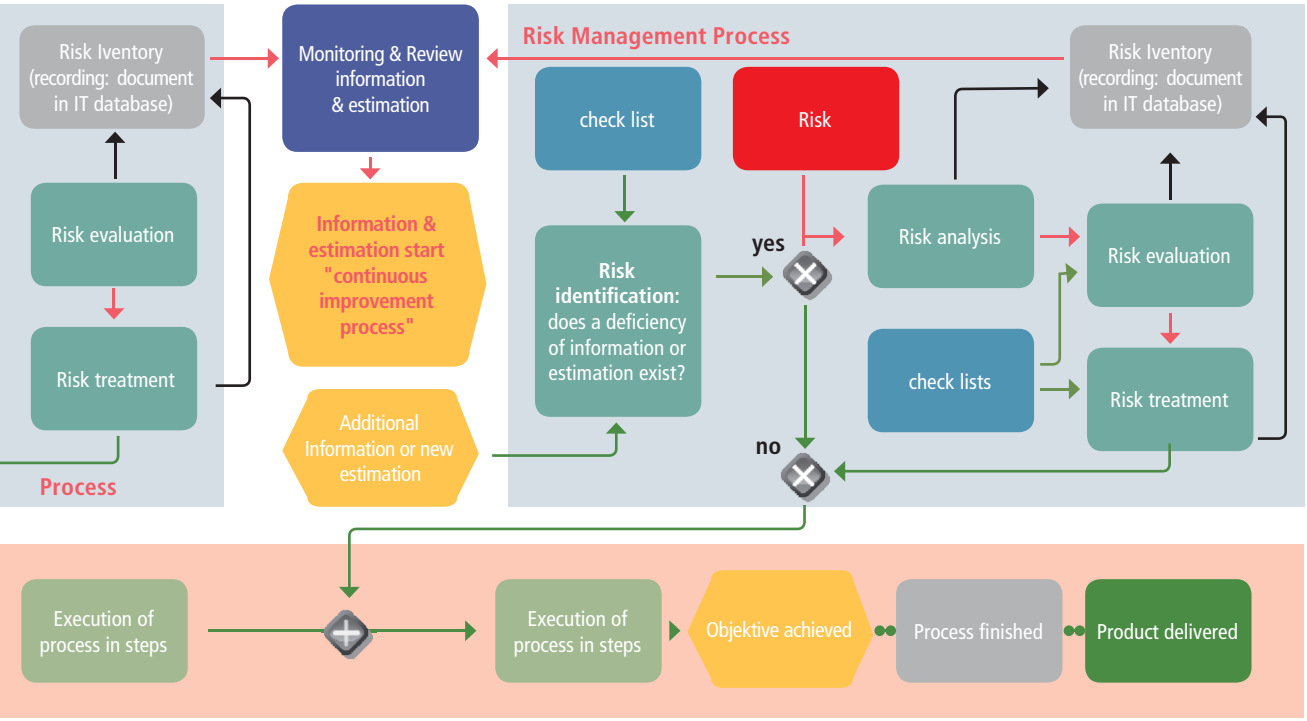


Abbildung 3: Nach ISO 31000 (Figure 1 – Relationships between the risk management principles, framework and process)[7]



Abschnitt 3 bedarf der zweite [b) Risikomanagement ist Bestandteil aller Organisationsprozesse] besonderer Erwähnung. Neben der breiten oder besser janusköpfigen Definition von Risiko, die Chancen mit einschließt, ist hier die entscheidende Regel der ISO 31000 zusammengefasst: Risikomanagement ist keine eigenständige Aufgabe besonderer Funktionsträger, sondern muss in allen Bereichen einer Organisation von allen und zu allen Zeiten für ihre eigenen Zuständigkeiten vorgenommen werden. Die Abschnitte 4 und 5 behandeln die Rahmenbedingungen und den Prozess.

Management von Compliance-Risiken nach ISO 31000

Mit dem Grundsatz b) und dem allgemeinen Teil von Abschnitt 5 wird der Unterschied zu dem risikobasierten Ansatz in den spezifischen MSS wie der ISO 19600 oder auch der ISO 9001 deutlich. Dort ist das Risikomanagement naturgemäß auf den jeweiligen Sachzusammenhang beschränkt, so im Compliance Management z.B. auf die Konsequenzen aus der Noncompliance. Nach der ISO 31000 sind die Auswirkungen aller Abweichungen von Erwartungen – in positiver wie negativer Hinsicht – zu berücksichtigen. Dies hindert jedoch keineswegs, ISO 31000 im Rahmen der ISO 19600 und der dort zu behandelnden Compliance-Risiken anzuwenden, um so ein kohärentes System zu etablieren.

Die Gestaltung des Rahmens für das Risikomanagement wird in Abschnitt 4.3 von ISO 31000 behandelt: Sowohl der externe als auch der interne Zusammenhang der Organisation sind auszuwerten, die Risikomanagementpolitik festzulegen, die Verantwortlichkeiten und Kompetenzen sind festzulegen, entsprechende Ressourcen bereitzustellen, die interne und die externe Kommunikation zu organisieren und das Berichtswesen sicherzustellen. Auch hier wird noch einmal betont, dass Risikomanagement in alle Verfahren und Prozesse der Organisation eingebettet werden sollte. Der Risikomanagementprozess sollte Teil der Organisationsprozesse werden und nicht getrennt von ihnen ablaufen.

Der Risikomanagementprozess

Der wichtigste Teil der ISO 31000 befasst sich mit dem Prozess. Der Kernprozess ist in der Abbildung 5 farbig Blau-Grau hinterlegt dargestellt und die relevanten Abschnitte der Norm sind mit ihren Gliederungspunkten aufgeführt. Auch hier wird die Bedeutung der Kommunikation und Konsultation mit den internen Stakeholdern hervorgehoben und externer (Umfeld) wie interner Zusammenhang (interne Gegebenheiten) sind zu ermitteln. (Siehe Abbildung 5 auf der nächsten Seite)

Dann folgen die drei Schritte der Risikobeurteilung (Risikoidentifikation, -analyse und -bewertung) und die Risikobewältigung sowie Überwachung und Dokumentation. Abbildung 6 zeigt, wie der Kernprozess in einen Geschäftsprozess eingebunden werden kann.

Zur Aufwandsminimierung empfiehlt es sich, das Risikomanagement im Rahmen der Modellierung (oder Aktualisierung) der Geschäftsprozesse für das Organisationshandbuch des Unternehmens (OHB) zu berücksichtigen und dabei eine Kombination von grafischer Darstellung und textlicher Erläuterung zu verwenden. Zu den einzelnen Prozess-Schritten sollten die notwendigen Hilfsmittel (Entscheidungsmatrix, Musterschreiben, Checklisten etc.) hinterlegt werden. Welche (wesentlichen) Prozesse den Weg in das OHB finden, muss das Unternehmen selbst [vergl. Grundsatz g): Risikomanagement ist maßgeschneidert] entscheiden. Es bildet, sobald das Unternehmen die Größe eines Kleinbetriebes überschreitet, die unverzichtbare Basis für eine gute Unternehmensführung und damit für die Vermeidung von Organisationsverschulden.[8]

Beispiele für die Prozessverzahnung

In der ISO 19600 wird in den Abschnitten 4.5.1 und 4.5.2 die Identifikation der Compliance-Pflichten und in Abschnitten 5.2.1 und 5.2.2 die Etablierung der Compliance-Politik beschrieben. Die Organisation kann sich entscheiden, für diese Aufgaben einen oder zwei Prozesse im OHB abzubilden.

Der im Abschnitt 4.6 dargestellte risikobasierte Ansatz kann zu der Entscheidung führen, in diesen Prozess bzw. diese Prozesse in den Risikomanagementprozess in der oben dargestellten Form zu integrieren. Zur Sicherstellung von Relevanz, Wirksamkeit und Effizienz des Risikomanagements wird die Integration im Grundsatz b) der ISO 31000 empfohlen[9] – diese ist insofern präziser (oder enger) als die ISO 19600. Risikomanagement betrifft ausdrücklich die Unternehmensleitung genauso wie alle Unternehmensteile einschließlich der strategischen Planung und aller Projekte und Veränderungsprozesse.[10]
Das Gleiche gilt bei Aufbau und Unterstützung des Compliance Management Systems nach Abschnitt 7 und bei Umgang mit Compliance-Risiken und Verstößen nach den Abschnitten 8.1 und 8.2 sowie 10.1 der ISO 19600.

FAZIT

Risikomanagement nach ISO 31000 kann als Bindeglied aller Managementsysteme eingesetzt werden. Die Grundsätze und Leitlinien der Norm ergänzen die Empfehlungen und Vorgaben der Standards spezifischer Managementsystemnormen. Das gilt um so mehr, wenn solch eine Norm – wie die ISO 19600 – ausdrücklich auf die ISO 31000 verweist. Beide Standards sind miteinander verzahnt und vereinfachen damit die Anforderungen der Governance an das Management, was sich besonders bei kleineren und mittleren Unternehmen positiv im Sinne von Synergien und Aufwandsreduktion auswirkt.

1 DCGK 2013 Nr. 4.1.3 - http://www.dcgk.de/de/kodex/archiv.html?file=files/dcgk/usercontent/de/download/kodex/D_CorGov_Endfassung_2013.pdf.
2 Vergl. z.B. Herdmann, Executive Summary Nr. 12 (2013 – Dezember) - http://herdmann.de/executive/nummer12.php.
3 PDCA = Plan – Do – Check Act (Demingkreis) – Darstellung nach Wikipedia: https://de.wikipedia.org/wiki/Demingkreis.
4 Makowicz, Compliance-Management-Systeme leicht gemacht! (comply. 1/2015, S. 36 – 39).
5 E DIN ISO 31000:2011-01 (Entwurf vom Januar 2011), S. 8 Nationale Fußnote N2).
6 E DIN ISO 31000:2011-01 (Entwurf vom Januar 2011), S. 3 Nationales Vorwort Abschnitt a).
7 ISO 31000:2009 (E), S. vii.
8 Herdmann, Executive Summary Nr. 8 (2012 – August) - http://herdmann.de/executive/nummer8.php.
9 ISO 31000:2009 (E), S. 11 Abschnitt 4.3.4 Abs. 1 – Übersetzung des Autors.
10 ISO 31000:2009 (E), S. 7 Abschnitt 3 b) – Übersetzung des Autors.

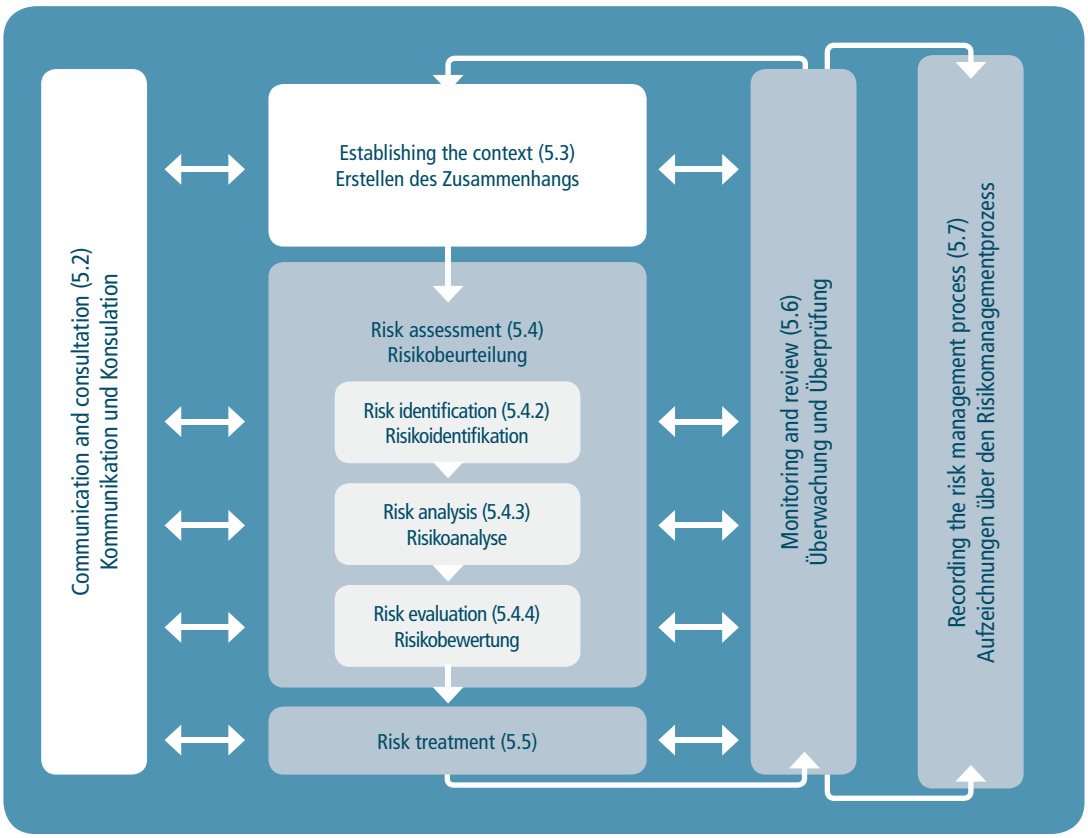


Abbildung 4: Der Risikomanagementprozess

Zur Vertiefung:

Praxishandbuch Compliance

Risikomanagement (2-10)

www.riu-online.de