Management Service zu Themen, die wichtig sind, aber immer wieder dem Eiligen weichen müssen. Kurz und knapp angerissen – in einer »**EXECUTIVE SUMMARY**«, die an ein solches wichtiges Thema erinnert und das Wesentliche dieses Themas zusammenzufasst.

Dauerbrenner Compliance und Risikomanagement reloaded

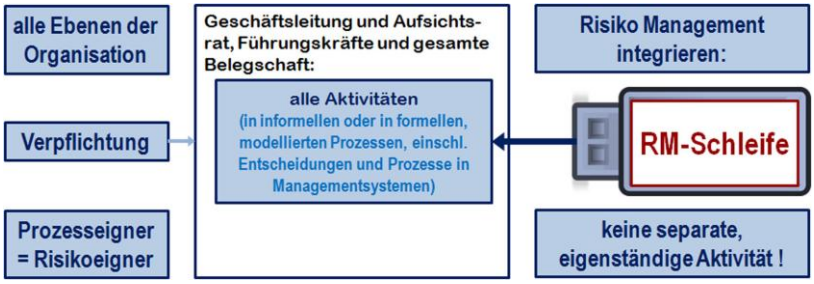
Die Nrn. 3 und 12 der EXECUTIVE SUMMARY befassten sich mit Compliance und die Nrn. 7 und 8 mit dem Thema Risikomanagement. Welche neuen Entwicklungen gibt es seitdem auf diesen wichtigen Gebieten? Um gleich auf den Punkt zu kommen: die ISO hat Ende 2014 die ISO 19600 veröffentlicht. Das ist eine Managementsystemnorm[1], die der sogenannten »High Level Structure« folgt. Was ist das? Um zu erreichen, dass die ISO Managementsystemnormen besser aufeinander abgestimmt sind, wurde in den Regularien eine einheitliche Struktur und einheitlicher Kern-Text incl. einheitlicher Definitionen vorgegeben.[2]

Inzwischen folgen mehr und mehr ISO-Normen dieser Struktur und zumeist dann auch dem vorgegebenen Wortlaut und weitere sind in der Entwicklung.[3] Die entscheidende Vorgabe findet sich im Abschnitt 6.1 des Appendix 2 (DIN Spec 36601), wonach das jeweilige Managementsystem einer Organisation (eines Unternehmens) Maßnahmen zum Umgang mit Chancen und Risiken vorsehen und in seine Prozesse integrieren sowie umsetzen muss. Diese Regelung ist von der ISO 19600 wortgetreu übernommen worden. Derzeit laufen die Arbeiten an der Übernahme der ISO 19600 als nationale DIN-Norm.

Der sogenannte risikobasierte Ansatz der Managementsystemnormen

Die Vorgabe, in den Managementsystemnormen Regelungen (verpflichtend – zertifizierbar – oder als Empfehlung – nicht zertifizierbar[4]) zum Umgang mit Risiken und Chancen vorzusehen, wird vielfach leicht irreführend als »risk based approch« (risikobasierter Ansatz bezeichnet. Auch in der ISO 19600 findet sich diese Terminologie in einem Obiter Dictum.[5] Im Abschnitt 4.6 geht diese Norm (zulässigerweise) über die Mindestanforderungen hinaus und macht Empfehlungen dazu, wie Compliance-Risiken zu identifizieren und bewerten sind, was in einer Randnotiz als risikobasierter Ansatz bezeichnet wird. Deutlich wichtiger erscheint allerdings die direkt darauffolgende NOTE 3, die auf die ISO 31000 verweist, die detaillierte Empfehlungen zur Risikobeurteilung gebe. Dieser Verweis auf die Risikomanagementnorm der ISO entspricht den Vorgaben im Abschnitt 6.1, wonach Maßnahmen zum Umgang mit Chancen und Risiken vorzusehen und in die Prozesse des Unternehmens zu integrieren sind.

Risikomanagement ist Bestandteil **aller** Organisationsprozesse



ISO 31000

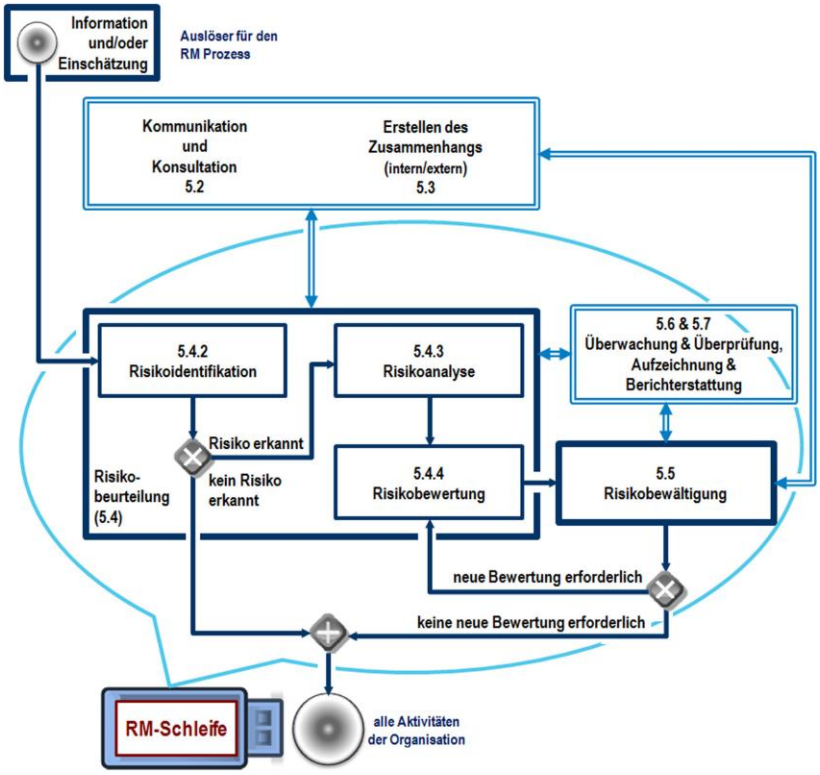
Seit 2009 finden sich in der – in Deutschland bisher nicht übernommenen – internationalen Norm Empfehlungen zum Risikomanagement. Darüber wurde zuletzt im August 2012 in der EXECUTIVE SUMMARY Nr. 8 (GESCHÄFTSPROZESSE UND ISO 31000) berichtet. Der wichtigste Ansatz dieser Norm findet sich im Grundsatz b), wonach Risikomanagement Bestandteil aller Organisationsprozesse ist.[6] Dabei kommt es nicht drauf an, ob für eine Aktivität ein formaller Geschäftsprozess (z.B. als EPK – ereignisgesteuerte Prozesskette) modelliert und dokumentiert wurde, weshalb der Terminus Prozesse auch durch den Begriff

[1] Erläuterungen zu Managementsystemnormen: http://www.iso.org/iso/home/standards/management-standards.htm
[2] ISO/IEC Directives Part 1, Annex SL, Appendix 2 (normative), deutsche Fassung: DIN Spec 36601
[3] Eine Liste findet sich auf der Webseite der ISO: http://www.iso.org/iso/home/standards/management-standards/mss-list.htm
[4] ISO 19600 hat als Managementsystemnorm Typ B nur empfehlenden Charakter und ist nicht zur Zertifizierung geeignet
[5] ISO 19600:2014, Clause 4.6 NOTE 2
[6] ISO 31000:2019, Clause 3 b)

Aktivität ersetzt werden kann, wie dies in obiger Graphik erfolgte. Diese zeigt auch, worum es eigentlich geht: Der Risikomanagementprozess soll in alle Aktivitäten des Unternehmens eingebunden werden – wie ein Plug-In-Dongle. Das gilt auch für die Prozesse der Managementsysteme wie dem Compliance Management oder dem Qualitätsmanagement (vergl. ISO 9001, die allerdings noch irreführender neben der HLS noch umfangreiche Ausführungen zu dem sogenannten »risk based thinking« enthält, zu dem gesonderte Ausführungen folgen werden).

Der Risikomanagementprozess als Plug-In-Dongle

Eine Unschärfe entsteht dadurch, dass Abschnitt 5 der ISO 31000 nicht nur den Kernprozess behandelt, sondern auch Regeln zur Modellierung bzw. Konfigurierung dieses Kernprozesses. Abweichend von den Abbildungen im Standard selbst hilft die Abbildung rechts den Kernprozess als Risikomanagement-Loop zu identifizieren, der an die einzelnen Aktivitäten/Geschäftsprozesse angedockt werden soll. Es geht letztlich weder um risikobasierten Ansatz noch um risikobasiertes Denken sondern darum, dass alle Aktivitäten der Organisation / des Unternehmens sich auf ein effektives und effizientes Risikomanagement stützen.



Compliance Risiken

Zentrale Aufgabe im Compliance Management ist die Identifikation, Analyse und Bewertung der Compliance Risiken. Diese sind zu ermitteln, indem die zuvor ermittelten und dokumentierten Compliance-Pflichten in Relation zu allen relevanten Betriebsaspekten gesetzt werden, um die Situationen zu identifizieren, in denen Compliance-Verstöße vorkommen können. Der Organisation / dem Unternehmen steht es frei, dies in einem modellierten Prozess im Organisationshandbuch abzubilden oder einen anderen geeigneten Ansatz zu wählen – in jedem Fall sollte dabei der RM-Loop in geeigneter Weise [nach ISO 31000 Grundsatz g) maßgeschneidert auf die Organisation] zum Einsatz kommen.

Weitere Einzelheiten zu diesem Thema sind von uns im März 2016 in der Ausgabe 01/2016 im Fachmagazins für Compliance-Verantwortliche »comply.« auf den Seiten 38 – 44 unter dem Titel »Der risikobasierte Ansatz der ISO 19600 und Risikomanagement nach ISO 31000« behandelt worden. Der Artikel findet sich auf unserer Webseite in der Rubrik »Themen im Fokus« zum Herunterladen. Als Fazit haben wir festgehalten, dass Risikomanagement nach ISO 31000 als Bindeglied aller Managementsysteme eingesetzt werden kann. Die Standards, die der High Level Structure der ISO folgen, sind miteinander verzahnt und vereinfachen die Anforderungen der Governance an die Unternehmensführung, was sich insbesondere bei kleinen und mittleren Unternehmen positiv im Sinne von Synergien und Aufwandsreduktion auswirkt.

Bei Fragen zu dieser »**EXECUTIVE SUMMARY**« wenden Sie sich bitte an:

Dr. Frank Herdmann, Auxilium Management Service
Gluckweg 10 | 12247 Berlin
Tel.: +49 30 – 771 90 321
Fax: +49 30 – 771 90 322
Mobil: +49 172 – 301 91 24
Mail: **auxilium@herdmann.de**